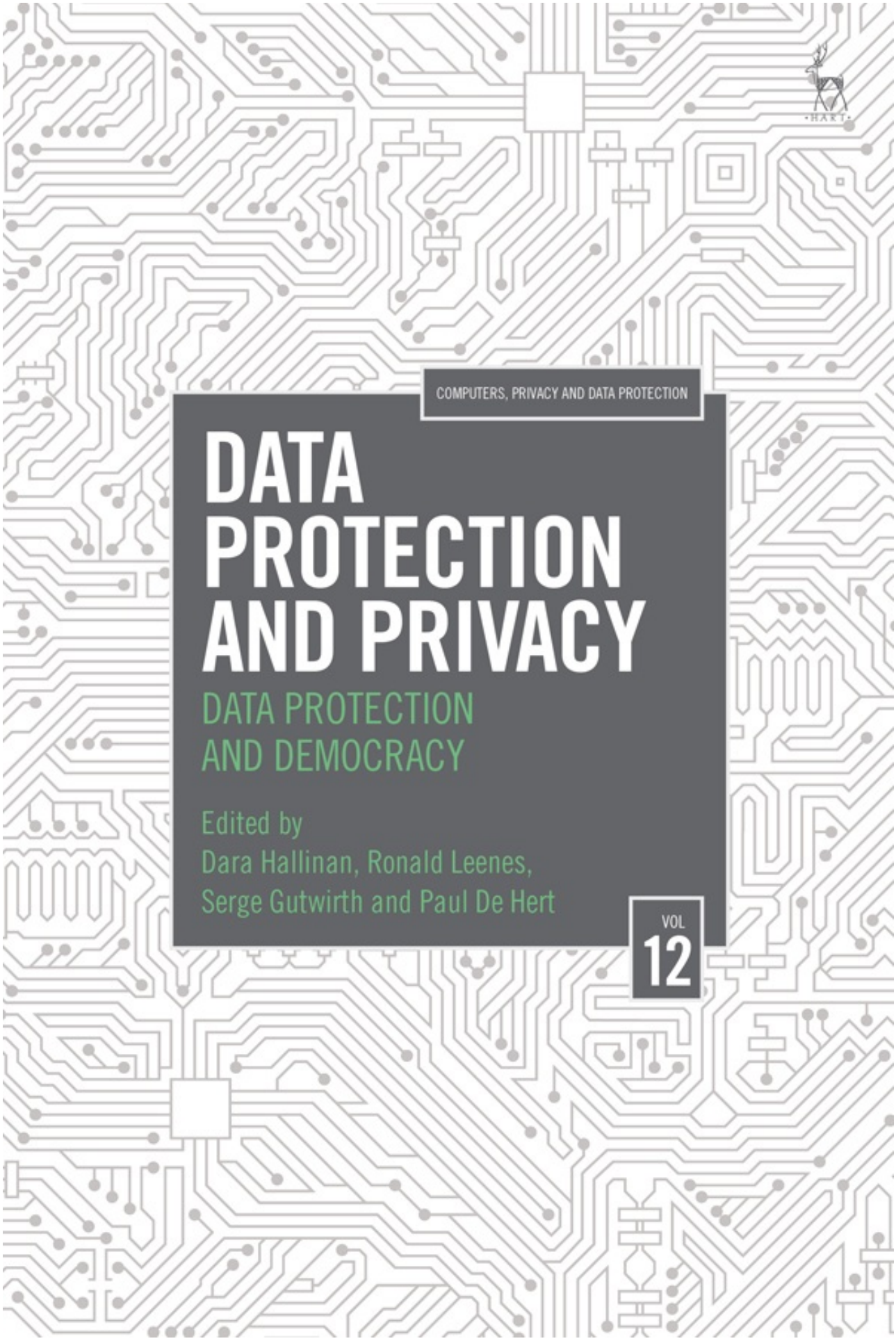

COMPUTERS, PRIVACY AND DATA PROTECTION
DATA PROTECTION AND PRIVACY
DATA PROTECTION AND DEMOCRACY
Edited by
Dara Hallinan, Ronald Leenes,
Serge Gutwirth and Paul De Hert
VOL
12

DATA PROTECTION AND PRIVACY

The subjects of this volume are more relevant than ever, especially in light of the raft of electoral scandals concerning voter profiling.

This volume brings together papers that offer conceptual analyses, highlight issues, propose solutions, and discuss practices regarding privacy and data protection. It is one of the results of the twelfth annual International Conference on Computers, Privacy and Data Protection, CPDP, held in Brussels in January 2019.

The book explores the following topics: dataset nutrition labels, lifelogging and privacy by design, data protection iconography, the substance and essence of the right to data protection, public registers and data protection, modelling and verification in data protection impact assessments, examination scripts and data protection law in Cameroon, the protection of children's digital rights in the GDPR, the concept of the scope of risk in the GDPR and the ePrivacy Regulation.

This interdisciplinary book has been written at a time when the scale and impact of data processing on society – not only on individuals, but also on social systems – is becoming ever starker. It discusses open issues as well as daring and prospective approaches, and will serve as an insightful resource for readers with an interest in computers, privacy and data protection.

Computers, Privacy and Data Protection

Previous volumes in this series (published by Springer)

2009
Reinventing Data Protection?
Editors: Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne, Sjaak Nouwt
ISBN 978-1-4020-9497-2 (Print) ISBN 978-1-4020-9498-9 (Online)

2010
Data Protection in A Profiled World?
Editors: Serge Gutwirth, Yves Poullet, Paul De Hert
ISBN 978-90-481-8864-2 (Print) ISBN: 978-90-481-8865-9 (Online)

2011
Computers, Privacy and Data Protection: An Element of Choice
Editors: Serge Gutwirth, Yves Poullet, Paul De Hert, Ronald Leenes
ISBN: 978-94-007-0640-8 (Print) 978-94-007-0641-5 (Online)

2012
European Data Protection: In Good Health?
Editors: Serge Gutwirth, Ronald Leenes, Paul De Hert, Yves Poullet
ISBN: 978-94-007-2902-5 (Print) 978-94-007-2903-2 (Online)

2013
European Data Protection: Coming of Age
Editors: Serge Gutwirth, Ronald Leenes, Paul de Hert, Yves Poullet
ISBN: 978-94-007-5184-2 (Print) 978-94-007-5170-5 (Online)

2014
Reloading Data Protection
Multidisciplinary Insights and Contemporary Challenges
Editors: Serge Gutwirth, Ronald Leenes, Paul De Hert
ISBN: 978-94-007-7539-8 (Print) 978-94-007-7540-4 (Online)

2015
Reforming European Data Protection Law
Editors: Serge Gutwirth, Ronald Leenes, Paul de Hert
ISBN: 978-94-017-9384-1 (Print) 978-94-017-9385-8 (Online)

2016
Data Protection on the Move
Current Developments in ICT and Privacy/Data Protection
Editors: Serge Gutwirth, Ronald Leenes, Paul De Hert
ISBN: 978-94-017-7375-1 (Print) 978-94-017-7376-8 (Online)

2017
Data Protection and Privacy: (In)visibilities and Infrastructures
Editors: Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth, Paul De Hert
ISBN: 978-3-319-56177-6 (Print) 978-3-319-50796-5 (Online)

Previous titles in this series (published by Hart Publishing)

2018
Data Protection and Privacy: The Age of Intelligent Machines
Editors: Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth, Paul De Hert
ISBN: 978-1-509-91934 5 (Print) 978-1-509-91935-2 (EPDF) 978-1-509-91936-9 (EPUB)

2019
Data Protection and Privacy: The Internet of Bodies
Editors: Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth, Paul de Hert
ISBN: 978-1-509-92620-6 (Print) 978-1-509-92621-3 (EPDF) 978-1-509-9622-0 (EPUB)

Data Protection and Privacy

Data Protection and Democracy

Edited by
Dara Hallinan
Ronald Leenes
Serge Gutwirth
and
Paul De Hert

•HART•
OXFORD • LONDON • NEW YORK • NEW DELHI • SYDNEY

PREFACE

It is the end of June 2019 as we write this foreword. Data protection is now more relevant than ever. Until recently, data protection seemed to be something of a niche topic, considered only by a small community of experts. Over the past year, however, following both the long-awaited applicability of the GDPR and the raft of prominent scandals concerning the illicit gathering and use of personal data – particularly those concerning the use of personal data in electoral campaigns – the relevance of data protection for society at large came clearly into focus. Now, everyone has an opinion.

This year thus arguably represented the moment in which data protection truly arrived in the public consciousness. It is no longer unusual to hear matters of data protection mentioned in the daily news or in coffee shop conversation. Yet, the prominence of the topic does not necessarily mean more, or better, data protection. Rather, the prominence of the topic simply means the fora in which it plays a role have grown more numerous and the balances it strikes have become more contested. There are likely few data controllers, for example, who now wish to collect less personal data due to the GDPR.

In the meantime, the international privacy and data protection crowd gathered in Brussels for the twelfth time to participate in the international Computers, Privacy and Data Protection Conference (CPDP) – between 30 January and 1 February 2019. An audience of over 1,100 people had the chance to discuss a wide range of contemporary topics and issues with 440 speakers in 90 panels, during the breaks, side events and at ad-hoc dinners and pub crawls. Striving for diversity and balance, CPDP gathers academics, lawyers, practitioners, policymakers, computer scientists and civil society from all over the world to exchange ideas and discuss the latest emerging issues and trends. This unique multi-disciplinary formula has served to make CPDP one of the leading data protection and privacy conferences in Europe and around the world.

The conference bustled with a sense of purpose. Conversations naturally dealt with the implementation and applicability of the GDPR. However, conversations also addressed much broader themes. Amongst these themes, the role of data protection in safeguarding democratic processes and democratic values – the core theme of the conference – featured prominently. Also heavily discussed were cross-cutting issues emerging around the need for, and the substance of, algorithmic regulation – the core topic of next year's conference.

The CPDP conference is definitely the place to be, but we are also happy to produce a tangible spin-off every year: the CPDP book. CPDP papers are cited very frequently and the series has a significant readership. The conference cycle starts with a call for papers in the summer preceding the conference. The paper submissions are peer reviewed and those authors whose papers are accepted present their work in the various academic panels at the conference. After the conference, speakers are also invited to submit papers based on panel discussions. All papers submitted on the basis of these calls are then (again) double-blind peer reviewed. This year, we received 14 papers in the second round, of which nine were accepted for publication. It is these nine papers that are to be found in this volume,

complemented by the conference closing speech traditionally given by the EDPS chair (then Giovanni Buttarelli).

The conference addressed many privacy and data protection issues in its 90 panels ranging from the impact of data processing on democracy, to AI regulation, to blockchain, to border control, to Islamic privacy, to research, to the implementation of the GDPR. The conference covered far too many topics to completely list them all here. For more information, we refer the interested reader to the conference website: www.cpdpconferences.org.

The current volume only offers a very small part of what the conference has to offer. Nevertheless, the editors feel the current volume represents a valuable set of papers describing and discussing contemporary privacy and data protection issues.

All the chapters of this book have been peer reviewed and commented on by at least two referees with expertise and interest in the relevant subject matters. Since their work is crucial for maintaining the scientific quality of the book, we would explicitly take the opportunity to thank all the CPDP reviewers for their commitment and efforts: Alessandro Mantelero, Anni Karakassi, Arnold Roosendaal, Ashwinee Kumar, Aviva de Groot, Bart Van der Sloot, Bert-Jaap Koops, Bettina Berendt, Carolin Moeller, Chiara Angiolini, Christopher Millard, Claudia Quelle, Colette Cuijpers, Damian Clifford, Daniel Le Métayer, Deepan Kamalakanthamurugan Sarma, Diana Dimitrova, Edoardo Celeste, Eleni Kosta, Emre Bayamlıoglu, Franziska Boehm, Frederik Zuiderveen Borgesius, Gabriela Zanfir-Fortuna, Gergely Biczók, Gianluigi Riva, Hideyuki Matsumi, Hiroshi Miyashita, Inge Graef, Ioannis Kouvakas, Ioulia Konstantinou, Iraklis Symeonidis, Irene Kamara, Ivan Szekely, Jaap-Henk Hoepman, Jef Ausloos, Joris van Hoboken, Joseph Savirimuthu, Kristina Irion, Lina Jasmontaite, Linnet Taylor, Lorenzo Dallacorte, Maria Grazia Porcedda, Marit Hansen, Massimo Durante, Michael Birnhack, Michael Friedewald, Michael Veale, Monica Palmirani, Nicholas Martin, Nicolo Zingales, Nora Ni Loideain, Omer Tene, Raphael Gellert, Robin Pierce, Rosamunde Van Brakel, Sascha Van Schendel, Shaz Jameson, Silvia De Conca, Simone Casiraghi, Tetyana Krupiy, Tjerk Timan and Yung Shin Van Der Sype.

As had become customary, the conference concluded with closing remarks from the European Data Protection Supervisor, Giovanni Buttarelli. All of us in the privacy community were profoundly saddened by Giovanni’s passing away in August 2019. He was a fervent and inspirational champion of privacy and digital rights. In recent years, he spearheaded efforts to put data protection at the heart of debates on digital ethics and democracy in the digital age. Giovanni’s support and fondness for CPDP was as invaluable as it was reciprocated, and he will be greatly missed. It is fitting and poignant that his closing remarks to the 2019 CPDP are the final chapter in this volume.

Dara Hallinan, Ronald Leenes, Serge Gutwirth & Paul De Hert
1 July 2019

TABLE OF CONTENTS

Preface
List of Contributors

1. *The Dataset Nutrition Label: A Framework to Drive Higher Data Quality Standards*
   Sarah Holland, Ahmed Hosny, Sarah Newman, Joshua Joseph and Kasia Chmielinski
2. *A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection*
   Lorenzo Dalla Corte
3. *What's in an Icon? Promises and Pitfalls of Data Protection Iconography*
   Arianna Rossi and Monica Palmirani
4. *'We're All in This Together': Actors Cooperating in Enhancing Children's Rights in the Digital Environment after the GDPR*
   Domenico Rosani
5. *Risk to the 'Rights and Freedoms': A Legal Interpretation of the Scope of Risk under the GDPR*
   Katerina Demetzou
6. *Modelling and Verification in GDPR's Data Protection Impact Assessment: A Case Study on the AccuWeather/Reveal Mobile Case*
   Wolfgang Schulz, Florian Wittner, Kai Bavendiek and Sibylle Schupp
7. *In Search of Data Protection's Holy Grail: Applying Privacy by Design to Lifelogging Technologies*
   Liane Colonna
8. *Public Registers Caught between Open Government and Data Protection – Personal Data, Principles of Proportionality and the Public Interest*
   Geert Lokhorst and Mireille van Eechoud
9. *Examination Scripts as Personal Data: The Right of Access as a Regulatory Tool against Teacher-Student Abuses in Cameroon Universities*
   Rogers Alunge
10. *The Proposed ePrivacy Regulation: The Commission's and the Parliament's Drafts at a Crossroads?*
    Elena Gil González, Paul De Hert and Vagelis Papakonstantinou
11. *CPDP: Closing Remarks*
    Giovanni Buttarelli

Index

LIST OF CONTRIBUTORS

Rogers Alunge is a candidate for a Joint PhD in Law, Science and Technology at the University of Bologna, Italy.

Kai Bavendiek is a PhD-candidate at Hamburg University of Technology.

Kasia Chmielinski is the Project Lead of the Data Nutrition Project, an initiative that launched out of Assembly (MIT Media Lab and Harvard University) which builds tools to improve the health of artificial intelligence through healthier data.

Liane Colonna is a post-doctoral fellow at the the Swedish Law and Informatics Research Institute (IRI).

Lorenzo Dalla Corte is a PhD candidate at Tilburg Law School (TILT) and a researcher at TU Delft (A+BE).

Paul De Hert is Professor of Criminal Law and Co-Director of the Law, Science, Technology & Society Research Group, Vrije Universiteit Brussel.

Katerina Demetzou is a PhD Researcher at the Business and Law Research Center (OO&R) and at the Institute for Computing and Information Sciences (iCIS) in Radboud University, Nijmegen, The Netherlands.

Elena Gil González is a PhD candidate at CEU San Pablo University of Madrid.

Sarah Holland is a member of the 2018 cohort of Assembly at the Berkman Klein Center & MIT Media Lab.

Ahmed Hosny is a machine learning scientist at Dana Farber Cancer Institute.

Joshua Joseph is a member of the Data Nutrition Project.

Geert Lokhorst is a research master student at the University of Amsterdam, Institute for Information Law.

Sarah Newman is a Senior Researcher at metaLAB at Harvard University, and a co-founder of the Data Nutrition Project, which creates tools to mitgate bias in algorithms by assessing the quality of the underlying data.

Monica Palmirani is full professor at CIRSFID (University of Bologna).

Vagelis Papakonstantinou is a professor of law at the Faculty of Law & Criminology of the Vrije Universiteit Brussel (VUB). He is the Coordinator of VUB's Cyber and Data Security Lab (CDSL), a core member of VUB's Research Group on Law Science Technology & Society (LSTS), and a research member of the Brussels Privacy Hub.

Domenico Rosani is a research and teaching associate at the University of Innsbruck, Department of Italian Law.

Arianna Rossi is a postdoc researcher at SnT – Interdisciplinary Centre for Security, Reliability and Trust (University of Luxembourg).

Wolfgang Schulz is the director of the Leibniz-Institute for Media Research | Hans-Bredow-Institute (HBI) and holds the chair for Media Law and Public Law including their Theoretical Foundations at University of Hamburg.

Sibylle Schupp is Head of the Software Technology Systems (STS) Institute at Hamburg University of Technology.

Mireille van Eechoud is Professor of Information Law at IVIR, University of Amsterdam.

Florian Wittner is a PhD candidate at Leibniz-Institute for Media Research | Hans-Bredow-Institute (HBI).

1

The Dataset Nutrition Label

A Framework to Drive Higher Data Quality Standards

SARAH HOLLAND,[1] AHMED HOSNY,[2] SARAH NEWMAN,[3] JOSHUA JOSEPH[4] AND KASIA CHMIELINSKI[5]

Abstract

Data is a fundamental ingredient in building Artificial Intelligence (AI) models and there are direct correlations between data quality and model robustness, fairness and utility. A growing body of research points to AI systems deployed in a wide range of use cases, where algorithms trained on biased, incomplete, or ill-fitting data produce problematic results. Despite the increased critical attention, data interrogation continues to be a challenging task with many issues being difficult to identify and rectify. Algorithms often come under scrutiny only after they are developed and deployed, which exacerbates this problem and underscores the need for better data vetting practices earlier in the development pipeline. We introduce the Dataset Nutrition Label,[6] a diagnostic framework built by the Data Nutrition Project, comprising a label that provides a distilled yet comprehensive overview of dataset 'ingredients'. The label is designed to be flexible and adaptable; it is comprised of a diverse set of qualitative and quantitative modules generated through multiple statistical and probabilistic modelling backends. Working with the ProPublica dataset 'Dollars for Docs', we developed an open source tool[7] consisting of seven sample modules. Consulting such a label prior to AI model development promotes vigorous data interrogation practices, aids in recognising inconsistencies and imbalances, provides an improved means to selecting more appropriate datasets for specific tasks and subsequently increases the overall quality of AI models. We also explore some challenges of the label, including generalising across diverse datasets, as well as discussing research and public policy agendas to further advocate its adoption and ultimately improve the AI development ecosystem.

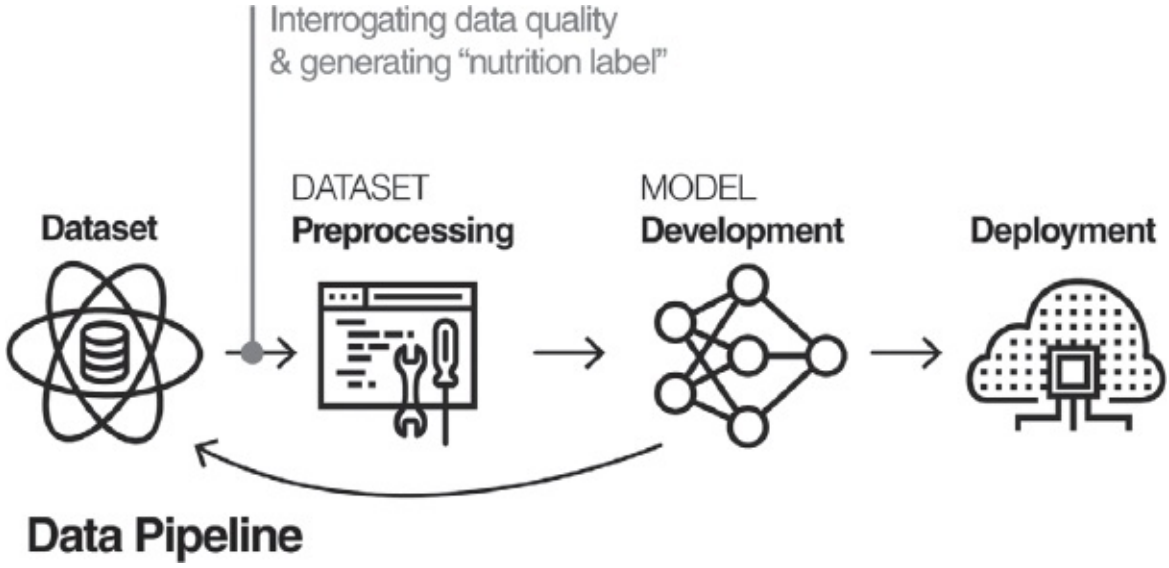
Keywords

Artificial intelligence, machine learning, data ethics, bias, ethics.

I. Introduction

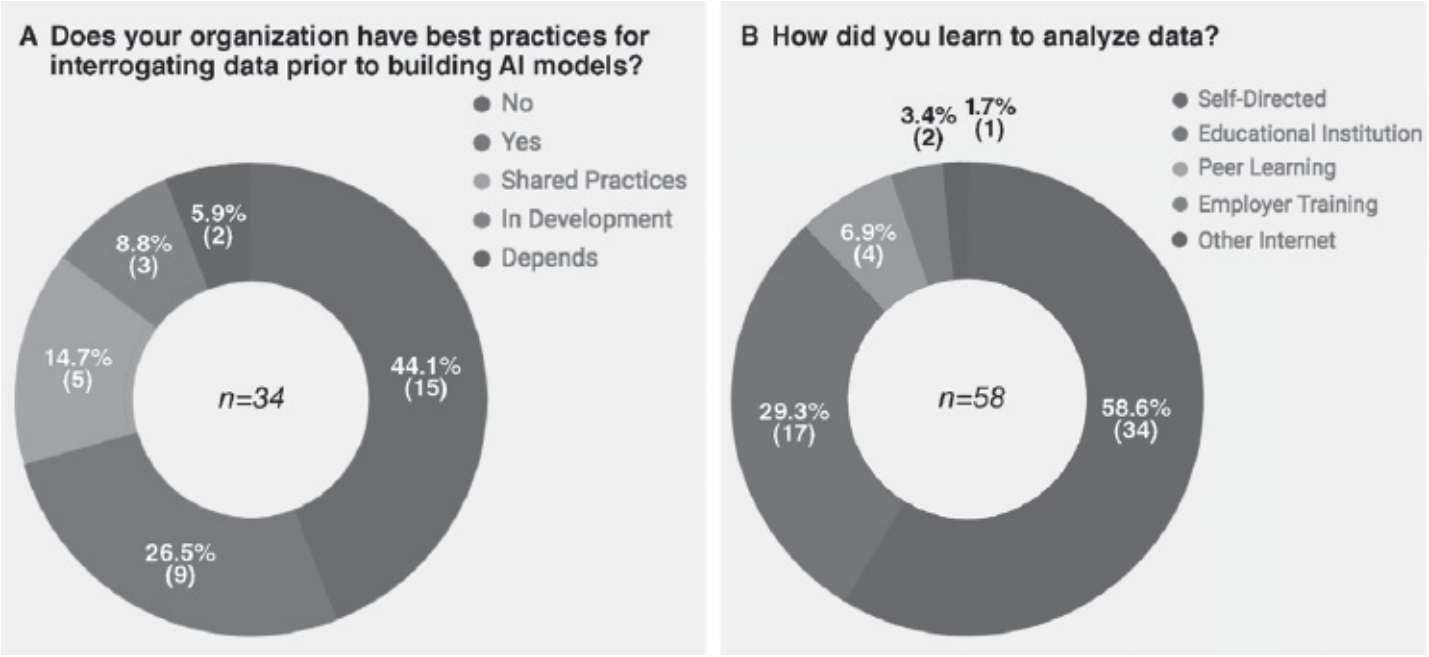
Data-driven decision-making systems play an increasingly important role in our lives. These frameworks are built on increasingly sophisticated artificial intelligence (AI) systems and are created and tuned by a growing population of data specialists[8] to arrive at a diversity of decisions: from movie and music recommendations to digital advertisements and mortgage applications.[9] These systems deliver untold societal and economic benefits, but they can also be harmful to individuals and society at large.

Figure 1.1 Model Development Pipeline



Data is a fundamental ingredient of AI and the quality of a dataset used to build a model will directly influence the outcomes it produces. An AI model trained on problematic data will likely produce problematic outcomes. Examples of these include gender bias in language translations surfaced through natural language processing[10] and skin shade bias in facial recognition systems due to non-representative data.[11] Typically, the model development pipeline (Figure 1.1) begins with a question or goal. Within the realm of supervised learning, for instance, a data specialist will curate a labelled dataset of previous answers in response to the guiding question. Such data is then used to train a model to respond in a way that accurately correlates with past occurrences. In this way, past answers are used to forecast the future. This is particularly problematic when outcomes of past events are contaminated with (often unintentional) bias. Models often come under scrutiny only after they are built, trained and deployed. If a model is found to perpetuate a bias – for example, over-indexing for a particular race or gender – the data specialist returns to the development stage to identify and address the issue. This feedback loop is inefficient, costly and does not always mitigate harm; the time and energy of the data specialist is a sunk cost and, if in use, the model deployment may have already produced problematic outcomes. Some of these issues could be avoided by undertaking a thorough interrogation of data at the outset of model development. However, this is still not a widespread practice within AI model development efforts.

Figure 1.2 (A) Survey results about data analysis best practices in respondents' organisations and (B) Survey results about how respondents learned to analyse data



We conducted an anonymous online survey (see Figure 1.2), the results of which further lend credence to this problem. Although many (47%) respondents report conducting some form of data analysis prior to model development, most (74%) indicate that their organisations do not have explicit best practices for such analysis. Fifty-nine per cent of respondents reported relying primarily on experience and self-directed learning (through online tutorials, blogs, academic papers, Stack Overflow and online data competitions) to inform their data analysis methods and practices. This survey indicates that, despite limited current standards, there is widespread interest in improving data analysis practices and making them accessible.

To improve the accuracy and fairness of AI systems, it is imperative that data specialists can assess more quickly the viability and fitness of datasets and more easily find and use better-quality data to train their models. As a proposed solution, we introduce a dataset nutrition label, a diagnostic framework to address and mitigate some of these challenges by providing critical information to data specialists at the point of data analysis. The label thus acts as a first point of contact where decisions regarding the utility and fitness of specific datasets can be made. This is achieved by allowing the recognition of dataset inconsistencies and exclusions as well as promoting dataset interrogation as a crucial and inevitable procedure in the AI model development pipeline – with the ultimate goal of improving the overall quality of AI systems.

We begin with a review of related work, largely drawing from the fields of nutrition and privacy, where labels are a useful mechanism to distill essential information, enable better decision-making and influence best practices. We then discuss the dataset nutrition label prototype, our methodology, demonstration dataset and key results. This is followed by an overview of the benefits of the tool, its potential limitations and ways to mitigate those limitations. We then briefly summarise some future directions, including research and public policy agendas that would further advance the goals of the label. Lastly, we discuss

implementation of the prototype and key takeaways.

II. Labels in Context and Related Work

To inform the development of our prototype and concept, we surveyed the literature for labelling efforts. Labels and warnings are utilised effectively in product safety,[12] pharmaceuticals,[13] energy[14] and material safety.[15] We largely draw from the fields of nutrition, online privacy and algorithmic accountability as they are particularly salient for our purposes. The former is the canonical example and a long-standing practice subject to significant study while the latter provides valuable insights in the application of a 'nutrition label' in other domains, particularly in subjective contexts and where there is an absence of legal mandates and use is voluntary. Collectively, they elucidate the impacts of labels on audience engagement, education and user decision making.

In 1990, Congress passed the Nutrition Labeling and Education Act (P.L. 101–535), which includes a requirement that certain foodstuffs display a standardised 'Nutrition Facts' label.[16] By mandating the label, vital nutritional facts were communicated in the context of the 'Daily Value' benchmark and consumers could quickly assess nutrition information and more effectively abide by dietary recommendations at the moment of decision.[17] In the nearly three decades since its implementation, several studies have examined the efficacy of the now ubiquitous 'Nutrition Facts' label; these studies include analyses of how consumers use the label[18] and the effect it has had on the market.[19] Though some cast doubt on the benefits of the mandate in light of its cost,[20] most research concludes that the 'Nutrition Facts' label has had a positive impact.[21] Surveys demonstrate widespread consumer awareness of the label and its influence in decision making around food, despite a relatively short time since the passage of the Nutrition Labeling and Education Act.[22] According to the International Food Information Council, more than 80 per cent of consumers reported they looked at the 'Nutrition Facts' label when deciding what foods to purchase or consume and only 4 per cent reported never using the label.[23] Five years after the mandate, the Food Marketing Institute found that about one-third of consumers stopped buying a food because of what they read on the label.[24] With regard to the information contained on the label and consumer understanding, researchers found that 'label format and inclusion of (external) reference value information appear to have (positive) effects on consumer perceptions and evaluations',[25] but consumers indicated confusion about the 'Daily Value' comparison, suggesting that more information about the source and reliability of ground truth information would be useful.[26] The literature focuses primarily on the impact to consumers rather than on industry operations such as production and advertising. However, the significant impact of reported sales and marketing materials on consumers[27] provides a foundation for further inquiry into how this has affected the greater food industry.

In the field of privacy and privacy disclosures, the nutrition label serves as a useful point

of reference and inspiration.[28] Researchers at Carnegie Mellon and Microsoft created the 'Privacy Nutrition Label' to better surface essential privacy information to assist consumer decision making with regard to the collection, use and sharing of personal information.[29] The 'Privacy Nutrition Label' operates much like 'Nutrition Facts' and sits atop existing disclosures. It improves the functionality of the Platform for Privacy Notices, a machine-readable format developed by the World Wide Web Consortium, itself an effort to standardise and improve the legibility of privacy policies.[30] User surveys that tested the 'Privacy Nutrition Label' against alternative formats found that the label outperformed alternatives with 'significant positive effects on the accuracy and speed of information finding and reader enjoyment with privacy policies' as well as improved consumer understanding.[31]

Ranking and scoring algorithms also pose challenges in terms of their complexity, opacity and sensitivity to the influence of data. End users and even model developers face difficulty in interpreting an algorithm and its ranking outputs and this difficulty is further compounded when the model and the data on which it is trained is proprietary or otherwise confidential, as is often the case. 'Ranking Facts' is a web-based system that generates a 'nutrition label' for scoring and ranking algorithms based on factors or 'widgets' to communicate an algorithm's methodology or output.[32] Here, the label serves more as an interpretability tool than as a summary of information as the 'Nutrition Facts' and 'Privacy Nutrition Label' operate. The widgets work together, not modularly, to assess the algorithm on author-created categories of transparency, fairness, stability and diversity. The demonstration scenarios for using real datasets from college rankings, criminal risk assessment and financial services establish that the label is potentially applicable to a diverse range of domains. This lends credence to the potential utility in other fields as well, including the rapidly evolving field of AI.

More recently, in an effort to improve transparency, accountability and outcomes of AI systems, AI researchers have proposed methods for standardising practices and communicating information about the data itself.

The first draws from computer hardware and industry safety standards where datasheets are an industry-wide standard. In datasets, however, they are a novel concept. Datasheets are functionally comparable to the label concept and, like labels that by and large objectively surface empirical information, can often include other information such as recommended uses which are more subjective. 'Datasheets for Datasets', a proposal from researchers at Microsoft Research, Georgia Tech, University of Maryland and the AI Now Institute, seeks to standardise information about public datasets, commercial APIs and pretrained models. The proposed datasheet includes dataset provenance, key characteristics, relevant regulations and test results, but also significant yet more subjective information such as potential bias, strengths and weaknesses of the dataset, API, or model and suggested uses.[33] As domain experts, dataset, API and model creators would be responsible for creating the datasheets, not end users or other parties.

We are also aware of a forthcoming study from the field of natural language processing (NLP), 'Data Statements for NLP: Toward Mitigating System Bias and Enabling Better Science'.[34] The researchers seek to address ethics, exclusion and bias issues in NLP systems. Borrowing from similar practices in other fields of practice, the position paper puts forward

the concept and practice of ‘data statements’ which are qualitative summaries that provide detailed information and important context about the populations the datasets represent. The information contained in data statements can be used to surface potential mismatches between the populations used to train a system and the populations in planned use prior to deployment, to help diagnose sources of bias that are discovered in deployed systems and to help understand how experimental results might generalise. The authors suggest that data statements should eventually become required practice for system documentation and academic publications for NLP systems and should be extended to other data types (eg image data) albeit with tailored schema.

We take a different, yet complementary, approach. We hypothesise that the concept of a ‘nutrition label’ for datasets is an effective means to provide a scalable and efficient tool to improve the process of dataset interrogation and analysis prior to and during model development. In supporting our hypothesis, we created a prototype, a dataset nutrition label. Three goals drive this work. First, to inform and improve data specialists’ selection and interrogation of datasets and to prompt critical analysis. Consequently, data specialists are the primary intended audience. Second, to gain traction as a practical, readily deployable tool, we prioritise efficiency and flexibility. To that end, we do not suggest one specific approach to the label or charge one specific community with creating the label. Rather, our prototype is modular and the underlying framework is one that anyone can utilise. Lastly, we leverage probabilistic computing tools to surface potential corollaries, anomalies and proxies. This is particularly beneficial because resolving these issues requires excess development time and can lead to undesired correlations in trained models.

III. Methods

Some assumptions are made to focus our prototyping efforts. Only tabular data is considered. Additionally, we limit our explorations to datasets <10k rows. This allows for a narrower scope and deeper analysis. The label’s first contribution lies in the standard format it provides for metadata communication. This works to address weaknesses in the most common format for tabular data exchange: comma separated values, or the ‘.csv’ format. Despite its simple plain-text nature, portability and interoperability,[35] the lack of additional .csv metadata describing how data should be interpreted, validated and displayed is, perhaps, its biggest drawback. As early as 2015, the World Wide Web Consortium published recommendations on ‘Metadata Vocabulary for Tabular Data’ and ‘Access methods for CSV Metadata’.[36] However, the adoption of these recommendations within the data science community is not widespread. The label also builds on existing data science practices: directly following the acquisition of a dataset, most data specialists often enter an ‘exploratory phase’. This can be seen, for instance, on web-hosted machine learning competition platforms such as Kaggle and involves understanding dataset distributions through histograms and other basic statistics. The label attempts to provide these statistics ‘out of the box’ with the hopes of shortening model development lead times. The label also aims to provide insights from

advanced probabilistic modelling backends for more advanced users. While targeted mainly at a professional audience, many of the modules do not require expert training for interpretation and can thus be utilised in a public-facing version of the label.

Table 1.1 Seven modules of the label, together with their description, role, contents and attributes, highlighting the potential diversity of information included in a label

Module Name	Description	Contents	Module Characteristic – Level Required				
			Technical Expertise	Manual Effort	Subjectivity	Interactivity	Data Exposure
Metadata	Meta information. This module is the only required module. It represents the absolute minimum information to be presented	Filename, file format, URL, domain, keywords, type, dataset size, % of missing cells, licence, release date, collection range, description	Low	High	Low	Low	Low
Provenance	Information regarding the origin and lineage of the dataset	Source and author contact information with version history	Low	High	Low	Low	Low
Variables	Descriptions of each variable (column) in the dataset	Textual descriptions	Low	High	Medium	Low	Medium
Statistics	Simple statistics for all variables, in addition to stratifications into ordinal, nominal, continuous, and discrete	Least/most frequent entries, min/max, median, mean,.etc	Medium	Low	Low	Low	Medium
Pair Plots	Distributions and linear correlations between 2 chosen variables	Histograms and heatmaps	Medium	Low	Low	High	High
Probabilistic Model	Synthetic data generated using distribution hypotheses from which the data was drawn – leverages a probabilistic programming backend	Histograms and other statistical plots	High	Medium	High	Low	High
Ground Truth Correlations	Linear correlations between a chosen variable in the dataset and variables from other datasets considered to be "ground truth", such as Census Data	Heatmaps	Medium	Medium	Low	Low	High

A. Modular Architecture

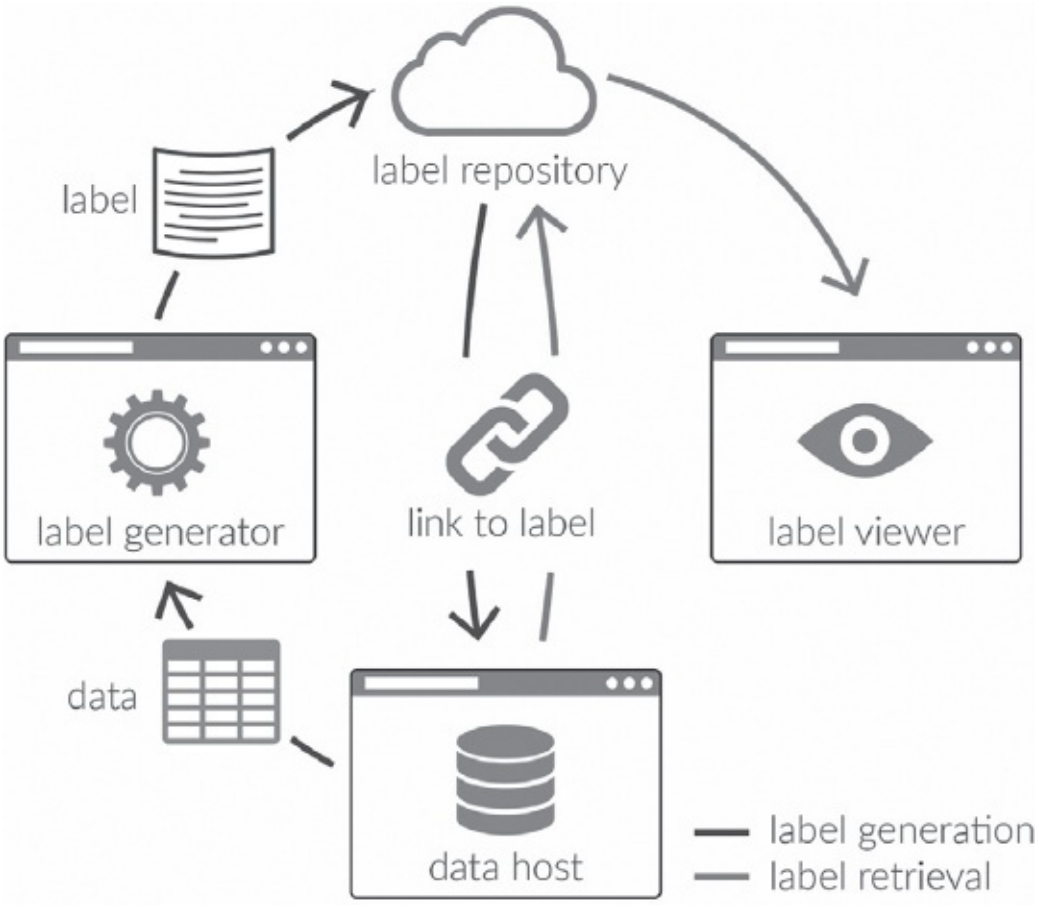
The label is designed in an extensible fashion with multiple distinct components that we refer to as 'modules' (see Table 1.1). The modules are stand-alone, allowing for greater flexibility as arrangements of different modules can be used for different types of datasets. This format also caters to a wide range of requirements and information available for a specific dataset. During label generation and subsequent updates, it also accommodates data specialists of different backgrounds and technical skill levels.

Modules (see Table 1.1) range from the purely non-technical, such as the Metadata module, to the highly technical, such as the Probabilistic Computing module. Some modules require manual effort to generate, such as those that provide qualitative descriptions of the data (Metadata, Provenance, Variables), while others can ideally be the result of an automated process (Statistics, Pair Plots). Modules also vary in their subjectivity, especially where there exists a reliance on the label author to identify which questions should be asked of the data and in what way (eg Probabilistic Computing). Many of the example modules are also interactive, highlighting a crucial benefit of a label living on a platform (such as a web page) that supports user interaction. This allows label users to interrogate various dataset

aspects with great flexibility and free of preconceived notions developed during label generation. Lastly, some modules could be designed to act as proxies for their corresponding dataset as they do not expose the underlying data. This could be key when dealing with proprietary datasets, as much of this data will not or cannot be released to the public based on intellectual property or other constraints. Other modules expose information such as distribution metrics which, in theory, would allow adversaries to approximate the dataset contents. The choice of module(s) is thus based on the availability of information, level of willingness and effort volunteered to document the dataset and privacy concerns.

The list of modules currently examined in this study, while not exhaustive, provides a solid representation of the kinds of flexibility supported by the label framework. Other modules considered for future iterations or additional datasets include but are not limited to: a comments section for users to interact with authors of the label for feedback or other purposes; an extension of the Provenance section that includes the versioning history and change logs of the dataset and associated labels over time, similar to Git; a privacy-focused module that indicates any sensitive information and whether the data was collected with consent; and finally, a usage tracking module that documents data utilisation and references using some form of identifier, similar to the Digital Object Identifier[37] and associated citation systems in scientific publishing.

Figure 1.3 Architecture of the proposed nutrition label ecosystem



B. Web-based Application

The label is envisioned as a digital object that can be both generated and viewed by web-based applications. The label ecosystem comprises two main components: a label maker and a label viewer (see Figure 1.3). Given a specific dataset, the label maker application allows users to select the desired modules and generate them. While the generation of some modules is fully automated, some require human input (see Table 1.1). For instance, the Metadata module mainly requires explicit input, while the Pair Plots module can be generated automatically from the dataset. The label generator pre-populates as many fields as possible and alerts users to those requiring action. The label itself lives in a .json format, as one that is human readable and well supported. The label can then be viewed within the label viewer application where formating is carried out to achieve the desired user interface and user interaction effects. In terms of visual appearance and design, format and typeface requirements of the 'Nutrition Facts' label[38] is used. These guidelines, such as the all black font color on white contrasting background, are optimised for clarity and conciseness. Design changes are anticipated in further iterations and should be informed by user testing.

Figure 1.4 Prototype label demonstrating the metadata, provenance and variables modules

Dataset Facts

ProPublica's Dollars for Docs Data

Metadata

Filename	201612v1-docdollars-product_payments
Format	csv
Url	https://projects.propublica.org/docdollars/
Domain	healthcare
Keywords	Physicians, drugs, medicine, pharmaceutical, transactions
Type	tabular
Rows	500
Columns	18
Missing	%
License	cc
Released	JAN 2017
Range	
From	AUG 2013
To	DEC 2015

Description This is the data used in ProPublica's Dollars for Docs news application. It is primarily based on CMS's Open Payments data, but we have added a few features. ProPublica has standardized drug, device and manufacturer names, and made a flattened table (product_payments) that allows for easier aggregating payments associated with each drug/device. In [1], one payment record can be attributed to up to five different drugs or medical devices. This table flattens the payments out so that each drug/device related to each payment gets its own line.

Provenance

Source

Name	U.S. Centers for Medicare & Medicaid Services
Url	https://www.cms.gov/OpenPayments/
Email	openpayments@cms.hhs.gov

Author

Name	Propublica
Url	https://www.propublica.org/datastore/
Email	data.store@propublica.org

Variables

Id A unique ID number for this payment & product combination. This is assigned by ProPublica for internal use

Applicable_manufacturer_or_applicable_gpo_making_payment_id ID of the applicable manufacturer or submitting applicable GPO making the payment or other transfer of value

Date_of_payment If a singular payment, then this is the actual date the payment was issued; if a series of payments or an aggregated set of payments, this is the date of the first payment to the covered recipient in this program

C. Backends

Simple statistical analyses involving the generation of histograms, distribution information and linear correlations are carried out directly in the browser, given tabular datasets of <100K rows. Server-side processing is thus reserved for more specialised and sophisticated analyses requiring additional computational power. Such processing could run multiple backends with the ultimate aim of providing the label authors with a diverse set of options, fueled by the plethora of tools developed by research groups for automating the generation of summaries, insights and understandings of datasets. The label thus becomes a medium for the continuous deployment and testing of these tools. A somewhat recent and particularly powerful example of this is probabilistic computing and specifically, BayesDB,[39] an open source platform developed by researchers at MIT. With minimal modeling and programming effort, BayesDB enables inference of a model that captures the structure underlying the data and generates statistical summaries based on such structure.

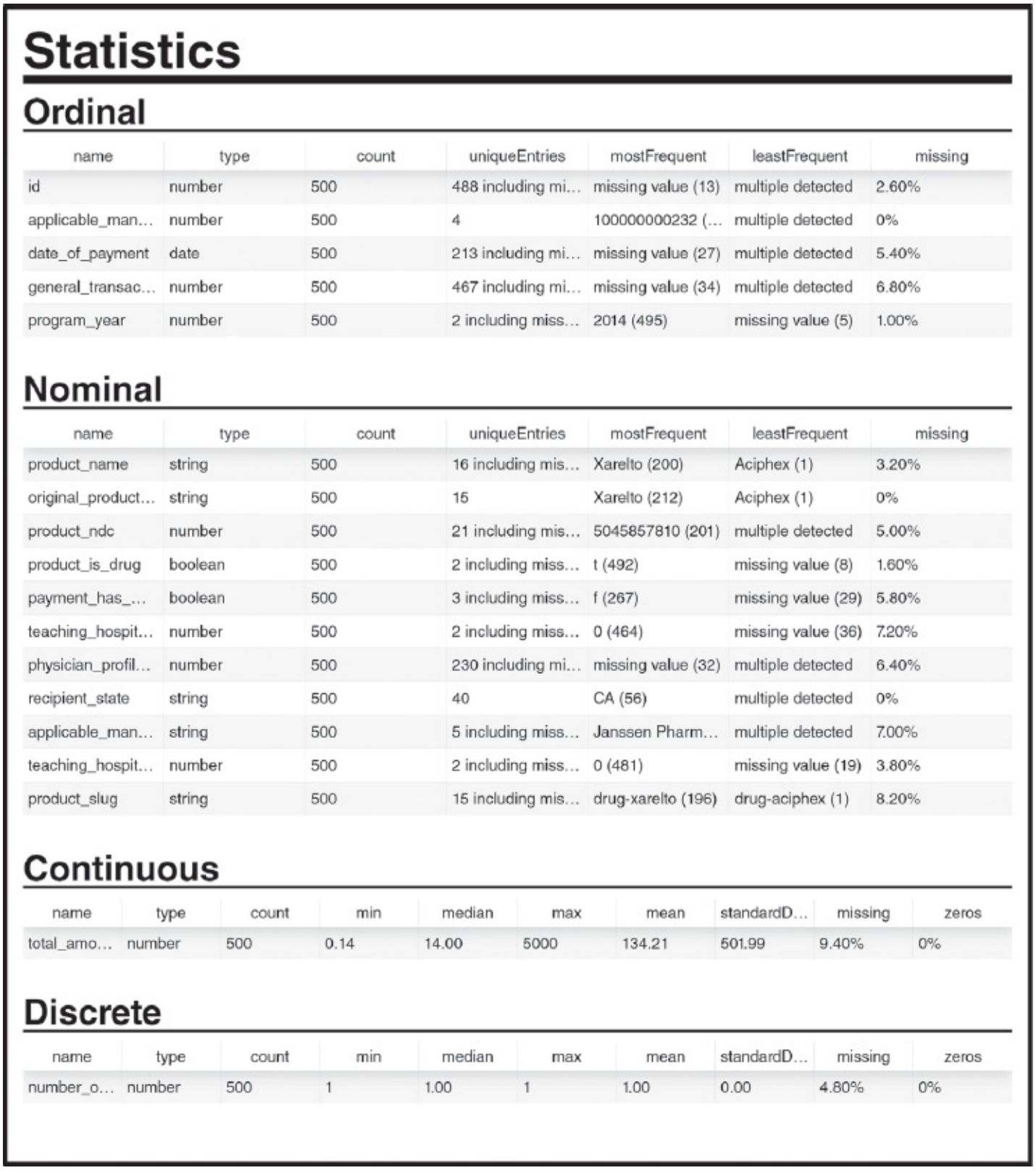
IV. Results

To test the concept generally and the modular framework specifically, we built a prototype with a dataset that included information about people and was maintained by an organisation invested in better understanding the data. This combination of factors provides necessary information and access to build a wide variety of modules, including those that require full knowledge of the data and the ability to contact the organisation that maintains the dataset. We were granted access to the 'Dollars for Docs' database from ProPublica, an independent, nonprofit newsroom that produces investigative journalism in the public interest.[40] The dataset, which contains payments to doctors and teaching hospitals from pharmaceutical and medical device companies over a two-year time period (August 2013–December 2015), was originally released by the US Centers for Medicare and Medicaid Services (CMS) and compiled by ProPublica into a single, comprehensive database.

The resulting prototype successfully demonstrates how disparate modules can be built on a specific dataset in order to highlight multiple, complementary facets of the data, ideally to be leveraged for further investigation by data specialists through the use of additional tools and strategies. The prototype label includes seven modules (see Table 1.1). The Metadata, Provenance and Variables modules (see Figure 1.4) provide as-is dataset information. They mirror information submitted by the label authors as well as provide a standard format for both the generation and consumption of such data. The Statistics module (see Figure 1.5) starts to offer a glimpse into the dataset distributions. For instance, the skewness of a 500-row dataset subset towards a particular drug 'Xarelto' can be quickly identified as the most frequent entry under the variable 'product name' and 'Aciphex' as the least frequent entry. The Pair Plot module (see Figure 1.6) starts to introduce interactivity into the label where the viewer is able to choose the variable pair being compared to one another. A specialist

building a model predicting marketing spend in each state, for example, may choose to compare ‘recipient_state’ and ‘total_amount_of_payment_USdollars’ and will observe that some states (CA, NY) are more highly correlated with spend. In this case, the specialist would probably normalise for population as the next step beyond consulting the label in order to identify anomalous spending trends.

Figure 1.5 Prototype label demonstrating the Statistics module, splitting the variables into four groups: ordinal, nominal, continuous and discrete



Statistics

Ordinal

name	type	count	uniqueEntries	mostFrequent	leastFrequent	missing
id	number	500	488 including mi…	missing value (13)	multiple detected	2.60%
applicable_man…	number	500	4	100000000232 (…	multiple detected	0%
date_of_payment	date	500	213 including mi…	missing value (27)	multiple detected	5.40%
general_transac…	number	500	467 including mi…	missing value (34)	multiple detected	6.80%
program_year	number	500	2 including miss…	2014 (495)	missing value (5)	1.00%

Nominal

name	type	count	uniqueEntries	mostFrequent	leastFrequent	missing
product_name	string	500	16 including mis…	Xarelto (200)	Aciphex (1)	3.20%
original_product…	string	500	15	Xarelto (212)	Aciphex (1)	0%
product_ndc	number	500	21 including mis…	5045857810 (201)	multiple detected	5.00%
product_is_drug	boolean	500	2 including miss…	t (492)	missing value (8)	1.60%
payment_has_…	boolean	500	3 including miss…	f (267)	missing value (29)	5.80%
teaching_hospit…	number	500	2 including miss…	0 (464)	missing value (36)	7.20%
physician_profil…	number	500	230 including mi…	missing value (32)	multiple detected	6.40%
recipient_state	string	500	40	CA (56)	multiple detected	0%
applicable_man…	string	500	5 including miss…	Janssen Pharm…	multiple detected	7.00%
teaching_hospit…	number	500	2 including miss…	0 (481)	missing value (19)	3.80%
product_slug	string	500	15 including mis…	drug-xarelto (196)	drug-aciphex (1)	8.20%

Continuous

name	type	count	min	median	max	mean	standardD…	missing	zeros
total_amo…	number	500	0.14	14.00	5000	134.21	501.99	9.40%	0%

Discrete

name	type	count	min	median	max	mean	standardD…	missing	zeros
number_o…	number	500	1	1.00	1	1.00	0.00	4.80%	0%

Figure 1.6 Prototype label demonstrating the Pair Plot module and highlighting the interactive dropdown menus for selecting variables

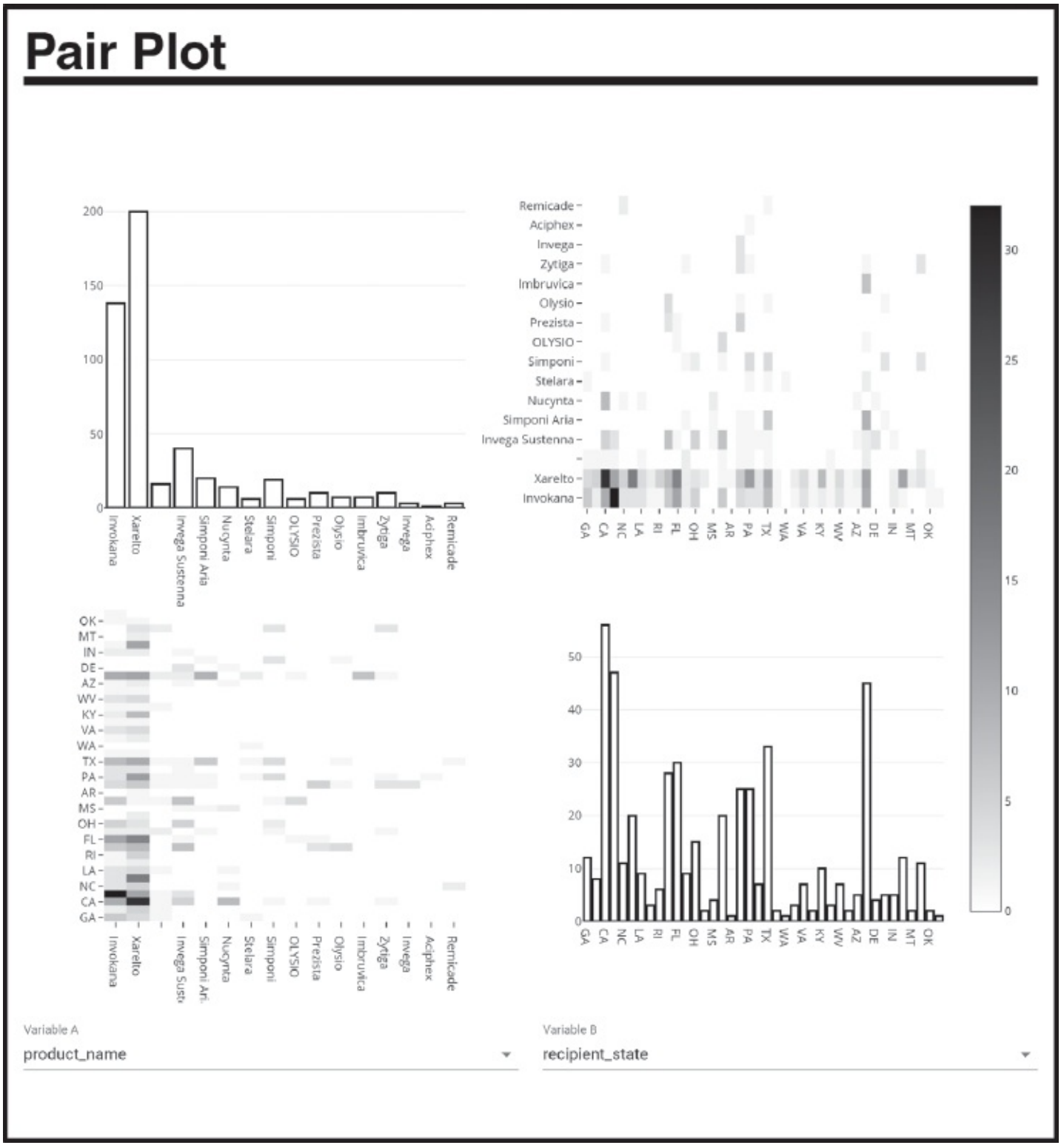
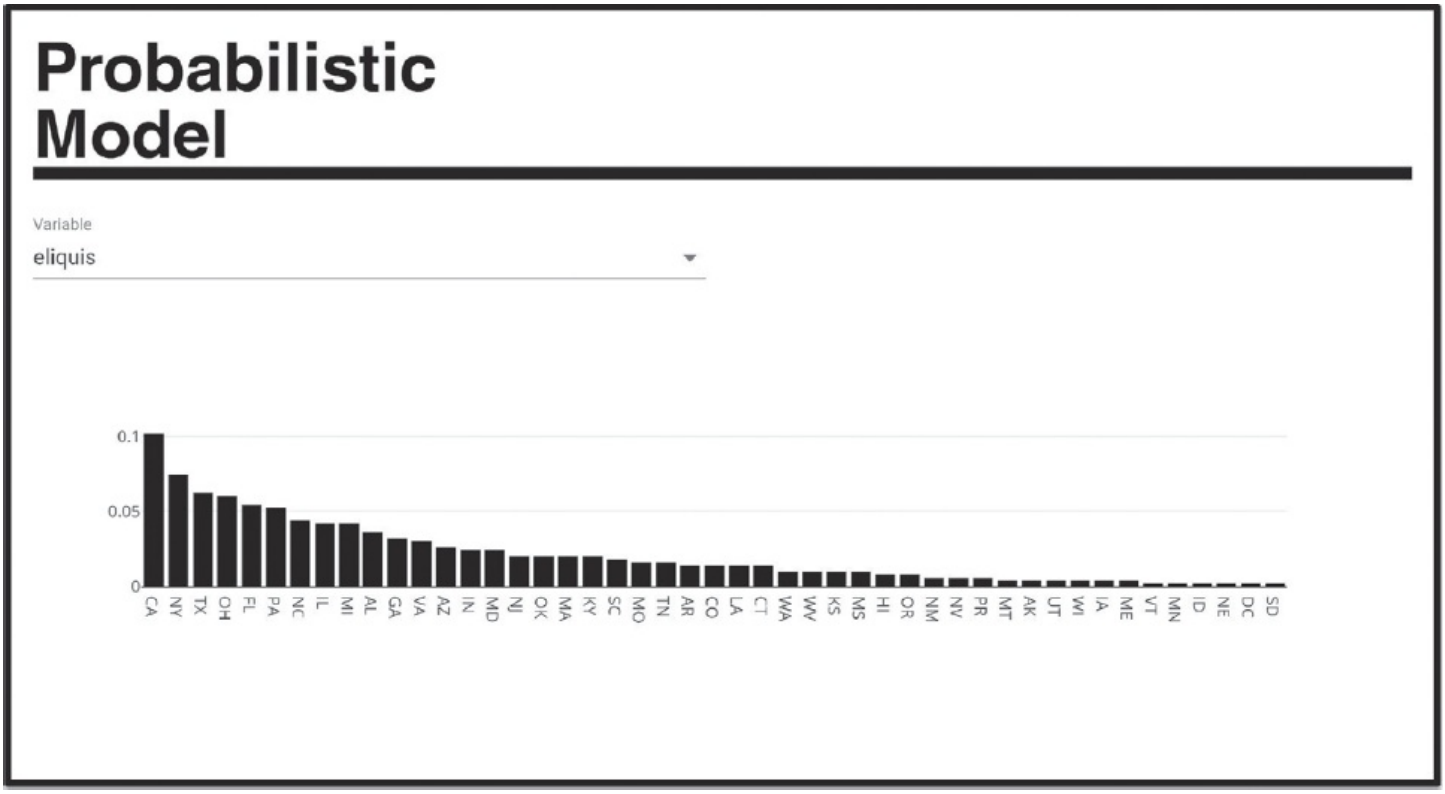


Figure 1.7 Prototype label demonstrating the Probabilistic Model module and showcasing a hypothetical distribution for payments made towards the drug ‘Eliquis’ across different states

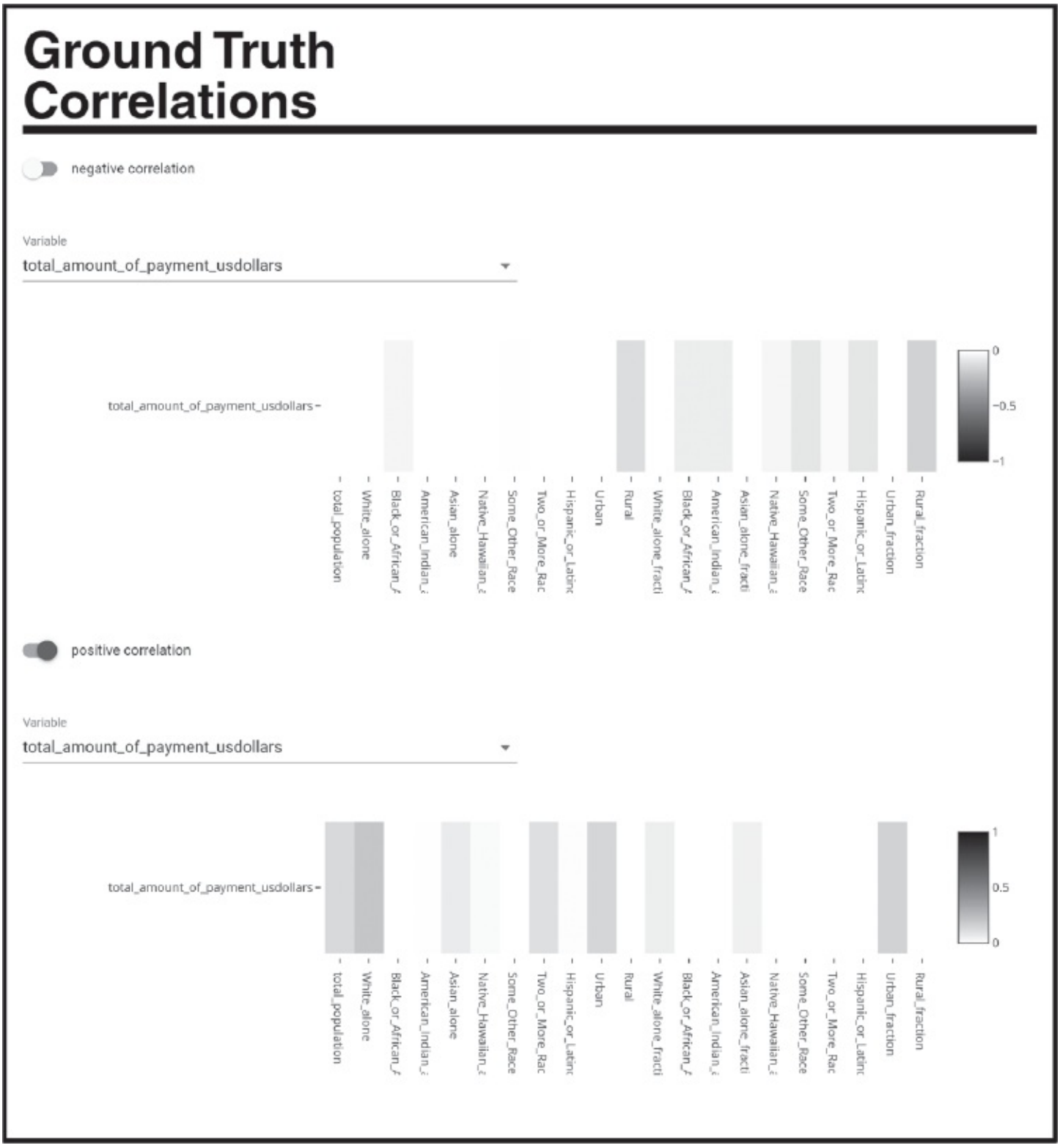


While all modules thus far investigate the dataset itself, the Probabilistic Model module (see Figure 1.7) attempts to generate synthetic data by utilising the aforementioned BayesDB backend. Computed from an inferred generative model, this module allows for the full benefits of Bayesian analysis,[41] such as interpretability of inferences, coping with missing data and robustness to outliers and regions of sparse data. In this specific use case, an underrepresented drug is chosen from the dataset and the probability of this drug receiving a payment in different states is inferred. With the inevitable variation in the representation of different groups in datasets, such analyses are of great utility in extracting insights – even from relatively small sample sizes. A quick toggle indicates that the top few states for marketing spend are likely the same few states – with a few exceptions, including that New Jersey is likely to receive a lot more money for marketing activities relating to the drug Xarelto. Again, this information only acts as a flag for the 'what'; specialists will ideally continue to investigate the data in order to identify the 'why'.

It is unavoidable that datasets collected from the real world have relationships to demographics that the data specialist or other entities do not wish to propagate into the learned model and the inferences produced from it. For example, is a variable or an aggregate of a variable strongly correlated with the Hispanic population in a given region? To surface relationships like this, it is often necessary to explicitly compute a comparison between the dataset and demographic 'ground truth' data, which is a task that can be both time consuming and challenging. The Ground Truth Correlation module (see Figure 1.8) provides the data specialist initial evidence as to whether such relationships are likely, thus warranting further analysis. In order to surface any anomalies in the demographic distribution of these variables, we selected the 2010 US Census data as 'ground truth' for zip code and race. The module then correlates zip code Census data with the dataset and calculates the Pearson correlation

between demographics and field aggregates. To demonstrate its utility, the label (see Figure 1.8 top) highlights the negative correlations between the (sum of the) amount of payment field and demographics. A second example (see Figure 1.8 bottom), highlights the positive correlation between a ‘spend_per_person’ aggregate and demographics. This module demonstrates, in a straightforward way, specific anomalous relationships in the data that the data specialist should pay attention to during model training. In the prototype, we observe a slight positive correlation between white zip codes and payments and a slight negative correlation between rural zip codes and payments. Toggling to per person spend underscores similar overall trends.

Figure 1.8 The negative (top) and positive (bottom) correlations to demographics produced by the Ground Truth Correlations module



V. Discussion

The label offers many benefits. Overall, it prompts critical questions and interrogation in the preprocessing phase of model development. It also expedites decision making, which saves time in the overall model development phase without sacrificing the quality or thoroughness

of the data interrogation itself, perhaps encouraging better practices at scale. These benefits apply across the spectrum of data specialists' skill and experience but are particularly useful for those new to the field or less attuned to concerns around bias and algorithmic accountability. First, the label creates a pre-generated 'floor' for basic data interrogation in the data selection phase. It also indicates key dataset attributes in a standardised format. This gives data specialists a distilled yet comprehensive overview of the 'ingredients' of the dataset, which allows for a quick and effective comparison of multiple datasets before committing to one for further investigation. It also enables the data specialist to better understand and ascertain the fitness of a dataset by scanning missing values, summary statistics of the data, correlations or proxies and other important factors. As a result, the data specialist may discard a problematic dataset or work to improve its viability prior to utilising it.

Improved dataset selection affords a secondary benefit: higher quality models. The label provides data specialists improved means by which to interrogate the selected dataset during model development, previously a costly and onerous enterprise. The Ground Truth Correlation module, in particular, provides a helpful point of reference for the data specialist before model completion and surfaces issues such as surprising variable correlations, missing data, anomalous data distributions, or other factors that could reinforce or perpetuate bias in the dataset. Addressing these factors in the model creation and training phase saves cost, time and effort and could also prevent bad outcomes early on, rather than addressing them after the fact.

The label is built with scalability in mind and with an eye towards standardisation. The modular framework provides flexibility for dataset authors and publishers to identify the 'right' kind and amount of information to include in a label; over time, this could become a set of domain-specific best practices. The interactivity of the label also permits flexibility, as insights about the dataset may arise over time. For example, the ground truth data used for comparison could evolve, rendering a previously unsuitable dataset suitable. Interactive labels also give data specialists the ability to dive further into anomalous data, rather than simply accepting static information provided by the label author. With some modules more subjective in nature and with a range of domain expertise across data specialists, this is particularly important. For advanced data specialists, the flexible label backend makes it easy to 'plug-in' more complex engines. Such complex backends can provide different statistical tools; for example, the Probabilistic Computing module makes it possible to investigate low frequency variables by generating synthetic data. Synthetic data gives data specialists the ability to address incomplete data and opens a potential path to privacy preserving data usage.[42]

Lastly, the label functioning as a proxy for the dataset itself is an intriguing, even if distant, possibility. Increased calls for accountability of AI systems demand investigation of datasets used in training models, but disclosing those datasets, even to a limited audience, may pose risks to privacy, security and intellectual property that calls this approach into question. If the label is able to convey the information essential for accountability in the dataset without disclosing the data itself, it would provide a valuable and much-needed auditing tool[43] for AI systems while still preserving privacy, security and proprietary

information.

A. Limitations and Mitigations

There are challenges to our approach. The extensive variety of datasets used to build models raises important questions around whether the label can generalise across data and dataset type, size, composition and in different domains and furthermore, whether a data specialist or domain expert will need to be involved in the creation of a label across these different datasets. This could arise in an instance where important semantic information is atypically labeled and would be challenging to interpret automatically, such as if the field for zip code in a dataset had a custom field for ‘geographic area’. A data specialist or domain expert may also be required when building a label for sensitive or proprietary data, which may be accessible only to those who built the dataset and not accessible to the public. Building the label as a modular system somewhat mitigates the complication of requiring input from a domain expert, as the framework can adapt to domain-specific best practices and can easily support the generation of different types of labels based on access. Within the Provenance module, it may be necessary or helpful to surface who made the label and what relationship they have to the dataset.

The veracity and usefulness of the Ground Truth Comparison module depends on the accuracy of the ‘ground Truth’ dataset, which serves as a benchmark standard and is considered objective, accurate and provable and with clear provenance. However, problematic ground truth data may lead to futile or even harmful comparisons. Without a realistic way to eliminate bias in all datasets, a mitigating step is to build labels for ground truth datasets themselves. If these labels include community feedback and comment modules, dataset authors can address the issues directly.

Further investigation is necessary to understand the feasibility and desirability of using the label as a proxy for proprietary datasets. This would likely require that the dataset creator or controller create the label. Another challenge is that the label might not prompt the right questions or reactions for the data specialist, leaving certain biased data undetected. Analyses of machine bias indicate that zip codes often proxy for race, but many others proxies still exist, especially as the models themselves approach levels of complexity that are difficult or impossible for humans to comprehend and new or unexpected proxies emerge. Integrating new methods or tools to help identify proxies will be important to the industry and our hope is that the label will be flexible in such a way that these tools can be leveraged to create additional modules as they become available.

Finally, design of the label itself will require additional attention to determine the appropriate amount of information for presentation, comprehension and adoption. As made clear in the work on Privacy Nutrition Label,[44] design is a key element in the efficacy of the label. It is worth investigating and testing the most effective presentation to drive adoption.

VI. Future Directions

This paper and prototype are the first step toward bringing together a wide range of data specialists, from those creating and publishing datasets to those utilising datasets to build models, in order to improve the quality of datasets used in AI-generated models.

Deeper research and iteration will be necessary as we continue to build additional prototypes of the label. Creating a ‘nutrition label’ for datasets is nascent and requires additional investigations about what information (in the form of modules or otherwise) is useful and practical to include. Based on the relatively small reach of our survey, we also recommend that a more rigorous survey be conducted to more accurately identify needs, as the survey we administered was limited in its reach and disproportionately indexed to American and European respondents working in the private sector. The information pertinent to a data specialist will also shift based on the domain of the data, necessitating the building of additional prototypes for different kinds of datasets. The opportunities afforded by complex machine learning tools such as BayesDB in the creation of additional modules deserve more fulsome exploration to maximise the usability and usefulness of the label.

Through building relationships with dataset publishers and circulating the label, we hope to identify not only additional datasets for prototypes, but also to launch our label on open datasets so that we can study the impact of the label on the use of and conversation around the data. We will consider collaborations with colleagues from industry and academia to further drive this work, building knowledge around the impediments to adoption and considering ways that regulatory frameworks could further support the creation of a best practice or standard.

In terms of the label ecosystem, the existence of a label for any given dataset could be notated using a mark or symbol, such as the ‘Conformité Européenne’ (CE) mark used by the European Union,[45] on the author’s or dataset host’s webpage. Clicking on the mark would then navigate to the label viewer application and fetch the corresponding label from a central repository where all labels are hosted. Such a centralised archive of labels would allow for generating usage statistics, least and most used modules and eventually help inform future label iterations. More importantly, a repository of this sort could act as an index of datasets without hosting the datasets themselves. For instance, API calls to such a repository could help locate datasets with queries like ‘MIT license dataset for facial recognition with >100k samples’.

Beyond its utility as a tool, the label could also drive a change in norms. Through using the label, data specialists will build a habit around questioning datasets through analysis and interrogation techniques, even if a particular dataset does not include a label. In time, the label will facilitate an environment that encourages a broad spectrum of dataset creators, cleaners, publishers and users to create labels to publish alongside their datasets. This would lead to better identification of issues with data and bias, or inappropriate data collection practices, which in turn would increase data and dataset quality overall.

Looking beyond the label itself, there are longer term opportunities for this framework and the data science community. Decisions made around the authorship and ownership model for the label will be critical to the overall direction of the project; who will create these labels going forward and who will maintain them? Will there be a single place where all labels live or from where they are all linked? Additional future directions could include: building a

public consortium or governing body to consider standards across the industry; creating curriculum for those collecting and working with datasets; and further exploration of appropriate ground truth data.

VII. Conclusions

In an effort to improve the current state of practice of data analysis, we created the dataset nutrition label, a diagnostic framework that provides a concise yet robust and standardised view of the core components of a dataset. We use the ProPublica Dollars for Docs dataset to create the label prototype.

The label serves as a proof of concept for several conceptual questions, beginning with the general feasibility of an extensible and diverse modular framework. It also confirms the possibility of mixing qualitative and quantitative modules that leverage different statistical and probabilistic modelling backend technologies in the same overall user experience. The label integrates both static and interactive modules, underscoring the importance of using an interactive platform (such as a website) for the distribution of the label itself. Together, this promises flexibility, scalability and adaptability.

With the label, data specialists can efficiently compare, select and interrogate datasets. Additionally, certain modules afford the ability to check for issues with the dataset before and during model development, surface anomalies and potentially dangerous proxies and find new insights into the data at hand. As a result, data specialists have a better, more efficient process of data interrogation, which will produce higher quality AI models. The label is a useful, practical, timely and necessary intervention in the development of AI models and a first step in a broader effort toward improving the outcomes of AI systems that play an increasingly central role in our lives.

Acknowledgements

We are grateful to the ProPublica team, including Celeste LeCompte, Ryann Jones, Scott Klein and Hannah Fresques, for their generosity in providing the Dollars for Docs dataset and for their assistance throughout prototype development. We are also grateful to the BayesDB team in the Probabilistic Computing Group at MIT, including Vikash Mansinghka, Sara Rendtorff-Smith and Ulrich Schaechtle for their valuable time, assistance and ongoing advice with regard to integrating the BayesDB backend with the label. Thanks also go to Patrick Gage Kelley for bringing key work to our attention and for his constructive feedback, as well as the 2018 Assembly Cohort and Advisory Board, in particular Matt Taylor, Jack Clark, Rachel Kalmar, Kathy Pham, James Mickens, Andy Ellis and Nathan Freitas; the City of Boston Office of New Urban Mechanics; and Eric Breck and Mahima Pushkarna of Google Brain for productive and insightful discussions. This work was made possible by the

Assembly programme led by Jonathan Zittrain of the Berkman Klein Center for Internet & Society and Joi Ito of the MIT Media Lab.

References

Balasubramanian SK and Cole C, 'Consumers' Search and Use of Nutrition Information: The Challenge and Promise of the Nutrition Labeling and Education Act' (2002) 66 *Journal of Marketing* 112.

Berger JO, Statistical Decision Theory and Bayesian Analysis (Springer Science & Business Media 2013).

Bolukbasi T and others, 'Man Is to Computer Programmer as Woman Is to Homemaker? Debiasing Word Embeddings', Advances in Neural Information Processing Systems (2016).

Borra S, 'Consumer Perspectives on Food Labels' (2006) 83 *The American Journal of Clinical Nutrition* 1235S.

Buolamwini J and Gebru T, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' in Sorelle A Friedler and Christo Wilson (eds), *Proceedings of the 1st Conference on Fairness, Accountability and Transparency* (PMLR 2018).

Burton S, Biswas A and Netemeyer R, 'Effects of Alternative Nutrition Label Formats and Nutrition Reference Information on Consumer Perceptions, Comprehension and Product Evaluations' (1994) 13 *Journal of Public Policy & Marketing* 36.

Chandrakar R, 'Digital Object Identifier System: An Overview' (2006) 24 *The Electronic Library* 445.

Ciocchetti CA, 'The Future of Privacy Policies: A Privacy Nutrition Label Filled with Fair Information Practices' (2008) 26 *The John Marshall Journal of Computer and Information Law* 1.

Davenport TH and Harris JG, 'Automated Decision Making Comes of Age' (2005) 46 *MIT Sloan Management Review* 83.

Drichoutis AC, Lazaridis P and Nayga RM Jr, 'Consumers' Use of Nutritional Labels: A Review of Research Studies and Issues' (2006) 2006 *Academy of Marketing Science Review* 1.

Gebru T and others, 'Datasheets for Datasets' (2018). Available at: http://arxiv.org/abs/1803.09010.

Guthrie JF and others, 'Who Uses Nutrition Labeling and What Effects Does Label Use Have on Diet Quality?' (1995) 27 *Journal of Nutrition Education* 163.

Hanson D, CE Marking, Product Standards and World Trade (Edward Elgar Publishing 2005).

Hunt A and Thomas D, *The Pragmatic Programmer: From Journeyman to Master* (Addison-Wesley Professional 2000).

Kelley PG and others, 'A Nutrition Label for Privacy', Proceedings of the 5th Symposium on Usable Privacy and Security (Association for Computer Machinery 2009).

——, 'Standardising Privacy Notices: An Online Study of the Nutrition Label Approach', Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (Association for Computer Machinery 2010)

Mansinghka V and others, 'Bayes DB: A Probabilistic Programming System for Querying the Probable Implications of Data' (2015). Available at: http://arxiv.org/abs/1512.05006.

McClure FD and United States Food and Drug Administration, 'FDA Nutrition Labeling Manual: A Guide for Developing and Using Databases' (US Food and Drug Administration 1993).

'Metadata Vocabulary for Tabular Data'. Available at: www.w3.org/TR/tabular-metadata/ (last accessed 17 April 2018).

'Model for Tabular Data and Metadata on the Web'. Available at: www.w3.org/TR/tabular-data-model/ (last accessed 17 April 2018).

n/a, 'Data Statements for NLP: Toward Mitigating System Bias and Enabling Better Science'

Petruccelli PJ, 'Consumer and Marketing Implications of Information Provision: The Case of the Nutrition Labeling and Education Act of 1990' (1996) 15 *Journal of Public Policy & Marketing* 150.

Safety O, Administration H and Others, 'Hazard Communication Standard: Safety Data Sheets' [2012] OSHA Brief.

Select Committee on Artificial Intelligence, 'AI in the UK: Ready, Willing and Able?' (House of Lords). Available at: https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf.

Silverglade BA, 'The Nutrition Labeling and Education Act: Progress to Date and Challenges for the Future' (1996) 15 *Journal of Public Policy & Marketing* 148.

Surendra H MHS, 'A Review of Synthetic Data Generation Methods for Privacy Preserving Data Publishing' (2017) 6(3) *International Journal of Scientific and Technology Research* 95–101. Available at: www.ijstr.org/final-print/mar2017/A-Review-Of-Synthetic-Data-Generation-Methods-For-Privacy-Preserving-Data-Publishing.pdf.

Teisl MF, Levy AS and Others, 'Does Nutrition Labeling Lead to Healthier Eating?' (1997) 28 *Journal of Food Distribution*

Research 18.
Union E, 'Directive 2009/28/EC of the European Parliament and of the Council of 23 April 2009 on the Promotion of the Use of Energy from Renewable Sources and Amending and Subsequently Repealing Directives 2001/77/EC and 2003/30/EC' (2009) 5 *Official Journal of the European Union* 2009.
United States. Congress. House. Committee on Energy and Commerce, Nutrition Labeling and Education Act of 1990: Report (to Accompany HR 3562) (including Cost Estimate of the Congressional Budget Office) (Washington DC: US Government Printing Office 1990).
US Consumer Product Safety Commission. Office of the General Counsel, Compilation of Statutes Administered by CPSC (Bethsada, MD: US Consumer Product Safety Commission 1998).
US Food Administration and Others, 'A Food Labeling Guide' [1999] Center for Food Safety and Applied Nutrition.
Yang K and others, 'A Nutritional Label for Rankings'. Available at: www.cs.drexel.edu/~julia/documents/cr-sigmod-demo-2018.pdf.

---

[1] Assembly, MIT Media Lab and Berkman Klein Center at Harvard University.

[2] Dana-Farber Cancer Institute, Harvard Medical Institute.

[3] metaLAB @ Harvard, Berkman Klein Center for Internet & Society, Harvard University.

[4] MIT Quest for Intelligence.

[5] Assembly, MIT Media Lab and Berkman Klein Center at Harvard University.

[6] Available at: https://datanutrition.media.mit.edu/.

[7] Available at: https://ahmedhosny.github.io/datanutrition/.

[8] The term 'data specialist' is used instead of 'data scientist' in the interest of using a term that is broadly scoped to include all professionals utilising data in automated decision-making systems: data scientists, analysts, machine learning engineers, model developers, artificial intelligence researchers and a variety of others in this space.

[9] Thomas H Davenport and Jeanne G Harris, 'Automated Decision Making Comes of Age' (2005) 46 *MIT Sloan Management Review* 83.

[10] Tolga Bolukbasi and others, 'Man Is to Computer Programmer as Woman Is to Homemaker? Debiasing Word Embeddings', Advances in Neural Information Processing Systems (2016).

[11] Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' in Sorelle A Friedler and Christo Wilson (eds), *Proceedings of the 1st Conference on Fairness, Accountability and Transparency* (PMLR 2018).

[12] US Consumer Product Safety Commission. Office of the General Counsel, *Compilation of Statutes Administered by CPSC* (US Consumer Product Safety Commission 1998).

[13] Foster D McClure and United States. *Food and Drug Administration, FDA Nutrition Labeling Manual: A Guide for Developing and Using Databases* (US Food and Drug Administration 1993).

[14] Europäische Union, 'Directive 2009/28/EC of the European Parliament and of the Council of 23 April 2009 on the Promotion of the Use of Energy from Renewable Sources and Amending and Subsequently Repealing Directives 2001/77/EC and 2003/30/EC' (2009) 5 *Official Journal of the European Union* 2009.

[15] Occupational Safety, Health Administration and Others, 'Hazard Communication Standard: Safety Data Sheets' [2012] OSHA Brief.

[16] United States. Congress. House. Committee on Energy and Commerce, *Nutrition Labeling and Education Act of 1990: Report (to Accompany H.R. 3562) (including Cost Estimate of the Congressional Budget Office)* (US Government Printing Office 1990).

[17] Ibid; Siva K Balasubramanian and Catherine Cole, 'Consumers' Search and Use of Nutrition Information: The Challenge and Promise of the Nutrition Labeling and Education Act' (2002) 66 *Journal of Marketing* 112; Joanne F Guthrie and others, 'Who Uses Nutrition Labeling and What Effects Does Label Use Have on Diet Quality?' (1995) 27 *Journal of Nutrition Education* 163.

[18] Balasubramanian and Cole (n 17); Guthrie and others (n 17).

[19] Bruce A Silverglade, 'The Nutrition Labeling and Education Act: Progress to Date and Challenges for the Future' (1996) 15 *Journal of Public Policy & Marketing* 148.

[20] Paul J Petruccelli, 'Consumer and Marketing Implications of Information Provision: The Case of the Nutrition Labeling and Education Act of 1990' (1996) 15 *Journal of Public Policy & Marketing* 150.

[21] Mario F Teisl, Alan S Levy and Others, 'Does Nutrition Labeling Lead to Healthier Eating?' (1997) 28 *Journal of Food Distribution Research* 18; Andreas C Drichoutis, Panagiotis Lazaridis and Rodolfo M Nayga Jr, 'Consumers' Use of Nutritional Labels: A Review of Research Studies and Issues' (2006) *Academy of Marketing Science Review* 1.

[22] United States Congress. House Committee on Energy and Commerce (n 16).

[23] Susan Borra, 'Consumer Perspectives on Food Labels' (2006) 83 *The American Journal of Clinical Nutrition* 1235S.

[24] United States Congress. House Committee on Energy and Commerce (n 16).

[25] Scot Burton, Abhijit Biswas and Richard Netemeyer, 'Effects of Alternative Nutrition Label Formats and Nutrition Reference Information on Consumer Perceptions, Comprehension and Product Evaluations' (1994) 13 *Journal of Public Policy & Marketing* 36.

[26] Borra (n 22).

[27] Silverglade (n 19).

[28] Corey A Ciocchetti, 'The Future of Privacy Policies: A Privacy Nutrition Label Filled with Fair Information Practices' (2008) 26 *The John Marshall Journal of Computer & Information Law* 1.

[29] Patrick Gage Kelley and others, 'A Nutrition Label for Privacy', *Proceedings of the 5th Symposium on Usable Privacy and Security* (Association for Computer Machinery (ACM) 2009).

[30] Patrick Gage Kelley and others, 'Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach', *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (ACM2010).

[31] Kelley and others (n 29); Kelley and others (n 30).

[32] Ke Yang and others, 'A Nutritional Label for Rankings'. Available at: www.cs.drexel.edu/~julia/documents/cr-sigmod-demo-2018.pdf.

[33] Timnit Gebru and others, 'Datasheets for Datasets' (2018). Available at: http://arxiv.org/abs/1803.09010.

[34] n/a, 'Data Statements for NLP: Toward Mitigating System Bias and Enabling Better Science'.

[35] Andrew Hunt and David Thomas, *The Pragmatic Programmer: From Journeyman to Master* (Boston: Addison-Wesley Professional 2000).

[36] 'Metadata Vocabulary for Tabular Data'. Available at: www.w3.org/TR/tabular-metadata/ (last accessed 17 April 2018); 'Model for Tabular Data and Metadata on the Web'. Available at: www.w3.org/TR/tabular-data-model/ (last accessed 17 April 2018).

[37] Rajesh Chandrakar, 'Digital Object Identifier System: An Overview' (2006) 24 *The Electronic Library* 445.

[38] US Food, Drug Administration and Others, 'A Food Labeling Guide' (Center for Food Safety & Applied Nutrition, 1999).

[39] Vikash Mansinghka and others, 'BayesDB: A Probabilistic Programming System for Querying the Probable Implications of Data' (2015). Available at: http://arxiv.org/abs/1512.05006.

[40] Available at: https://projects.propublica.org/docdollars/.

[41] James O Berger, *Statistical Decision Theory and Bayesian Analysis* (Springer Science & Business Media 2013).

[42] Mohan HS Surendra H, 'A Review of Synthetic Data Generation Methods For Privacy Preserving Data Publishing' (2017) 6 *International Journal of Scientific & Technology Research* 95–101. Available at: www.ijstr.org/final-print/mar2017/A-Review-Of-Synthetic-Data-Generation-Methods-For-Privacy-Preserving-Data-Publishing.pdf.

[43] Select Committee on Artificial Intelligence, 'AI in the UK: Ready, Willing and Able?' Available at: https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf.

[44] Kelley and others (n 29).

[45] David Hanson, *CE Marking, Product Standards and World Trade* (Edward Elgar Publishing 2005).

2

A Right to a Rule

On the Substance and Essence of the Fundamental Right to Personal Data Protection

LORENZO DALLA CORTE[1]

Abstract

In the European multilevel fundamental rights system, the right to personal data protection, enshrined in Article 8 of the EU Charter of Fundamental Rights, is formally distinct from the right to privacy, which is hallowed in its Article 7. From a substantive perspective, however, the dichotomy between the right to privacy and data protection is not as clean cut. Data protection is logically and historically entwined with privacy and disentangling their substance has proven to be a daunting task. Data protection is also a relatively young right and had a *sui generis* emergence within the EU (quasi)constitutional framework, which contributes to the blurriness of its distinction from the right to privacy and of its core components and very essence. Indeed, there is not a univocal and authoritative conception of what the fundamental right to data protection entails and the relevant doctrine and jurisprudence is highly discordant.

This chapter seeks to put forth a consistent interpretation of the EU right to data protection's substance and essence. It is grounded in an historical, doctrinal and jurisprudential analysis of the right to data protection and of the elements that make it distinct from privacy. Its purpose is to contribute to the doctrinal debate which still surrounds data protection and its blurry boundaries with the right to privacy. This chapter holds that data protection is evolving away from privacy into something entirely distinct, albeit still connected to it. EU data protection has become a procedural, auxiliary, *sui generis* fundamental right, which has emerged as a response to technological developments and to the growing importance of secondary data protection legislation and which embodies a collective stance towards how personal data processing has been shaping the modern world.

The chapter contends that data protection has become a sort of 'right to a rule', by now more akin to due process than to privacy or to informational self-determination. The most coherent reading of data protection's rationale is given by the democratic will of regulating the processing of personal data by virtue of its sheer importance for the functioning of contemporary society and of the inherent power asymmetry running between data controllers and data subjects. The chapter also maintains that there is an essence of the right to personal

data protection and that such essence is not to be directly sought in the list of rights and principles that can be derived from primary and secondary data protection legislation, but rather, *a contrario*, from the kinds of infringement that threaten the functioning of such a system of checks and balances as a whole.

Keywords

Data protection, privacy, fundamental rights.

I. Introduction

EU personal data protection is quite young, and its emergence as a standalone right a relatively recent phenomenon within the European legal framework. The rise of data protection to the status of fundamental right has also been quite peculiar: data protection is a *sui generis*[2] fundamental right in that its content derives from preceding legislation that regulated personal data processing at a national, international and Union level. Seminal national legislation, several international instruments and EU secondary regulation chronologically preceded data protection's formal emergence as an individual fundamental right. Before the Charter of Fundamental Rights of the European Union[3] (CFR or Charter) data protection was often framed as a facet of the right to privacy, or as an intermediary tool aiming at the protection of overlying rights, such as self-determination and human dignity. The issue is that, to this day, there is not a univocal, authoritative conception of what constitutes the right to data protection, nor of its essence and rationale. The lack of a common understanding of what data protection *is*, and the fact that it is still often conflated with privacy, can hamper the further development of the right to personal data protection *ex* Article 8 CFR.[4] A debate on the rationale and essence of personal data protection is thus needed: the right, as it has been pointed out, is currently still 'in flux'.[5]

This chapter offers a modern interpretation of the rationale and essence of the right to personal data protection. It is grounded in an historical, doctrinal and jurisprudential analysis of the right to data protection and of the elements that make it distinct from privacy. Its purpose is to contribute to the doctrinal debate which still surrounds data protection and its blurry boundaries with the right to privacy. It has been written that 'the connotations associated with "data protection" have shifted repeatedly and substantially and further defining the term turned out to be a futile if not tautological quest'.[6] It has also been held, more recently, that distinguishing between privacy and data protection[7] would be of marginal utility, as the two rights would be part of the same system: privacy as a substantive right (the game) and data protection as a procedural right (its rules), protecting the same array of rights and freedoms.[8] This chapter rather holds that data protection is evolving away from privacy into something entirely distinct, albeit still connected to it. EU data protection has become a procedural, auxiliary, *sui generis* fundamental right, that emerged as a response to technological development and to the growing importance of secondary data protection

legislation and that embodies a societal stance towards how personal data processing has been shaping the modern world.

The structure of the chapter is as follows: the next section sketches the evolution of data protection in the EU, underlining its ties to technological development and to the secondary legislation that preceded its emergence as a fundamental right. The third section investigates data protection's rationale by comparing it with privacy and the fourth one argues about the structure and placement of Article 8 CFR. The fifth and sixth section outline this chapter's understanding of the rationale underlying data protection and of its essence, respectively.

II. Birth of a Strange Fundamental Right

Data protection has historically been tied to privacy,[9] itself a multifaceted, foggy concept since its very inception.[10] While the roots of the right to personal data protection are entrenched in privacy, it did not take long for data protection to begin assuming its own specific, individual connotations. From the end of the eighteenth century, several social processes involving the political West – most significantly the US, the UK and continental Europe – fostered the need for centralised information collection. Amongst other factors, one can identify the advances in communication and transportation technologies; the growth of the active electoral pool; the rampant urbanisation deriving from the growing industrialisation and consequent migrations from the countryside to the city; and thus an increasingly condensed workforce.[11] '*(B)ureaucracy emerged as a response to nineteenth-century industrialization*'.[12]

During the Second World War, military necessities spurred an upsurge of research and development initiatives aiming at developing technologies that would allow the nations involved to get the upper hand in the escalating confrontation. From the code-breaking efforts of Bletchley Park,[13] to the development of semi-autonomous anti-aircraft and anti-missile systems to counter German ballistic progress,[14] war stimulated a wave of innovation whose ripples lasted long after its end. After the conclusion of the conflict, part of the investment and the technologies that were designed or employed for military purposes were adapted to peacetime needs, resulting in the start of the mainframe era. 'The computer, originally designed to track missiles and break secret codes, came at exactly the right time for government bureaucracy.'[15] From a regulatory perspective, the Second World War and its aftermath[16] also led to the recognition of the right to privacy at an international level;[17] of paramount importance, in this respect, is the foundation of the Council of Europe (CoE) in 1949 and to the subsequent drafting of the European Convention on Human Rights (ECHR) in 1950. The right to privacy is incorporated in Article 8 ECHR,[18] which protects private and family life, home and correspondence.[19] While the ECHR does not contain any article specifically dedicated to data protection, over time Article 8 has gradually been interpreted by the European Court of Human Rights (ECtHR) as covering personal data processing as well.

The two decades between 1950 and 1970 witnessed the rise of general-purpose mainframe computers. Concerns about data processing were not new at the time – the census, for instance, has been an historically problematic instrument and so have been, for example, the postal system, the telegraph, the telephone and its wiretapping, the photo camera, and the growth of government record systems in general.[20] The magnified information storage and processing capacity deriving from the rise of mainframe computing caused a newfound wave of concern, which began to be addressed by national legislatures.[21] The 1970s saw the advent of a wave of novel legislative instruments meant to address what has been called the 'computers and privacy' issue[22] – the novel set of problematics deriving from centralised, large-scale data processing. Mayer-Schönberger divides[23] this earliest wave of national data protection regulation into two distinct phases. The first phase, where the emphasis of the regulatory intervention was on the new-fangled role of personal data processing in society, took a functional, *ex-ante* approach, mostly focusing on licensing and registration procedures. '(F)irst-generation data protection norms [did] not entrust individual citizens to ensure compliance with substantive data protection regulation':[24] adherence to the law was directed by and through special institutions and authorities and individuals had a secondary role. In this first stage, the role, pervasiveness and societal importance of databanks was still relatively limited.

A second regulatory wave,[25] which spanned from the end of the 1970s to the first half of the 1980s, was largely driven by the rapidly growing number of computers available, which got progressively smaller and more affordable and eventually began making their way into individual households. The period between the late 1960s and the early 1980s saw the rise of smaller (and cheaper) commercial computing systems at first, followed by the advent of personal computing. This second wave of national legislation focused on the individual, echoing the idea of (data) privacy as freedom[26] which arose as a response to the 'computers and privacy' issue of the previous decades. The legislature's focus, at the beginning of the personal computing era, shifted from the regulation of databanks to the protection of the individuals that might be impacted by the information those databanks processed. Seminal data protection laws[27] thus went from the regulation of databanks to the protection of individuals' privacy vis-à-vis personal data processing.

A notable development within this second phase in the evolution of the right to data protection was not launched by national parliaments nor by international institutions, but by a landmark decision by the *Bundesverfassungsgericht*, the German Constitutional Court.[28] In its 1983 Census decision, the Court tied data protection with the idea of privacy as freedom and with the concept of informational self-determination – *Informationelle Selbstbestimmung*. The Court developed a novel right to informational self-determination, stemming from the general, monistic personality right recognised by the *Grundgesetz*, the German federal constitution. Under the conception of data protection as informational self-determination, any processing of personal data is seen as an interference with the right,[29] unless the data subject exercises her self-determination by consenting to it.[30] Such approach, however, was not really followed by the contemporary and successive data protection

instruments enacted at CoE and EU level.[31]

Due to the growing amount and importance of transborder (personal) data flows, data protection also began to internationalise, with respect to both its sources and its scope, particularly by virtue of the work done by the Organisation for Economic Co-operation and Development (OECD)[32] and by the CoE. The CoE's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108),[33] the first binding international data protection instrument, was enacted to 'reconcile the fundamental values of the respect for privacy and the free flow of information between peoples'.[34] Convention 108 contains a list of essential data protection principles which still form the core of any regulatory initiative in the field,[35] and defines as data protection individuals' 'right to privacy, with regard to automatic processing of personal data',[36] still tying it to privacy but, at the same time, somehow distinguishing it from the right to private life *ex* Article 8 ECHR.

While European institutions have been inquiring about the 'computers and privacy' issue since the early 1970s, it is the beginning of the 1990s that saw the inception of EU data protection law, a third phase in the development of data protection as a standalone right within the European legal order. By then, personal computers became fairly widespread. The germinal internet, largely born out of government-backed R&D,[37] was transitioning into its modern form, and the World Wide Web had just been created. The first half of the 1990s witnessed a level of technological change in networking and computing technologies, which became increasingly pervasive and more and more available. In 1990, the Commission proposed, through a Communication,[38] a large regulatory package on the protection of personal data. The package included, inter alia, a proposal for a directive on the protection of individuals in relation to the processing of personal data, which eventually became the Data Protection Directive[39] (DPD), cornerstone of EU data protection law. Technology kept progressing rapidly and so did its societal impact, so additional data protection legislation[40] was enacted in the following years; the two decades after the Commission's 1990 Communication can, however, still be portrayed, unitarily, as a third phase in the development of the EU right to personal data protection. In this phase, EU data protection law was still framed as safeguarding 'the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data'.[41] Notably, since back then the EU (then EC) did not have competence for legislating on fundamental rights, the DPD was adopted under a market-making legal basis (Article 100a of the EC Treaty, now Article 114 TFEU). While the choice of an internal market basis depended mostly from the necessity to overcome formal and procedural obstacles to the enactment of Union law, rather than from a genuinely privileged connection with the single market's development,[42] the DPD's market-making legal basis has been an important element in shaping EU data protection law and jurisprudence.

The third stage in the progress of EU data protection law, the DPD age, entwines with a fourth one, which is demarcated by the enactment of the Charter in 2000 and by the Lisbon treaty in 2009. The Charter, the EU's own fundamental right catalogue, differentiates

between the right to privacy (Article 7) and the one to data protection (Article 8) for the first time, cementing their formal difference at a primary level. The proclamation of the Charter meant the explicit constitutional recognition of data protection as a fundamental right in the European framework.[43] Initially, the Charter had no binding force and the dichotomy between privacy and data protection could still be questioned; its incorporation in the EU Treaties by the Lisbon Treaty[44] put such debate at rest: the EU right to data protection is now unambiguously distinct from the right to privacy. The Lisbon Treaty, aside from incorporating by reference the Charter into the Treaties system, also abolished the previous 'three-pillar'[45] system, which were absorbed into a new, 'monistic' EU that inherited legal personality from the EC.[46] Article 16 of the Treaty on the Functioning of the European Union (TFEU)[47] emerged as a result of such overhaul, laying down the mandate of the EU in relation to data protection. Article 16(1) TFEU and Article 8 CFR enshrine the right to data protection; Article 16(2) TFEU broadly tasks the legislature with setting rules on personal data protection, subjecting them to an independent authority's control in accordance with Article 8(3) CFR. The broad mandate to enact fundamental rights legislation and ensure data protection ex Article 16 TFEU adds to the general duty of the EU and of its Member States to respect the fundamental rights listed in the Charter.[48] The abolition of the pillar structure and the enactment of Article 16 TFEU broadened the EU's mandate with regard to personal data protection legislation, deepening the latter's distance from the right to privacy *ex* Article 7 CFR and from Article 8 ECHR.

Since 2011, data protection entered its fifth age: The General Data Protection Regulation[49] (GDPR) era. The tectonic shifts in technological development (eg cloud computing, big data analytics, automated decision making) that occurred during the preceding decade spurred the need for a modernised data protection system fit for the twenty-first century.[50] The beginning of the decade marked the start of a period of regulatory overhauls in data protection law, from the repealing of the DPD by the GDPR and of Decision 2008/977/JHA by the Police Directive[51] to the modernisation of the OECD Guidelines[52] and Convention 108.[53] The GDPR, born well after the promulgation of the Charter, never actually mentions the right to privacy,[54] focusing on all 'fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data'[55] instead. The right to data protection, during this regulatory wave, appears to be further detaching itself from privacy, increasing its conceptual autonomy as a response to technical progress and to the importance that (personal) data processing assumed over time. After the promulgation of the Lisbon Treaty, the EU acquired an explicit mandate to regulate data protection through Article 16 TFEU (a fundamental rights' instrument) and does not have to rely on a market-making basis like Article 114 TFEU anymore. The substantive effects that the choice of Article 114 TFEU as a legal basis had on the content of the DPD (and on the jurisprudence that developed it) are, however, still visible in the GDPR's architecture.

The path of data protection has led to the birth of a strange, *sui generis* fundamental right. Spun out of privacy, itself one of the hardest rights to define, data protection law has always

been extremely responsive to technological progress and to its impact on society,[56] changing its substantive provisions as the state of the art evolved.[57] Some constitutions of EU Member States recognised data protection as a fundamental right early on;[58] at EU level, however, secondary legislation (ie the DPD) preceded data protection's (quasi) constitutionalisation[59] as a separate fundamental right. Data protection's inclusion in the Charter was largely driven by the growing societal importance of secondary legislation like the DPD and by the necessity to sustain its fundamental rights dimension[60] in light of the developing state of the art in data processing and of its growing societal importance. These are amongst the main peculiarities of the fundamental right to personal data protection: its historical and logical ties with privacy, its responsiveness to the developments in computing technology and to the significance that personal data processing acquired in contemporary society, and the fact that its (quasi)constitutionalisation as a fundamental right by the Charter came after the secondary legislation from which it gained (and to which it gave) further legitimacy.

III. On the Distinction between Privacy and Data Protection

Privacy and data protection are historically and conceptually entwined. Before the Charter, at a primary level, data protection was based on an extensive interpretation of Article 8 ECHR, read as enshrining both the right to privacy and the one to data protection, the latter particularly after Convention 108. With the Charter, the EU got its own fundamental rights catalogue and the distinction between privacy and data protection has finally been formalised. At a substantive level, such distinction is, however, much less clear, and the two rights are still often conflated. Still, to pinpoint the essence and rationale of the right to data protection, moving from what makes it distinct from the right to privacy seems a sound starting point. In consideration of the multi-level structure of fundamental rights[61] in Europe, this section frames the right to privacy as enshrined in the Charter, in the ECHR and in the ECtHR's jurisprudence[62] and the right to data protection as deriving from the Charter, the CJEU's and the ECtHR's jurisprudence, but also from the legislative framework implementing it in secondary legislation. The development of data protection is particularly entwined with the secondary legislation that preceded its (quasi)constitutionalisation – the DPD in particular – and it can be argued that the introduction of data protection as a fundamental right drew legitimacy from, and gave legitimacy to, the pre-existing secondary law.

As Lynskey notes,[63] it might be useful to consider the overlap between the right to privacy and Article 8 ECHR on the one hand and EU data protection on the other. Lynskey holds that a first distinction could derive from the applicability of each framework to private relations. While Article 8 ECHR (and Article 7 CFR, for that matter) do not have direct horizontal effect, the fundamental right to data protection *ex* Article 8 CFR is implemented through secondary legislation that is applicable to public and private parties alike and thus

has direct horizontal effect. From this perspective, the applicability of data protection seems to be broader than privacy. However, Lynskey also notes that ECHR rights can have an indirect horizontal effect by virtue of the positive obligations doctrine,[64] which obliges states to actively safeguard ECHR rights. Moreover, ECHR rights can be (and often are) taken in consideration by national courts in their judgments, akin to how German constitutional doctrine constructs the indirect horizontal effect (*mittelbare Drittwirkung*) of constitutional provisions.[65] Finally, EU law aside, ECHR rights have been transposed into national legislation,[66] or were enshrined in the states' national law even before the ECHR. The difference between the horizontal effects of the right to privacy ex Article 8 ECHR vis-à-vis EU data protection does not appear to be particularly meaningful in determining, by comparison, what constitutes data protection's rationale. The same considerations seem to hold true,[67] *mutatis mutandis*, for the horizontal effect of Article 7 CFR.[68] As Kokott and Sobotta point out, the differences in the personal scope of privacy and data protection result from data protection's implementation in a secondary framework, rather than from the applicability of Article 8 ECHR and Articles 7 and 8 CFR to horizontal relations.[69]

Considering the differences in the two rights' material scope turns out to be more fruitful. Not all kinds of data processing seem to have the potential to breach the right to information privacy, while data protection has a wider and 'agnostic' scope. When it comes to the information falling within the scope of the right to privacy, the ECtHR recognises that all kinds of personal data can potentially interfere with the scope of Article 8 ECHR,[70] and yet never actually ruled that all kinds of personal data *processing*, regardless of its nature and contextual elements, fall under Article 8 ECHR.[71] The ECtHR, while recognising that even public data can interfere with the right to privacy, seems to consider, when assessing violations of Article 8 ECHR, that the latter covers the processing of publicly available information only if the processing is systematic in nature[72] or reasonably unexpected by the data subject.[73] Data protection, on the contrary, applies to personal data – any information relating to an identified or identifiable natural person[74] – regardless of whether it is private or public.[75] Furthermore, the meanings of 'processing'[76] and 'information'[77] adopted by EU data protection law are practically all-encompassing, so that any treatment of the data considered integrates the legal definition of data processing under Article 8 CFR, but might not be considered under the scope of Article 8 ECHR (and hence Article 7 CFR). The *Österreichischer Rundfunk* case[78] is an early example of the developing distinction between the respect for private life and the protection of personal data by virtue of their scope.[79] The Court, after stating that the DPD must be interpreted in accordance with Article 8 ECHR when applied to an area within its scope,[80] divides the processing operations that can breach Article 8 ECHR from those that cannot. A national law compelling a certain category of data subject to supply salary data to a governmental body was found to be a compression of Article 8 ECHR, while the processing of the same data by the employer for its own internal purposes did not, provided that data protection rules were respected.[81]

The right to private life, which has always been voluntarily left undefined by the ECtHR,[82] has become, over time, almost a general personality right,[83] covering the broadest

range of situations, only a subset of which involves information processing.[84] However, the facet of the right to privacy *ex* Article 8 ECHR that involves the processing of personal data (data privacy) has a narrower scope than the right to data protection, since it either requires the information processed to be somehow private in nature[85] or the processing to be systematic in kind. Privacy, in a nutshell, does not necessarily extend to all kinds of personal data processing, as does data protection.[86] Either the processing of data or the data itself are 'excluded from the privacy scope when (1) the data as such are not considered as private, (2) when there are no systematically stored […] data, (3) when the data are not systematically stored with the focus on the data subject and (4) when the data subject could reasonably expect the processing'.[87] Hijmans, while recognising the narrower scope of *data* privacy under the ECHR,[88] contends that, considering the right to privacy *ex* Article 7 CFR, such conclusion does not hold true any more, and that since the Charter and the Lisbon Treaty 'all processing of personal data has a potentially adverse effect on the right to privacy under Article 7 Charter'.[89] The author however recognises that 'interference with the right to privacy is assessed in a contextual manner',[90] thus implicitly acknowledging how circumstantial factors about, for example, the way the data is processed or the subjective elements of the data subject, might still exclude the processing instance from the scope of the right to privacy – but not from data protection.

The substantive protection granted by privacy and personal data protection, albeit partly overlapping, is another element that can allow it to distinguish the two rights' rationale: not all rights afforded by data protection law can be mirrored in Article 8 ECHR.[91] Many rights granted by secondary data protection legislation have been incorporated in the ECHR's privacy framework by the ECtHR's jurisprudence, but the substantive safeguards granted by data protection law are still more varied and heterogenous. Some provisions of the DPD, such as those about automated decision making or the security of the processing, are arguably extraneous to the scope of Article 8 ECHR, a postulate that has been reinforced by the introduction of additional rights (eg personal data portability)[92] by the GDPR. The right to personal data protection substantiates itself in a wide array of diverse information rights, a hodgepodge whose coherence is given by the dual objective of safeguarding data subject's rights and freedoms and ensuring the free flow of data within the Union. The market-making framing of the DPD has been largely due to the 'treaty-based games'[93] through which the EU managed to legislate on fundamental rights before having the competence to do so, but the construction of EU data protection secondary law as (also) a single market tool has arguably had an impact on how the substantive safeguards offered by data protection law, on its differentiation from privacy, and ultimately on its standing as a different autonomous right.

A contribution by De Hert and Gutwirth[94] identifies another fundamental difference between privacy and data protection, distinguishing them on teleological grounds by reference to their function within the democratic constitutional state. The authors define privacy as a 'tool of opacity', which protects individuals against interference by the state and by private actors by requiring abstention from undesired intervention. Privacy curtails power by setting normative limits to it. Data protection, on the other hand, is mainly a 'tool of

transparency', regulating and channelling the exercise of power, rather than stopping it.[95] The distinction advanced between privacy as a tool of opacity and data protection as a tool of transparency is convincing, well-grounded and possibly one of the soundest justifications of the dichotomy between the two rights. It does not, however, entirely pinpoint the rationale of the right to data protection. As the authors themselves recognise, data protection is *mainly* a 'tool of transparency', but sometimes its substantive provisions curtail the possibility of processing personal data or set limits on the kinds of processing that can be done on personal data. As an example of the latter, the authors identify the rules applicable to sensitive data, profiling and the purpose specification principle.[96] Likewise, as the authors acknowledge, privacy has *mainly* a negative role, stopping the exercise of power, but *also* a positive one, ensuring individual freedom and self-determination.[97] De Hert and Gutwirth's theory is persuasive, yet its main utility is to clarify the teleological dichotomy between privacy and data protection, rather than the latter's substance.

The different nature of privacy and data protection could be highlighted, finally, by reference to substantive and procedural rights.[98] Substantive rights are created to protect and uphold interests considered important, while procedural rights appear at a later stage, setting the conditions through which those substantive rights are implemented.[99] Privacy, it is argued, is largely upheld through substantive provisions,[100] while data protection has an eminently procedural nature.[101] Data protection is meant to enable a broad range of rights and freedoms, privacy amongst others, through a varied range of provisions. It has been stated, in this respect, that it would only exist to serve other rights and 'does not directly represent any value or interest per se'.[102] While the following section disputes that the right to personal data protection does not represent a value or interest on its own, its eminently procedural nature appears hardly disputable. Hustinx, in this respect, highlights that data protection is meant to provide a proactive, structural protection of the rights and freedoms that might be dented by personal data processing, regardless of a possible interference with the right to respect for private life.[103]

The EU right to personal data protection is thus, formally and substantively, not privacy anymore. Its (quasi)constitutionalisation by the Charter formally separated from the right to privacy, and its evolution in the jurisprudence of the ECJ and the ECtHR and in EU secondary legislation made it essentially different,[104] albeit still clearly connected to privacy. Data protection differs from privacy by virtue of the width of its scope and of the number of individual rights it grants. It is also distinct from privacy in that it is, mostly, a tool of transparency, rather than a tool of opacity. Data protection also has a prevalently formal and procedural nature, rather than a substantive one. Those traits may *help* delineate the essence and rationale of the right to data protection but are not enough to do so on their own.

IV. Data Protection and the Structure of the Charter

The content and structure of Article 8 CFR are also helpful in enucleating the constitutive elements of the right to data protection and thus its rationale and, perhaps, its essence as well. In its initial paragraph, Article 8 states, quite generically, that '(e)veryone has the right to the protection of personal data concerning him or her'. The first paragraph grants a right – the protection of personal data – but does not specify its content. The second paragraph details that '(s)uch data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law' and that '(e)veryone has the right of access to data which has been collected concerning him or her and the right to have it rectified'. The third and last paragraph of Article 8 mandates that '(c)ompliance with these rules shall be subject to control by an independent authority'.

The Charter's Article 8 lends itself to two possible readings: either a positive, permissive conception of data protection, or a negative, prohibitive one.[105] The core of the distinction is the interpretation of the second and third paragraphs of Article 8: do they detail the content of the right to data protection, or is the content of the right given by the first paragraph, while the second and third paragraphs detail the conditions under which such right can be limited? [106] The structure of the Charter would seem to point towards the former, framing data protection as a permissive right. The Charter lists the rights it contains in its first 50 articles, while Articles 51–54 contain a number of general provisions governing the interpretation and application of the Charter. Article 52, 'Scope and interpretation of rights and principles', provides for the conditions under which those rights can be limited. This construction echoes the binary nature of Article 8 ECHR, in which the right is asserted in the first paragraph[107] and its admissible limitations in the second.[108] It is also consistent with the parallelism between Article 7 CFR, which enshrines the right to privacy and Article 8(1) ECHR: the right is contained in Article 7 CFR and in Article 8(1) ECHR and the limitations are regulated by Article 52 CFR and by Article 8(2) ECHR, respectively.

Conceptualising data protection as a restrictive right and thus Article 8(2) as special conditions that legitimise an interference, rather than parts of the right itself, would arguably deviate from the binary structure of the Charter. That is also consistent with the fact that, as reported by González Fuster and Gutwirth,[109] early appearances of what would later become Article 8 CFR were initially connected not to privacy, but to the right of access to documents. That would lean towards the conceptualisation of Article 8(2) CFR as part of the right to data protection, as it mentions access and rectification of personal data, rather than as (special) conditions justifying an interference, as does Article 52.[110] The authors also report that all three paragraphs of Article 8 CFR were initially envisioned as a single paragraph,[111] an additional reason for conceptualising Article 8(2) and 8(3) CFR as parts of the right itself, rather than as additional conditions legitimising an interference. That is also coherent with Convention 108's approach, which 'is not that processing of personal data should always be considered as an interference with the right to privacy, but rather that […] processing of personal data must always observe certain legal conditions'.[112] Furthermore, the Convention tasked with the Charter's development reportedly considered making Article 8 about the right to informational self-determination, thus espousing a prohibitive conception of personal data protection, but such approach was eventually rejected.[113]

In accordance with a positive reading of the right to personal data protection as a tool of transparency, this chapter interprets Article 8 CFR as being unitarily prescriptive of the content of the right, as opposed to framing Article 8(2) and 8(3) as conditions legitimising an interference with the right.[114] Consequently, it argues the components of Article 8(2) and 8(3) should be seen as being strongly linked with the essence of the right itself. The fairness principle,[115] the purpose specification principle, the lawfulness principle, the right of access, the right to rectification and the control by an independent authority[116] are thus constitutive elements of the EU right to personal data protection, rather than conditions additional to those set by Article 52 CFR, legitimising an interference with it.

It appears, however, debatable whether the lengthy and varied list of rights and principles contained in Article 8(2) and 8(3) embodies data protection's rationale and (even more so) whether it directly constitutes data protection's essence. If anything, Article 8's elements confirms the tie that the fundamental right to data protection has with international instruments and the secondary legislation that preceded its (quasi)constitutionalisation, and its eminently procedural nature. The following section argues that the actual essence of the right to data protection is to be sought in a systematic, teleological interpretation of Article 8 CFR, in light of (and as distinct from) Article 8 of the ECHR, and Article 7 CFR and with due consideration to the peculiar historical characteristics of the right's development.

V. A Right to a Rule

The right to data protection has been strongly shaped by the evolution of the secondary legislation that has been enacted, since the early 1970s, to tackle the 'computers and privacy' issue.[117] Such legislation, in turn, has been entwined with and responsive to, technological progress,[118] so that its provisions have been changing in a substantial manner as time has passed and as new technologies impacted society. The increasing pervasiveness and societal importance that technology has had since the turn of the past century has led to the rapid emergence of a normative *corpus*, data protection law, which predated its constitutionalisation. In this sense, data protection legislation and hence the fundamental right to data protection responds to necessities that diverge, partly and yet sensibly, from those covered by the right to privacy, at least in the European milieu. This is reflected in the different scope data protection has vis-à-vis privacy. Narrower, as it only covers the processing of personal data, rather than the whole spectrum of activities covered by privacy, but also broader, as it applies also to information not considered as private, that is not systematically stored or processed, or whose processing could reasonably be expected by the data subject. It is also reflected in the narrower set of rights on information granted by privacy, in comparison to data protection.

The dichotomy between privacy as a tool of opacity, meant to curtail power, and data protection as a tool of transparency, meant to permit but channel through a set of rules,[119] is also a key element in understanding the rationale of the right to data protection. It explains

the reason of the constitutionalisation of data protection as a separate right and is coherent with the functioning of secondary data protection legislation at a national and supra-national level. Data protection is meant to allow information sharing: there would be no need for it if there were a general prohibition of personal data disclosure,[120] the law very seldom prohibits the processing of personal data, rather mandating the requirements to be respected to make it lawful. This permissive conception of the right to personal data protection as a tool of transparency is also coherent with its procedural nature.[121] Data protection channels a particular activity – personal data processing – by setting certain procedures and by granting a number of rights to data subjects and obligations to controllers and processors. Data protection aims at safeguarding a broad and diverse spectrum of rights and freedoms, privacy (inter alia) included.

If data protection were a negative, restrictive right, forbidding the processing of personal data, then every personal data processing instance would be a compression of such right, regardless of whether it is legitimate. In that case, the provisions ex Article 8(2) and 8(3) CFR would be special legitimising conditions, identifying the requirements rendering a compression to the right to data protection legitimate. This chapter, however, adheres to a positive, permissive view of data protection,[122] where personal data processing does not result in a breach of the right by itself. Accordingly, Article 8(2) and 8(3) CFR and the elements it enumerates (the fairness principle, the purpose specification principle, consent and the other grounds substantiating the legality principle, the right of access, the right to rectification and the control by an independent authority) are seen as constitutive elements of the fundamental right to data protection, crucial elements to be considered in ascertaining its substance. That is not to say, however, that they constitute the essence of the right by themselves: it cannot be discounted that the CJEU might find other core elements of data protection, framing them as implied in Article 8(1) CFR.[123] The list of rights and principles contained in Article 8(2) and 8(3) CFR is too specific, reductive and heterogenous to constitute the rationale of data protection on its own. Rather, it constitutes a synthetic representation of the societal posture that was developed over the years and through several legislative instruments, as a response to the pervasiveness and importance that personal data processing acquired since the turn of the last century. To understand the essence and rationale of a right, one may also move from its infringement: a breach of the fairness, purpose specification or lawfulness principle, of the rights to access and rectification,[124] or of the independent authority's control,[125] does not necessarily amount to a breach of the *essence* of the right to data protection *per se*. There must be more to it than that: the CJEU often ruled on those matters without mentioning a breach of the essence of the right, nor a *serious* interference thereof.

It appears useful, at this point, to recapitulate what this chapter identified as constitutive elements of the right to personal data protection, as enshrined in the EU Charter of Fundamental Rights. To begin, data protection has had, since its very inception, a strong tie with the development of computing technologies. Such a tie led to the fast-paced development of a *corpus* of norms, that predated the (quasi)constitutionalisation of the right at EU level. EU data protection law emerged, in its distinction from privacy, as an *omnibus*

regime, sector-neutral and applicable to public and private actors alike,[126] whose broad scope encompasses an extremely wide range of processing instances.[127] If privacy is prohibitive, a tool of opacity, data protection is permissive – a tool of transparency,[128] designed to provide safeguards to individuals whenever their personal data is processed. Data protection is also a procedural right,[129] in that it hardly protects a specific interest on its own, but rather serves the goals pursued by other substantive fundamental rights. Finally, as data protection is a permissive right, the contents of Article 8(2) and 8(3) CFR (the fairness, purpose specification and lawfulness principles, the rights of access and rectification and the control by an independent authority) are to be seen as constitutive of the right, rather than special conditions legitimising an interference with it.[130]

This chapter's conclusion is that the most coherent construction of data protection (as separate from privacy), at least in the European milieu, is simply as the fundamental right to having a (set of) rule(s) regulating the processing of personal data. While that may seem reductive, I believe it is not, and while that can *prima facie* appear generic, I argue that it is rather quite specific. Most importantly, I maintain that it is the most consistent explanation of the (quasi)constitutionalisation of the right to data protection as distinct from privacy, in light of its characteristics and of its *sui generis* development. In this respect, my argument echoes the notion of proceduralism[131] in democratic theory, but applied, rather than to institutional legitimacy, to the identification of the value underlying personal data protection. The definition of 'proceduralism' has different nuances depending on the specific context of reference, but can be broadly defined as a theory that 'justifies rules, decisions, or institutions by reference to a valid process, as opposed to their being morally correct according to a substantive account of justice or goodness'.[132] Under this definition, proceduralism contrasts with epistemic theories of justice that ground the legitimacy of rules, decisions, or institutions by reference to underlying values like knowledge and truth, however specified, rather than on the validity of the underlying procedure.[133] Similarly, a 'proceduralist' view of data protection[134] derives the latter's legitimacy and status of fundamental right from the process through which it came into existence and from the rules through which it is substantiated, as both are expression of the collective will to regulate personal data processing. The value of data protection is, in a way, in the very existence of a system of rules and norms applying to the processing of personal data, regardless of its connection with concepts like privacy, or the secrecy and confidentiality of the information processed.

The European fundamental right to personal data protection emerged as a consequence of, and a response to, the rampant digitalisation of society and the ever-growing importance of the processing of (personal) information. It embodies the collective[135] decision of allowing personal data processing if and to the extent that it is subject to a certain set of rules, rather than prohibiting it unless specific requirements are satisfied. Such rules (and their judicial interpretation) have substantially changed over time, evolving as the technological environment mutated. Their core is (partly) epitomised (yet not represented in its entirety) by Article 8(2) and 8(3) CFR, whose content portrays a heterogeneous array of rights and principles that have remained staple regulatory mechanisms since the inception of EU data protection law. Data protection is 'a catch-all term for a series of ideas with regard to the

processing of personal data',[136] which makes the core of the right hard to pinpoint. At the same time, such heterogeneity is indicative of the fact that data protection's core goes beyond the elements enumerated by Article 8(2) and 8(3) CFR. The Charter unequivocally granted the status of standalone fundamental right to data protection, explicitly distinguishing it from privacy, which, at least from an EU perspective, makes the position identifying data protection as a subset of the right to privacy hard to maintain. Considering data protection's *sui generis* emergence[137] and its (quasi)constitutionalisation by the Charter, this chapter contends that the most coherent reading of the *fil rouge* underlying the potpourri of disparate rights and principles that make up data protection is given by the societal will of regulating the processing of personal data by means of information technologies in itself. A 'right to a rule', so to speak,[138] its rationale by now more akin to due process or effective judicial protection than it is to privacy.

That partly explains how the CJEU, in the *Schrems* case,[139] after noting that 'legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life',[140] stated that 'legislation not providing for any possibility for an individual to pursue legal remedies in order to have access […] rectification or erasure of [personal] data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter',[141] without, however, tying its reasoning with Article 8 (or to its essence) directly. The Luxemburg court found attributes pertaining to data protection at the core of the right to an effective remedy[142] *ex* Article 47, so much so, that it considered the lack of the possibility to enforce them a breach of the very essence of the right. On the one hand, the *Schrems* case highlights the ties that data protection has with neighbouring notions as procedural justice, democratic legitimacy and the rule of law; on the other hand, it is regrettable that the CJEU did not tie Articles 8 and 47 together, somehow leaving their connection to further interpretation. As it has been already noted,[143] both Articles give expression to different facets of the rule of law and it is unfortunate that the CJEU did not clarify their substantive relationship when it had the chance. Regardless, the reference to data protection provisions within the frame of Article 47 CFR still highlights how data protection substantiates itself in a procedural system of heterogeneous checks and balances that is gradually detaching itself from privacy's rationale.

VI. The Essence of the Right to Data Protection

Defining data protection in the terms above – as the fundamental right to have a system of rules regulating personal data processing – leads to postulating, lacking authoritative interpretation, about what the essence of the right to data protection may be.[144] It also serves the purpose of distinguishing it from the right to privacy, respecting the dichotomy introduced by the Charter. In this respect, it has been noted how the CJEU has been (regrettably) assessing possible compressions of the right to data protection through the

lenses of the right to privacy, following what has been defined as 'privacy thinking'.[145] As plenty of authors have already delved into the conflation between data protection and privacy by the CJEU,[146] this section elaborates on this chapter's view of the essence of the right to personal data protection.

The concept of essence of rights, explicitly mentioned by the Charter,[147] is somehow pervasive within the EU multi-level[148] fundamental rights framework; as has been noted,[149] its source can be traced in many Member States' constitutional traditions, in the CJEU's pre-Charter jurisprudence and in the ECHR and ECtHR jurisprudence. Brkan depicts the possible interferences with fundamental rights as concentric circles, where one finds, at the outermost layer, no interference with the right and then – progressing towards the centre – justified interference, unjustified interference, serious interference and interference with the right's essence at its very core.[150] The distinction between interferences is particularly meaningful in light of the debate surrounding the relationship between balancing (proportionality *sensu lato*) and the essence of fundamental rights. A relative (or integrative)[151] stance admits the possibility of compressing the essence of a fundamental right to safeguard another fundamental right; an absolute (or exclusive)[152] stance constructs essence and proportionality as mutually exclusive concepts.[153] Theorising the essence of the right to data protection is meaningful regardless of whether one adheres to the exclusive stance or the integrative one.[154] In the former case, it identifies the interferences that are inadmissible regardless of the relative nature[155] of the right to data protection; in the latter, it permits to nuance the gradation of the interference in view of the performance (*ex ante*) or the assessment (*ex post*) of the balancing test.

Brkan posits[156] that the essence of a fundamental right is interfered with if (1) the interference threatens the very existence of that right, either for all right holders or for a specific right holder or group of right holders;[157] and (2) if overriding reasons for such interference do not exist. The second part of the test espouses the absolute/excusive position, which conceives interferences with the essence of the right as unjustifiable through proportionality balancing and – conversely – does not consider an interference with a right as a compression of its essence in all cases where there is possible to justify it by reference to overriding reasons (ie balancing). The first part of the test determines the presence of an interference with the essence of the right, which happens where the very existence of the right is called into question for all right holders (objective interference with the essence) or for a particular right holder (subjective interference with the essence).[158] Brkan's test to determine an interference with the essence of a fundamental right is particularly interesting in light of the conception of the right to data protection set out in this chapter. The author postulates that the essence of a right is infringed where the existence of the right is called into question and when there are no overriding reasons for the compression, as overriding reasons would introduce proportionality balancing, which is seen as incompatible with the concept of essence. Following such framework and the framing of data protection outlined above, this chapter maintains that an infringement of the *essence* of the right to data protection is a compression strong enough to threaten the very existence of the system of checks and

balances in which the right to data protection is substantiated, when overriding reasons do not exist.[159]

Data protection is not an absolute right,[160] so it can be legitimately compressed by other overriding rights; it can also be illegitimately encroached upon, which would derive from a result of the balancing test favouring data protection rather than the other conflicting right. A violation of the essence of the right to data protection, which would be configurable (following an absolute/exclusive approach) only in absence of overriding reasons justifying the compression, should be constructed only in cases where the functioning of the regime regulating personal data processing is called into question,[161] regardless of which specific provision is infringed, but rather having regard to the functioning of the system in its entirety.[162] A violation of the essence of the right to data protection would thus exist in cases where the interference with the right challenges, explicitly or implicitly, the very societal choice of having an *omnibus* regime regulating the processing of personal data. Let us think of all the ways the system of checks and balances of which data protection is made can be practically broken by neglecting, exploiting, or misreading secondary law provisions that are not directly mentioned in Article 8 CFR or defined as 'essential' by the CJEU, such as perhaps Article 14(5) of the GDPR on the information to be provided where personal data have not been obtained from the data subject, or Article 23 on the possibility to restrict the scope of (some of) the obligations and rights of the GDPR, or again the provisions about transfers of personal data to third countries or international organisations contained in Chapter V, or the provisions relating to specific processing situations in Chapter IX.

The rights and principles listed in Article 8(2) and 8(3) CFR are amongst the earliest and most foundational instruments on which the EU's data protection framework is based and their violation[163] would intuitively appear as a very plausible way to encroach upon the essence of data protection. They do not constitute the essence on their own but represent and embody the decision of regulating personal data processing at a fundamental rights level: it is such collective will that constitutes the essence of the right to data protection. A recent contribution by Porcedda[164] follows a different route and attempts at enucleating the data protection's essence by identifying a number of attributes – 'the intrinsic and distinctive substantive dimensions of a right'[165] – drawn from a number of sources,[166] equating them with the 'essential components'[167] of the right. Porcedda sees the essence as the core of an essential component (or attribute), submits that there may be multiple essences to data protection and extracts those manifold essences[168] from the relevant attributes. Enucleating the essential components of data protection is a useful exercise to identify potential serious interferences with the right and the compression of one of the essential components of the right makes for a cogent case for a breach of the essence. However, the 'essences' identified by Porcedda seem to be mainly a further abstraction of data protection attributes/essential components, rather than its very essence. The fact that data protection may have several different essences is intuitively unsatisfactory, as it gives up on finding a single, unitary rationale underlying data protection, a whole which should be more than the sum of its parts. Moreover, data protection is a qualified right and can be compressed by competing rights: many of the 'essential elements' listed (eg those deriving from Article 8(2) CFR) can be

legitimately compressed by competing rights, if the conditions set by Article 52 CFR are met. If those attributes represented data protection's essence(s) their compression would not be allowed, which does not appear to be the case. There is, finally, an additional possible level of abstraction that can be reached by tying together the 'essential elements' identified by Porcedda, the substantive characteristics of data protection and its evolution in light of the function it gradually assumed in society. That last, essential abstraction level is given by the functioning, at a systemic level, of the checks and balances in which data protection is substantiated, as it represents the expression of a collective[169] stance towards personal data processing.

The essence of the system of checks and balances in which data protection is substantiated – our fundamental 'right to a rule' regulating personal data processing – should be seen as the collective decision of generally allowing the processing personal data by virtue of its promises, while at the same time regulating it on account of its perils. An interference with the essence of the right to data protection is thus different from a 'regular' interference, regardless of how 'serious'. While the former dents part of data protection's system of checks and balances, the latter questions and endangers the very functioning and legitimacy of the collective posture towards personal data processing in its entirety, and hence ultimately its deepest roots: the rule of law and the democratic legitimacy of EU regulation.

VII. Conclusion

This chapter framed the fundamental right to data protection as the expression of a societal choice towards personal data processing. A permissive, procedural 'right to a rule', allowing – and yet channelling – an activity that is as fundamental for modern society as it is possibly dangerous. It tied the *sui generis* emergence of EU data protection to technological development and its (quasi)constitutionalisation to the growing importance of the secondary legislative framework. In light of the heterogeneousness of the rights and principles substantiating the fundamental right, both at primary and at secondary level, of its formal differentiation from privacy and of its procedural and permissive nature, this chapter argued that the most coherent conceptualisation of the right to data protection is of a system of rules and principles regulating personal data processing by virtue of its potential impacts on individuals and society. The essence of the right to data protection has been framed, accordingly, as the collective, societal choice of having a system of checks and balances regulating personal data processing. The infringement of the essence of the right to data protection has been defined as a compression strong enough to threaten the very existence of such a system of checks and balances when overriding reasons do not exist, regardless of which specific component of the right is compressed.

EU data protection is an inhomogeneous assortment of rules and norms whose substance hardly fits under a unitary rationale. Technological development, the diffusion of computing and the rampant datafication of society, led to the development of a *sui* generis right that spun out of privacy into something different, new and still in flux, which was then elevated to the

status of fundamental right by the Charter. Data protection is the answer to the power and information asymmetries running between who controls the means of data processing and the individuals those data refer to and responds to a recent need for protection that has risen in parallel with the advances in computing technologies and with their role in contemporary society. In a way, the justification of the ascension of data protection to the status of fundamental right should not be sought in the (scarce) conceptual autonomy or systematic coherence of the heterogeneous array of rights and principles of which data protection is made. Rather, it is the (quasi)constitutionalisation of data protection as an autonomous fundamental right that helps delineating its substance and its difference from privacy. The choice of creating an *omnibus* system of checks and balances regulating any kind of personal data processing and then to enshrine such a system at a primary level, was far from an obvious path. The seemingly incoherent set of rights and principles of which data protection is made, in light of its explicit (quasi)constitutionalisation by the Charter and moving from the assumption of the democratic legitimacy of the underlying legislative process, create a pragmatic system of protection that should be seen as the embodiment of such choice.

A consistent conceptualisation of the right to data protection serves the purpose of justifying the formal dichotomy between privacy and data protection introduced by the Charter, which are still too often conflated. It also boosts the legitimacy of the EU data protection framework by explicitly outlining how it expresses a definite societal posture towards personal data processing. Most importantly, recognising the conceptual autonomy of personal data protection and its ties to the advance of computing technology and (hence) modern society could foster the development of Article 8 CFR to its full potential. The law, both at a secondary and at a primary level, is an inherently living instrument, responsive to society's changing needs. The Charter, through the introduction of Article 8, created the possibility to further advance data protection into something able to steer society towards a place where the power and information asymmetry inherent to personal data processing is curbed by default. It would be a pity to let that chance go by keeping data protection under privacy's shadow and by focusing on its past emergence rather than on its capability to shape future society.

Acknowledgements

This research was performed with the financial support of the Dutch NWO/STW-Maps4Society program (project number 13718).

References

Alexy R, *A Theory of Constitutional Rights* (Oxford University Press 2009).
Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data WP136' (2007).
Bonnici JPM, 'Exploring the Non-Absolute Nature of the Right to Data Protection' (2014) 28 *International Review of Law,*

Computers & Technology 131.
Brkan M, 'The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors?' (2016) 23 *Maastricht Journal of European and Comparative Law* 812.
——, 'The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to Its Core' [2018] *European Constitutional Law Review* 1.
Bygrave LA, 'Information Concepts in Law: Generic Dreams and Definitional Daylight' (2015) 35 *Oxford Journal of Legal Studies* 91.
Ceruzzi PE, *A History of Modern Computing* (MIT Press 2003).
——, *Computing: A Concise History* (MIT Press 2012).
Clifford D and Ausloos J, 'Data Protection and the Role of Fairness' [2018] 37 *Yearbook of European Law* 130–187.
Corera G, *Intercept: The Secret History of Computers and Spies* (Hachette UK 2015).
de Andrade NNG, 'Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights' in Simone Fischer-Hübner *et al* (eds), *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life* (Springer 2010).
De Hert P and Gutwirth S, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in Erik Claes, Antony Duff and Serge Gutwirth (eds), *Privacy and the Criminal Law* (Intersentia 2006).
——, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Serge Gutwirth et al (eds), *Reinventing Data Protection?* (Springer 2009).
De Hert P and Papakonstantinou V, 'The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals' (2012) 28 *Computer Law & Security Review* 130.
Desai AC, 'Wiretapping before the Wires: The Post Office and the Birth of Communications Privacy' (2007) *Stanford Law Review* 553.
Docksey C, 'Articles 7 and 8 of the EU Charter: Two Distinct Fundamental Rights' in Alain Grosjean (ed), *Enjeux européens et mondiaux de la protection des données personelles* (Éd Larcier 2015).
Dougan M, 'The Impact of the General Principles of Union Law upon Private Relationships' in Dorota Leczykiewicz and Stephen Weatherill (eds), *The Involvement of EU Law in Private Law Relationships* (Bloomsbury Publishing 2013).
Fabbrini F, *Fundamental Rights in Europe: Challenges and Transformations in Comparative Perspective* (Oxford University Press 2014).
Fornasier M, 'The Impact of EU Fundamental Rights on Private Relationships: Direct or Indirect Effect?' (2015) 23 *European Review of Private Law* 29.
Fuster GG, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer Law, Governance and Technology Series 2014).
——, 'Curtailing a Right in Flux: Restrictions of the Right to Personal Data Protection' in Artemi Rallo Lombarte and Rosario García Mahamut (eds), *Hacia un Nuevo derecho europea de protección de datos, Towards a New European Data Protection Regime* (Tirant Lo Blanch 2015).
Fuster GG and Gellert R, 'The Fundamental Right of Data Protection in the European Union: In Search of an Uncharted Right' (2012) 26 *International Review of Law, Computers & Technology* 73.
Fuster GG and Gutwirth S, 'Opening up Personal Data Protection: A Conceptual Controversy' (2013) 29 *Computer Law & Security Review* 531.
Gellert R and Gutwirth S, 'The Legal Construction of Privacy and Data Protection' (2013) 29 *Computer Law & Security Review* 522.
Gutwirth S, *Privacy and the Information Age* (Rowman & Littlefield 2002).
Habermas J, *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy* 2nd edn (MIT Press 1996).
Hartzog W, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press 2018).
Hijmans H, *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU* (Springer 2016).
Hondius FW, *Emerging Data Protection in Europe* (North-Holland Publishing Company 1975).
Hondius FW, 'Data Law in Europe' (1980) 16 *Stanford Journal of International Law* 87.
Hornung G and Schnabel C, 'Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination' (2009) 25 *Computer Law & Security Review* 84.
Hustinx P, 'The Role of Data Protection Authorities' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009).
——, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' [2013] Collected Courses of the European University Institute's Academy of European Law, 24th Session on European Union Law.

Janciute L, ‘Data Protection and “Treaty-Based Games”: When Fundamental Rights Are Wearing Market-Making Clothes’ in Ronald Leenes et al (eds), *Data Protection and Privacy: The Age of Intelligent Machines* (Hart Publishing 2018).
Kokott J and Sobotta C, ‘The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR’ (2013) 3 *International Data Privacy Law* 222.
Koops BJ et al, ‘A Typology of Privacy’ (2016) 38 *University of Pennsylvania Journal of International Law* 483.
Korff D, ‘Comparative Summary of National Laws’ (2002) Brussels: EC Study on Implementation of Data Protection Directive.
Le Grand G and Barrau E, ‘Prior Checking, a Forerunner to Privacy Impact Assessments’ in Paul De Hert and David Wright (eds), *Privacy Impact Assessment* (Springer Netherlands 2012).
Levine Y, *Surveillance Valley: The Secret Military History of the Internet* (PublicAffairs 2018).
Lynskey O, ‘Deconstructing Data Protection: The “Added-Value” of a Right to Data Protection in the EU Legal Order’ (2014) 63 *International and Comparative Law Quarterly* 569.
——, *The Foundations of EU Data Protection Law* (Oxford University Press 2015).
Mayer-Schönberger V, ‘Generational Development of Data Protection in Europe’ in Philip E Agre and Marc Rotenberg (eds), *Technology and Privacy: the New Landscape* (MIT Press 1997).
Meldman JA, ‘Centralized Information Systems and the Legal Right to Privacy’ (1968) 52 *Marq. L. Rev.* 335.
Miller AR, ‘Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society’ (1969) 67 *Michigan Law Review* 1089.
——, ‘The Dossier Society’ [1971] *U. Ill. LF* 154.
Muir E, ‘Of Ages In-and Edges of-EU Law’ (2011) 48 *Common Market Law Review* 39.
Peter F, ‘Pure Epistemic Proceduralism’ (2008) 5 *Episteme* 33.
Porcedda MG, ‘On Boundaries – Finding the Essence of the Right to the Protection of Personal Data’ in Ronald Leenes et al (eds), *Data Protection and Privacy – The Internet of Bodies* (Hart Publishing 2018).
Poullet Y, ‘About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?’ in Serge Gutwirth, Yves Poullet and Paul De Hert (eds), *Data Protection in a Profiled World* (Springer 2010).
Prosser W, ‘Privacy’ (1960) 48 *California Law Review* 381.
Purtova N, ‘The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law’ [2018] *Law, Innovation and Technology* 1.
Quelle C, ‘Privacy, Proceduralism and Self-Regulation in Data Protection Law’ (2017) Teoria Critica della Regolazione Sociale.
Rainey B, Wicks E and Ovey C, *The European Convention on Human Rights* Bernardette Rainey, Elizabeth Wicks and Claire Ovey eds, 7th edn (Oxford University Press 2017).
Rid T, *Rise of the Machines. A Cybernetic History* (W W Norton 2016).
Rocheleau J, ‘Proceduralism’ in Deen K Chatterjee (ed), *Encyclopedia of Global Justice* (Springer Netherlands 2011).
Ruggles R, Pemberton Jr J de J and Miller AR, ‘Computers, Data Banks and Individual Privacy’ (1968) 53 *Minnesota Law Review* 211.
Solove DJ, ‘A Brief History of Information Privacy Law’, *Proskauer on Privacy, GW Law Faculty Publication & Other Works* (2006).
Tzanou M, ‘Data Protection as a Fundamental Right Next to Privacy? “Reconstructing” a Not so New Right’ (2013) 3 *International Data Privacy Law* 88.
van der Sloot B, ‘Privacy as Personality Right: Why the ECtHR’s Focus on Ulterior Interests Might Prove Indispensable in the Age of “Big Data”’ (2015) 31 *Utrecht Journal of International and European Law* 25.
Warren SD and Brandeis LD, ‘The Right to Privacy’ (1890) 4 *Harvard Law Review* 193.
Weller T, ‘The Information State An Historical Perspective on Surveillance’ in David Lyon, Kirstie Ball and Kevin D Haggerty (eds), *Routledge Handbook of Surveillance Studies* (Routledge 2012).
Westin AF, *Privacy and Freedom* (Athenaeum 1967).

---

[1] Tilburg University, TILT / TU Delft, A+BE.

[2] See Douwe Korff, ‘Comparative Summary of National Laws’ [2002] Brussels: EC Study on Implementation of Data Protection Directive.

[3] Charter of Fundamental Rights of the European Union. 26.10.2012, OJ C 326/391.

[4] See Peter Hustinx, ‘EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data

Protection Regulation' [2013] Collected Courses of the European University Institute's Academy of European Law, 24th Session on European Union Law.

[5] Gloria González Fuster, 'Curtailing a Right in Flux: Restrictions of the Right to Personal Data Protection' in Artemi Rallo Lombarte and Rosario García Mahamut (eds), *Hacia un Nuevo derecho europea de protección de datos, Towards a new European Data Protection Regime* (Tirant Lo Blanchm 2015); Maria Grazia Porcedda, 'On Boundaries – Finding the Essence of the Right to the Protection of Personal Data' in Ronald Leenes et al (eds), *Data Protection and Privacy – The Internet of Bodies* (Hart Publishing, 2018) 278.

[6] Viktor Mayer-Schönberger, 'Generational Development of Data Protection in Europe' in Philip E Agre and Marc Rotenberg (eds), *Technology and Privacy: the New Landscape* (MIT Press, 1997) 219.

[7] 'More precisely: the right to respect for private life and the right to the protection of someone's personal data': Hustinx (n 4) at 1.

[8] Hielke Hijmans, *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU* (Springer, 2016) 62.

[9] M Tzanou, 'Data Protection as a Fundamental Right next to Privacy? 'Reconstructing' a Not so New Right' (2013) 3 *International Data Privacy Law* 88.

[10] See Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193; William Prosser, 'Privacy' (1960) 48 *California Law Review* 381; Daniel J Solove, 'A Brief History of Information Privacy Law', *Proskauer on Privacy, GW Law Faculty Publication & Other Works*, *PLI* (2006).

[11] Toni Weller, 'The Information State An Historical Perspective on Surveillance' in David Lyon, Kirstie Ball and Kevin D Haggerty (eds), *Routledge Handbook of Surveillance Studies* (Routledge, 2012).

[12] Ibid.

[13] See Gordon Corera, *Intercept: The Secret History of Computers and Spies* (Hachette UK, 2015).

[14] See Thomas Rid, *Rise of the Machines. A Cybernetic History* (WW Norton 2016). See also Paul E Ceruzzi, *A History of Modern Computing* (MIT Press, 2003); Paul E Ceruzzi, *Computing: A Concise History* (MIT Press, 2012).

[15] Mayer-Schönberger (n 6) 222.

[16] Bernadette Rainey, Elizabeth Wicks and Clare Ovey, *The European Convention on Human Rights* 7th edn, (Oxford University Press, 2017) 3.

[17] Hustinx (n 4) at 2.A. See also United Nations General Assembly, Universal Declaration of Human Rights. General Assembly Resolution 217A, 10.12.1948, Art 12.

[18] Rainey, Wicks and Ovey (n 16) 400.

[19] ECHR, Art 8 – Right to respect for private and family life.

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[20] See eg Anuj C Desai, 'Wiretapping before the Wires: The Post Office and the Birth of Communications Privacy' [2007] *Stanford Law Review* 553; Solove (n 10).

[21] See Jeffrey A Meldman, 'Centralized Information Systems and the Legal Right to Privacy' (1968) 52 *Marquette v Law Review* 335; Richard Ruggles, John de J Pemberton Jr and Arthur Raphael Miller, 'Computers, Data Banks and Individual Privacy' (1968) 53 *Minnesota Law Review* 211; Arthur Raphael Miller, 'Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society' (1969) 67 *Michigan Law Review* 1089; Arthur Raphael Miller, 'The Dossier Society' [1971] *University of Illinois Law Review* 154.

[22] See Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer Law, Governance and Technology Series 2014) 28.

[23] Mayer-Schönberger (n 6) 221.

[24] Ibid at 224.

[25] Ibid at 226.

[26] Alan F Westin, *Privacy and Freedom* (Athenaeum, 1967). Westin's idea of privacy as freedom echoes in Serge Gutwirth, *Privacy and the Information Age* (Rowman & Littlefield, 2002).

[27] See Frederik Willem Hondius, *Emerging Data Protection in Europe* (North-Holland Publishing Company, 1975); Frits W Hondius, 'Data Law in Europe' (1980) 16 *Stanford Journal of International Law* 87.

[28] See Gerrit Hornung and Christoph Schnabel, 'Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination' (2009) 25 *Computer Law & Security Review* 84.

[29] Such interference can, of course, be legitimate, as data protection is a qualified right, not an absolute one. It remains, nonetheless, an interference with the right to informational self-determination, as no lawful processing ground except for consent expresses the data subject's self-determination, rather depending on the controller's will.

[30] Hustinx (n 4) s 2.D.

[31] Ibid.

[32] See OECD, Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980) C(80)58/FINAL.

[33] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. ETS No.108, Strasbourg, 28/01/1981.

[34] Ibid, Preamble.

[35] Hustinx (n 4) s 2.C. C108 – the 'mother' of the EU Data Protection Directive – is, in turn, based on the Fair Information Practice Principles (FIPPs) or Fair Information Practice (FIPs), which originated, in the 1970s, from a report from the US Department of Health, Education and Welfare – see Robert Gellman, 'Fair Information Practices: A Basic History' (2017). Available at: www.bobgellman.com/rg-docs/rg-FIPShistory.pdf. The FIPPs ended up being a 'blueprint' or 'common language' for data protection laws all over the world: Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press, 2018) 59.

[36] Convention 108, Art 1.

[37] See Yasha Levine, *Surveillance Valley: The Secret Military History of the Internet* (PublicAffairs, 2018); Rid (n 14).

[38] Commission of The European Communities, COM(90) 314 final – SYN 287 and 288, 13 September 1990.

[39] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 23.11.1995, OJ L 281/31.

[40] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. 30/01/1998, OJ L024/1, succeeded by Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). 31.07.2002, OJ L 201/37, as successively amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. 8.12.2009, OJ L 337/11; Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. 13.04.2006, OJ L 105/54; Council Framework Decision2008/877/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. 30.12.2008, OJ L350/60; Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. 12.01.2001, OJ L 8/1.

[41] DPD, Art 1.

[42] See Laima Janciute, 'Data Protection and 'Treaty-Based Games': When Fundamental Rights Are Wearing Market-Making Clothes' in Ronald Leenes et al (eds), *Data Protection and Privacy: The Age of Intelligent Machines* (Hart Publishing, 2018).

[43] Paul De Hert and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg:

Constitutionalisation in Action' in Serge Gutwirth et al (eds), *Reinventing Data Protection?* (Springer, 2009) 6.

[44] Art 6(1) Treaty on European Union (TEU).

[45] The pillars were: 1. European Communities, 2. Common Foreign and Security Policy (CFSP) and 3. Police and Judicial Co-operation in Criminal Matters (PJCCM). The last paragraph of Art 16 specifies that the rules adopted under its mandate shall be without prejudice to Art 39 TEU, which contains the mandate for laying down rules regulating personal data processing in the CFSP area.

[46] The European Communities pillar was, pre-Lisbon, the only one that had juridical personality.

[47] Article 16 TFEU states that: 'Everyone has the right to the protection of personal data concerning them' and that 'The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies and by the Member States when carrying out activities which fall within the scope of Union law and the rules relating to the free movement of such data […] subject to the control of independent authorities […] without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.'

[48] Hijmans (n 8) 4.

[49] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119/1.

[50] Paul De Hert and Vagelis Papakonstantinou, 'The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals' (2012) 28 *Computer Law & Security Review* 130.

[51] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and the free movement of such data and repealing Council Framework Decision 2008/977/JHA. OJ L 119/89.

[52] OECD, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013) [C(80)58/FINAL, as amended by C(2013)79].

[53] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) ETS No 108, as amended by Protocol CETS No 223 (C108+).

[54] The word privacy appears, in the English version of the text, only in a footnote referencing the ePrivacy Directive.

[55] GDPR, Art 1(2).

[56] Hijmans (n 8) 20; 48.

[57] For instance, the switch from the DPD's prior checking requirement to the GDPR's Data Protection Impact Assessments: see Gwendal Le Grand and Emilie Barrau, 'Prior Checking, a Forerunner to Privacy Impact Assessments' in Paul De Hert and David Wright (eds), *Privacy Impact Assessment* (Springer, 2012).

[58] Spain, Portugal and (through statutory law enjoying constitutional status) Austria: Fuster (n 22) 66 ss.

[59] I borrow the term from Raphaël Gellert and Serge Gutwirth, 'The Legal Construction of Privacy and Data Protection' (2013) 29 *Computer Law & Security Review* 522.

[60] Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press, 2015) 91; De Hert and Gutwirth (n 43) 8.

[61] See F Fabbrini, *Fundamental Rights in Europe: Challenges and Transformations in Comparative Perspective* (Oxford University Press, 2014).

[62] Member States' constitutional traditions differ between each other when it comes to conceptualizing privacy and the ECtHR's jurisprudence provides for the degree of harmony and uniformity that analysing individual Member States' constitutional jurisprudence would not provide.

[63] Lynskey (n 60) 112. The question of the horizontal effect of the right to data protection has also been tackled by Hijmans, who notes that ''an answer […] would clarify the nature of the right to data protection'': Hijmans (n 8) 61.

[64] See eg ECtHR, *Dickson v United Kingdom*, 46 EHRR 41 (2008) §70.

[65] Lynskey (n 60) 115.

[66] Ibid at 118.

[67] See Elise Muir, 'Of Ages In-and Edges of-EU Law' (2011) 48 *Common Market Law Review* 39; Michael Dougan, 'The Impact of the General Principles of Union Law upon Private Relationships' in Dorota Leczykiewicz and Stephen Weatherill (eds), *The Involvement of EU Law in Private Law Relationships* (Bloomsbury Publishing, 2013); Matteo Fornasier, 'The Impact of EU Fundamental Rights on Private Relationships: Direct or Indirect Effect?' (2015) 23 *European Review of Private Law* 29.

[68] Contra, see Hijmans (n 8).

[69] Juliane Kokott and Christoph Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 *International Data Privacy Law* 222 at 225.

[70] The ECtHR, in underlining the extensive interpretation to be given to the concept of private life with respect to personal data processing under the ECHR, has been pointing to Convention 108: see eg ECtHR, *Amann v Switzerland* (2000)30 EHRR 843, §65–67.

[71] Hustinx (n 4) s 2.D.

[72] See eg ECtHR. *Rotaru v Romania* (2000) 95 ECHR 192, §43: ''public information can fall within the scope of private life where it is systematically collected and stored''. The Court also acknowledges that permanent storage of otherwise mundane information can also bring the processing under the scope of Art 8 ECHR: ''The monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life […] On the other hand, the recording of the data and the systematic or permanent nature of the record may give rise to such considerations'' – ECtHR, *Perry v United Kingdom* (2004) 39 EHRR 3 §40.

[73] On the ECtHR's use of the reasonable expectations of privacy test, see eg ECtHR, *Halford v United Kingdom* (1997) 24 EHRR 523; *PG & JH v United Kingdom* (2001) I.X. ECtHR 195; *Peck v United Kingdom* (2003) 36 EHRR 41; Von Hannover v Germany (2005) 40 EHRR 1.

[74] GDPR, Art 4(1). On the expansive reading of the concept of personal data given by the Court, see CJEU, *Patrick Breyer v Bundesrepublik Deutschland*. Case C-582/14, 19 October 2016, ECLI:EU:C:2016:779 (on identifiability) and *Peter Nowak v Data Protection Commissioner*. Case C-434/16, 20 December 2017, ECLI:EU:C:2017:994 (on the meaning of 'relating to'), which expands on *YS and Others*. Joined Cases C-141/12 and C-372/12, 17 July 2014, ECLI:EU:C:2014:2081. See also *Bodil Lindqvist*. Case C-101/01, 6 November 2003, ECLI:EU:C:2003:596.

[75] See Art 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data WP136' (2007).

[76] GDPR, Art 4(2): 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means'. The ECtHR does, however, admit that mere storage of information is capable of interfering with the right to private life (see eg ECtHR, *Leander v Sweden* (1987) 9 EHRR 433 §48), which points toward a partial convergence between 'processing' in EU data protection law and the kinds of processing considered in the scope of Art 8 ECHR.

[77] See Lee A Bygrave, 'Information Concepts in Law: Generic Dreams and Definitional Daylight' (2015) 35 *Oxford Journal of Legal Studies* 91.

[78] CJEU, Österreichischer Rundfunk et al. Joined Cases C-465/00, C-138/01 and C-139/01, 20 May 2003, ECLI:EU:C:2003:294.

[79] Hustinx (n 4) s3.C.

[80] CJEU, Österreichischer Rundfunk et al (n 78) §68.

[81] Ibid at §74.

[82] See eg *ECtHR, Pretty v United Kingdom* (2002) 35 EHRR 1, §61; ECtHR, *Niemietz v Germany* (1992) 16 EHRR 97 §29; *Peck v United Kingdom* (2003) 36 EHRR 41 §57.

[83] See Bart van der Sloot, 'Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of 'Big Data'' (2015) 31 *Utrecht Journal of International and European Law* 25. There is, undeniably, 'a strong tendency in case law and literature to understand privacy as a broadly conceived concept of autonomy and information autonomy of the human person': Paul De Hert and Serge Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in Erik Claes, Antony Duff and Serge Gutwirth (eds), *Privacy and the Criminal Law* (Intersentia, 2006) 61.

[84] See Bert Jaap Koops et al, 'A Typology of Privacy' (2016) 38 *University of Pennsylvania Journal of International Law* 483.

[85] See eg CJEU, Österreichischer Rundfunk et al (n 78) §74, where the Court states that 'the mere recording by an employer of data by name relating to the remuneration paid to his employees cannot as such constitute an interference with private life' (while also finding that 'the communication of that data to third parties […] infringes the right of the persons concerned to respect for private life, whatever the subsequent use […] and constitutes an interference within the meaning of Article 8 of the Convention').

[86] Lynskey (n 60) 122; De Hert and Gutwirth (n 43) 24; Kokott and Sobotta (n 69).

[87] De Hert and Gutwirth (n 43) 26.

[88] Hijmans (n 8) 42.

[89] Ibid at 47.

[90] Ibid.

[91] See Lynskey (n 60) 127. Concrete examples are the right to data portability or the right not to be subject to automated decision making.

[92] GDPR, Art 20.

[93] Janciute (n 42).

[94] See De Hert and Gutwirth (n 83).

[95] Ibid at 3 and 4.

[96] Ibid at 4.3.

[97] Ibid at 3.2.

[98] 'The sheer wordings of the data protection principles […] already suggest heavy reliance on notions of procedural justice rather than normative (or substantive) justice': De Hert and Gutwirth (n 83) at 4.2.

[99] Norberto Nuno Gomes de Andrade, 'Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights' in Simone Fischer-Hübner et al (eds), *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life* (Springer, 2010) 96.

[100] 'Article 8 of the Convention is no place for procedural questions. The framers of the Convention have designed other articles for that purpose. The transformation of Article 8 into a source of procedural rights and procedural conditions takes it away from the job it was designed for, viz. to prohibit unreasonable exercises of power and to create zones of opacity': De Hert and Gutwirth (n 83) at 5.4.

[101] See de Andrade (n 99); De Hert and Gutwirth (n 83); De Hert and Gutwirth (n 43); Claudia Quelle, 'Privacy, Proceduralism and Self-Regulation in Data Protection Law' (2017) 1 *Teoria Critica della Regolazione Sociale* 89.

[102] de Andrade (n 99) 97.

[103] Hustinx (n 4) s 4.B.

[104] Yves Poullet, 'About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?' in Serge Gutwirth, Yves Poullet and Paul De Hert (eds), *Data Protection in a Profiled World* (Springer, 2010).

[105] See Gloria González Fuster and Serge Gutwirth, 'Opening up Personal Data Protection: A Conceptual Controversy' (2013) 29 *Computer Law & Security Review* 531; Gloria González Fuster and Raphaël Gellert, 'The Fundamental Right of Data Protection in the European Union: In Search of an Uncharted Right' (2012) 26 *International Review of Law, Computers & Technology* 73.

[106] In other words: is the processing of personal data an interference with the right to personal data protection in itself, to be legitimated through Arts 8(2) and 52 CFR, or does the processing of personal data become a compression of the right to data protection only when the conditions under Art 8(2) are not met and the conditions legitimising an interference are to be found only in Art 52?

[107] 'Everyone has the right to respect for his private and family life, his home and his correspondence' – Art 8(1) ECHR.

[108] 'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of

the rights and freedoms of others' – Art 8(2) ECHR.

109 Fuster and Gutwirth (n 105) 535.

110 Ibid.

111 Ibid.

112 Hustinx (n 4) s 2.C.

113 Ibid at s 4.B.

114 The CJEU's jurisprudence is however admittedly inconclusive in this respect and sometimes seems to frame personal data processing as an interference with the right in itself, justifiable through Art 8(2) and 52(1) CFR: see eg CJEU, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*. Joined Cases C-293/12 and C-594/12, 8 April 2014, ECLI:EU:C:2014:238, §21, 36.

115 On the elusive content of the fairness principle see Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness' (2018) 37 *Yearbook of European Law* 130–187.

116 See Peter Hustinx, 'The Role of Data Protection Authorities' in Serge Gutwirth et al (eds), *Reinventing Data Protection?* (Springer 2009); Hijmans (n 8) 325.

117 See Fuster (n 22).

118 Hijmans (n 8) 48.

119 De Hert and Gutwirth (n 83); De Hert and Gutwirth (n 43).

120 Opinion of AG Alber in Case C-369/98 *The Queen v Minister of Agriculture, Fisheries and Food, ex parte Trevor Robert Fisher and Penny Fisher*, §41; Fuster and Gutwirth (n 105) 537. As Hustinx also stated, 'The concept of "data protection" was developed […] to provide legal protection to individuals against the inappropriate use of information technology for processing information relating to them. It was not designed to prevent the processing of such information or to limit the use of information technology per se. Instead, it was designed to provide safeguards whenever information technology would be used for processing information relating to individuals': Hustinx (n 4) s 1.

121 See de Andrade (n 99); Hijmans (n 8).

122 See Fuster and Gellert (n 105); Fuster and Gutwirth (n 105).

123 Hustinx (n 4) s 4.B.

124 Charter, Art 8(2).

125 Ibid at Art 8(3).

126 Lynskey (n 60) 15. Lynskey identifies an additional characteristic of *omnibus* regimes: the supervision by an independent authority.

127 See Maja Brkan, 'The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors?' (2016) 23 *Maastricht Journal of European and Comparative Law* 812; Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' [2018] *Law, Innovation and Technology* 1.

128 De Hert and Gutwirth (n 43); De Hert and Gutwirth (n 83).

129 de Andrade (n 99).

130 Fuster and Gellert (n 105); Fuster and Gutwirth (n 105).

131 Jordy Rocheleau, 'Proceduralism' in Deen K Chatterjee (ed), *Encyclopedia of Global Justice* (Springer Netherlands, 2011).

132 Rocheleau (n 131) 906.

133 However, the dichotomy between proceduralism and epistemic theories is not the only way to conceive proceduralism and can be surpassed by coupling 'a concern with democratic procedures with a concern with the epistemic quality of outcomes': Fabienne Peter, 'Pure Epistemic Proceduralism' (2008) 5 *Episteme* 33. In other words, the idea that the legitimacy of a set of rules, decisions and institutions can derive from the validity of the process from which they originate does not exclude an epistemic approach to the determination of what a valid process is. Such 'epistemic proceduralism' frames institutional legitimacy as deriving from the validity of the underlying democratic processes and the validity of those processes through their epistemic value: their truth- and knowledge-seeking potential, however defined in the context of

reference.

134 The term ‘proceduralism’ has been previously used in connection with EU data protection law by Quelle, albeit with a different connotation – Quelle’s paper uses the term to describe the eminently procedural character of data protection: Quelle (n 101).

135 This chapter uses ‘collective’, ‘societal’ and equivalent wording under the assumption that the mechanisms of (representative) democracy allow the expression of an underlying shared posture towards certain issues, in this case personal data processing.

136 De Hert and Gutwirth (n 43) 3.

137 Ie its peculiar connection with technological development and the relation it has with the preceding secondary legislation.

138 Hijmans, similarly, defines data protection as ‘the rules of the game’, a system of checks and balances based on a claim to fairness: see Hijmans (n 8) 59 ss. See also Christopher Docksey, ‘Articles 7 and 8 of the EU Charter: Two Distinct Fundamental Rights’ in Alain Grosjean (ed), *Enjeux européens et mondiaux de la protection des données personelles* (Éd Larcier 2015); Hustinx (n 4).

139 CJEU, *Maximillian Schrems v Data Protection Commissioner*. Case C-362/14, 6 October 2015, ECLI:EU:C:2015:650, §41.

140 Ibid at §94.

141 Ibid at §95.

142 Porcedda (n 5) 283.

143 Ibid.

144 Gellert and Gutwirth seem to contest the very fact that the rights to privacy and data protection have an essence (Gellert and Gutwirth (n 46)); that position does not however seem to be sustainable anymore, as the CJEU explicitly confirmed the existence of the essence of both rights in *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* (n 114) §§39–40.

145 Fuster and Gellert (n 105); Hustinx (n 4) s4.D. Examples in case law are, eg CJEU, *Schecke and Eifert.* Joined Cases C-92/09 and C-93/09, 9 November 2010, ECLI:EU:C:2010:662 and *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* (n 114) §39.

146 See eg Orla Lynskey, ‘Deconstructing Data Protection: The “Added-Value” of a Right to Data Protection in the EU Legal Order’ (2014) 63 *International and Comparative Law Quarterly* 569; Fuster and Gutwirth (n 105); Fuster and Gellert (n 105); Tzanou (n 9).

147 Charter, Art 52(1): ‘Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect *the essence of those rights and freedoms*’ (italics added).

148 On the multi-level structure of the European fundamental rights’ framework, see Fabbrini (n 61).

149 Maja Brkan, ‘The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to Its Core’ [2018] *European Constitutional Law Review* 1, 338.

150 Ibid at 332. In the *Digital Rights Ireland case* (n 114) §39), for instance, the CJEU differentiates between a serious interference with the right to privacy and an interference with its core: ‘So far as concerns the essence of the fundamental right to privacy […] it must be held that, even though the retention of data required by Directive 2006/24 constitutes a particularly serious interference […] it is not such as to adversely affect the essence of those rights given that […] the directive does not permit the acquisition of knowledge of the content.’

151 See eg Robert Alexy, *A Theory of Constitutional Rights* (Oxford University Press, 2009).

152 See eg Jürgen Habermas, *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy*, 2nd edn, (MIT Press, 1996).

153 Brkan (n 149) 359.

154 While this chapter does not mean to participate to such a debate, it does implicitly adhere to an absolute approach, where an infringement of the essence of the right cannot be justified through proportionality balancing.

155 See Jeanne Pia Mifsud Bonnici, ‘Exploring the Non-Absolute Nature of the Right to Data Protection’ (2014) 28 *International Review of Law, Computers & Technology* 131.

156 Brkan (n 149) 363.

157 An objective interference with the essence results in the right being excessively restricted for all right holders, a subjective interference threatens the existence of the right for a particular right holder or group of right holders: Brkan (n 149) 350.

158 Brkan (n 149) 349 ss. Aside from objective and subjective interferences with the essence, the author also identifies absolute interferences with the essence when an absolute right is compressed. In a way, every compression of an absolute right is a compression of the essence of the right.

159 As Brkan points out, following an absolute/exclusive approach to the concept of essence of fundamental rights, the existence of overriding reasons through which the interference can be justified means that the interference does not compress the right's essence, as proportionality balancing (ie overriding reasons) and interferences upon the essence of a right are mutually exclusive concepts: Brkan (n 149) 364.

160 See Bonnici (n 155).

161 See CJEU, *Digital Rights Ireland Ltd* (n 114) §40: 'Nor is that retention of data such as to adversely affect the essence of the fundamental right to the protection of personal data enshrined in Article 8 of the Charter, because […] Directive 2006/24 provides […] that […] certain principles of data protection and data security must be respected'.

162 See, for instance, CJEU, Opinion 1/15 of the Court (Grand Chamber). 26 July 2017, ECLI:EU:C:2017:592, §150, where the Court considers that 'As for the essence of the right to the protection of personal data, enshrined in Article 8 of the Charter, the envisaged agreement limits […] the purposes for which PNR data may be processed and lays down […] rules intended to ensure, inter alia, the security, confidentiality and integrity of that data and to protect it against unlawful access and processing.' The CJEU appears to hold that the presence of a set of rules (some of which it lists, while keeping the list non-exhaustive by inserting the 'inter alia' syntagm) is enough to avoid the configuration of a breach of the essence of Art 8 CFR. The set of rules listed by the Court should not be read as a mere list of essential data protection principles, but rather as an indication that the compression of individuals' right to data protection deriving from the PNR (Passenger Name Record) data sharing does not threaten the functioning of data protection's system of checks and balances as a whole, as there still are 'rules intended to ensure, inter alia, the security, confidentiality and integrity of that data'.

163 Particularly regarding the lawfulness principle.

164 Porcedda (n 5).

165 Ibid at 289. The attributes identified by Porcedda are (1) legitimate processing, (2) oversight, (3) supervisory authority, (4) human intervention, (5), data subjects' rights, and (6) security and minimisation – see Porcedda (n 5) 310.

166 I.e. EU primary and secondary law, post-Charter CJEU jurisprudence, ECtHR jurisprudence in light of Convention 108, doctrine and the Fair Information Processing Principles (FIPPs).

167 Wording used in CJEU, *Maximillian Schrems v Data Protection Commissioner* (n 139) §41.

168 Porcedda (n 5) 310. The essences identified in the CJEU's jurisprudence and the ones proposed by Porcedda are purpose limitation, ex-post supervision, human intervention, a mixture of data subjects' rights (access, rectification, right to object) and the provision of security safeguards.

169 Again, framing data protection as a collective and shared social stance moves from the assumption of the legitimacy of the underlying democratic decision-making processes.

3

What's in an Icon?

Promises and Pitfalls of Data Protection Iconography

ARIANNA ROSSI[1] **AND MONICA PALMIRANI**[2]

Abstract

Under the General Data Protection Regulation (GDPR), transparency of information becomes an obligation aimed at creating an ecosystem where data subjects understand and control what happens to their personal data. The definition of transparency stresses its user-centric nature, while design considerations to comply with this obligation assume central importance. This chapter focuses on the icons established by the GDPR Article 12.7 to offer 'a meaningful overview of the intended processing'. Existing attempts to represent data protection through icons have not met widespread adoption and reasons for the strengths and weaknesses of their creation and evaluation are discussed here. Building on this analysis, we present an empirical research proposing a new icon set that responds to GDPR requirements. The chapter also discusses the challenges of creating and evaluating such icon set and provides some future directions of research for effective implementation and standardisation.

Keywords

GDPR, icons, data protection, legal design, semantic web, transparency.

I. Introduction

Information duties are a cornerstone of European data protection law[3] and are commonly realised through the regulatory tool of mandated disclosures: privacy terms both inform the data subjects about how data controllers will use and protect their personal information and about their rights. The underlying rationale postulates that the establishment of full transparency facilitates individuals with the decision about the permissible use of their personal data.[4]

Notwithstanding the historical, philosophical, legal and economic reasons supporting mandated disclosure, research[5] and anecdotal evidence show that privacy policies are

ineffective at informing individuals.[6] 'Most individuals simply do not read the [privacy] terms, and even if they did, most individuals have difficulty fully comprehending what they actually agreed to and the risk they inherited by that consent.'[7] It is frequently assumed that individuals do not care about their privacy[8] and they take the conscious decision of ignoring the legal terms at their own risk.[9] Yet, self-reported data indicate the opposite: they wish to be informed, but concrete obstacles hamper them.[10] Moreover, individuals are not able to base their decisions on full information disclosure and this effect grows stronger the less understandable the information and the less experienced the individuals in the domain.[11]

There are reasons of two orders behind non-readership: some generally concern the characteristics of human reasoning and decision-making,[12] while others are external and pertain to the quality of privacy policies. In this article, only the latter are addressed, by adopting an interdisciplinary perspective that crosses legal information design, semiotics, usable privacy research, user research and legal informatics. The rest of the chapter describes the motivation and the development of a research project that led to the creation of DaPIS, an ontology-based icon set representing core notions of data protection and aimed at enhancing the transparency of the information on data processing provided to individuals, as established by the General Data Protection Regulation.[13]

The main research questions motivating the DaPIS project were:

RQ1: What are the reasons why data subjects disregard the legally binding terms describing how their personal data will be processed?

RQ2: What are the requirements introduced by the GDPR's transparency obligations, especially for what concerns nonverbal communication?

RQ3: Which existing technologies can be used to create machine-readable visual structure and visualisations of legal documents?

RQ4: What idiosyncratic features have icons with respect to other kinds of graphical means and how do they impact ease of interpretation?

RQ5: What is the function and context of use of data protection icons?

RQ6: Given that an icon set is created, which icons 'work' best and why?

This chapter is organised as follows: section II provides a brief literature review of the documented problems that prevent privacy policies from being useful informative instruments for the data subject. Section III illustrates the novel requirements about the quality of information introduced by the GDPR, meant to implement transparency in a way that can respond to the above limitations. The thematic focus of this chapter lies on the machine-readable icons envisioned in Article 12.7 GDPR and, hence, the following sections tie together two strands of literature. Section IV provides a short overview of the technologies and standards currently used for the management and (semi-)automated extraction of information from legal documents, whilst section V introduces iconographical considerations, with a focus on the legal domain, and describes past attempts to create icons for the data protection domain. Section VI relies on both lines of research to present the

rationale, the design process and the outcomes of an interdisciplinary project that culminated in the creation of DaPIS. Finally, section VII details possible future directions of research, while section VIII takes stock of the lessons learned during the research described in the next pages.

II. Limitations of Privacy Policies: A Brief Literature Review

Privacy policies have long been criticised for a series of reasons[14] and have been defined as 'that dense, unreadable, boilerplate text tucked away in some corner of practically every website and application on the Internet'.[15] The communication about data practices is mainly drafted by lawyers for lawyers[16] and merely aims to fulfil the legal requirement of mandated disclosure.[17] This reality sharply contrasts with the stated objective, ie effectively inform data subjects about the collection and processing of their personal data and empower them to exercise their rights.[18] Studies show that privacy policies go beyond the understanding of the average internet user,[19] while their extreme length[20] causes information overload[21] and discourages reading.[22] Besides, privacy terms are frequently expressed in vague language,[23] leaving individuals puzzled about their intended meaning.[24]

Whereas attempts to simplify unnecessary language complexity are gaining acceptance and support,[25] whether legal information is displayed intelligibly is too often disregarded:[26] privacy notices are often presented as a visually undifferentiated 'wall of text'[27] that is 'impenetrable'[28] to the human eye. The absence of any information structure[29] in the text hinders comprehension and weakens intellectual performance.[30] Indeed, people do not read privacy policies word for word, but rather skim their text to find relevant information to answer their questions or to compare two services' practices.[31] Therefore, the presence of structural elements can guide readers towards the most relevant parts of the document (ie attention hierarchy).

Another critical dimension for disclosures to be used as decision-making tools is timing. Much legislation, such as the GDPR, requires data controllers to disclose information at the moment of collection (Article 13). However, if users are engaged in a different activity, the notice is experienced as a nuisance[32] rather than as a useful privacy tool, thus causing individuals to deliberately ignore it.[33]

III. The End or a New Era for Mandated Disclosures?

Given that privacy policies are rarely read and poorly understood, while consent is rarely

genuinely informed, the tool of mandated disclosure has attracted fierce criticism. Some scholars have reached the conclusion that information paradigm as regulatory tool has failed[34] and must therefore be abandoned. Solutions that enhance transparency are criticised because language simplification or similar interventions alone cannot solve the non-reading problem.[35]

Nevertheless, two main arguments can be proposed against the abandonment of privacy disclosures. Firstly, two-thirds of all legislation are still based on the information paradigm.[36] The GDPR is no exception. Secondly, the quality of disclosures shows extensive room for improvement. Encouraging results from a growing body of literature on good legal information design[37] and research on usable privacy,[38] both from Europe and US,[39] suggest that it is worth attempting to change the *status quo* for the better.

Opportunely, under the GDPR, a revolutionary shift has occurred: the quality, accessibility and comprehensibility of the information describing data practices[40] assume an unprecedented importance to demonstrate compliance.[41] Although plain and clear language has been advocated for years,[42] it is only with the GDPR that this requirement becomes prominent.[43] The specificity of the intended audience and the characteristics of human cognition must be taken into account to provide effective disclosures: '[t]he concept of transparency in the GDPR is user-centric rather than legalistic'[44] specifies the Article 29 Data Protection Working Party.[45] Communications cannot be addressed to abstract data subjects, but should rather be tailored to specific users in specific contexts.[46]

The unprecedented acknowledgement in the law of the potential of visualisations[47] to achieve transparency of information must be understood within this novel attention to user-centred communication. To reduce excessive amounts of written information,[48] Article 12.7 of the GDPR provides for the presentation of information in combination with machine-readable, standardised icons to give 'in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing'. Namely, the icons should be easily noticeable (ie visible), comprehensible (ie intelligible) and composed by recognisable elements (ie legible). Yet, it is harder to define exactly what 'a meaningful overview' might mean and translate it into concrete design requirements, while the standardisation process raises open questions. This chapter attempts to provide some preliminary answers to such doubts. Although eventually it will be the role of the European Commission to give directions on the creation of the icons, the need for expert advice is emphasised both in the GDPR[49] and WP29, which have encouraged an 'evidence-based approach' and 'extensive research'[50] to inform the development and application of the icons and determine their efficacy.[51]

The research described in the following intends to contribute to establishing the foundations for further research in the domain. The GDPR's incentive to machine-readable icons identifies two parallel and intertwined lines of research: the first direction is related to the technologies for the management and (semi-)automated extraction of legal information (see section IV), whilst the second is linked to legal visualisations and the user-centric design of legal information (see section V). Whereas the latter eases humans' understanding, the

former ameliorates machines' accessibility to legal information.[52] The final aim is the transformation of legal documents into formats that are easily understood by both humans and machines.[53]

IV. Machine-Readable Legal Information

Although the term 'machine-readable' does not figure among the definitions in the GDPR, it can be explained as 'a file format structured so that software applications can easily identify, recognise and extract specific data, including individual statements of fact, and their internal structure'.[54] It is from this definition and the extensive research area on semantic web technologies for the legal domain that the project presented in these pages has originated.

Legal documents can be enriched with machine-readable specifications that enable semantic reasoners to extract meaning from the text and apply inference rules:[55] XML[56] mark-up is used to embed meta-textual information into the legal document, complemented by languages (eg OWL)[57] which define conceptual structures pertaining to a certain domain knowledge. Hence, the concepts of a specific domain (eg EU data protection law) can be formally codified in an ontology,[58] which can assign machine-readable semantic meaning to the legal terms of a certain document.

With such architecture, it is therefore possible to operate concept mining on large quantities of privacy policies and to embed the machine-readable specifications into the legal terms either during or after the drafting. The XML encoding allows for a structured, semantically enriched layout: ideally, each section of a privacy policy provides details about a certain topic (eg purposes of data processing, place of storage of data, etc). Such information can be leveraged to improve the document architecture (ie structure it through elements that convey hierarchy of information and thereby ameliorate the ease of reading). The machine-readable specifications can be leveraged to adapt the display of information on multiple layers and thereby accommodate the informative needs of different audiences. For instance, whereas supervisory authorities need access to the entire notice, data subjects might find it more meaningful to only be shown the first layer of a layered notice.[59]

The project illustrated in the following sections is based on the idea that the concepts that are formally represented in the ontology can be linked to their linguistic realisation in the privacy notice and to their corresponding icons, thus creating a network of machine-readable and visual representations.[60] This only has the function of fulfilling the GDPR requirement of machine-readable icons, but also allows for the semi-automatic retrieval and display of the visualisations encoded in the ontology, once that the semantic expressions in natural language of the text have been associated to their corresponding ontological representations through the XML mark-up. Thus, semantically enriched privacy policies can be leveraged to generate a user-friendly visual layer composed of structured layout and iconographical elements that can ease the navigation, comprehension and comparability of these documents.[61]

The data protection icon set that will be described in the next section was modelled on a

selection of conceptual modules formalised in PrOnto[62] (Privacy Ontology). The icon set visualises fundamental aspects of data processing regulated by the GDPR (especially those information items mandated by Articles 13–14): data (eg personal data, sensitive data) and documents (eg consent, privacy policy), agents and roles (eg data subject, data controller, supervisory authority), data processing workflow (eg anonymise, encrypt, transfer), processing purposes (eg scientific purposes, marketing purposes), legal bases (eg legal obligation, consent, legitimate interest) and data subjects' rights (eg right to access, right to erasure).[63]

V. On the Nature of (Data Protection) Icons

Once a set of concepts was identified through the analysis of the legal requirements and the formal conceptualisation described in the previous sections, principles drawn from ergonomics, semiotics and Legal Design[64] provided the methodological framework for the creation and evaluation of DaPIS (Data Protection Icon Set). The following paragraphs will introduce a few necessary considerations on iconography, illustrate previous attempts to build an iconic language for the data protection domain and propose a function for the icons envisioned in Article 12.7. Such observations have been instrumental for the creation of DaPIS.

A. Semiotics and Iconography

Icons are attractive non-verbal means of communication because they can be easily recognised, processed and memorised and can serve as cognitive support for the classification of content.[65] Although it is commonly assumed that icons communicate quickly, concisely and across linguistic and cultural differences,[66] in fact their interpretability depends on a variety of factors. Familiarity is a crucial dimension for ease of recognition and it comprises both previous experience with the graphical symbol and knowledge of the symbol's underlying concept.[67] Semantic transparency is also a critical factor:[68] icons depicting objects (ie resemblance icons) are more easily interpreted than arbitrary icons,[69] whose meaning must be learned rather than deduced.[70] Moreover, the function assigned to a graphical symbol by its designer can be different from the meaning attributed to it in practice (ie there can be misalignments between the designers' intentions and the sense-making activity of the user). Complexity (ie the amount of icon's details, influences search activity).[71] Finally, when creating a set of icons, attention should be devoted both to the degree of discriminability of one icon from the others of the set and to the coherence across the elements of the set.[72]

B. The Specificity of Icons for Legal and Data Protection Matters

Since familiarity is a critical dimension to determine ease of interpretation, it is good practice in icon design to rely on established visual conventions.[73] However, only a few symbols exist for legal matters[74] (most notably the scale and the gavel), while in data protection only a few cybersecurity symbols are well-known (ie the shield and the padlock).[75] However, the widespread use of graphical user interfaces has favoured the creation of common mental references between a number of icons and their function (e.g. a pencil for the edit function, a bin for the cancel function, a user silhouette for the profile page on social medias, etc.).

Lack of familiarity with the icon's underlying legal concept (eg encryption) must also be taken into consideration to determine the efficacy of graphical symbols: only less arbitrary icons can be explanatory and reveal unknown meanings. An additional difficulty is posed by the fact that legal concepts are usually abstract in nature, thus difficult to depict. Such characteristics also challenge standard icon evaluation methods,[76] which are mainly suited to determine the comprehensibility of graphical symbols whose referent is known to the interpreter. Differences of comprehension rates among icons also depend on the person who interprets them (ie her culture, age, expertise, etc). Finally, researchers underline the importance of the provision of contextual cues which mirror the actual usage situation of the icons (ie ecological validity) to support the sense-making process of individuals.[77] These observations have demonstrated that establishing universally comprehensible icons is far from straightforward.

C. Lessons Drawn from Existing Data Protection Icon Sets

Some attempts to design and evaluate icons for privacy and data protection have been made[78] and vary deeply[79] (eg whether they represent a legal assessment of a certain data processing practice, or as whether they have undergone any comprehensibility evaluation). The PrimeLife project[80] is notably the most structured attempt to design and evaluate icons for data protection in the European context.

However, most of the icons created during such project were discarded based on the results of two user studies[81] and on founded fears of information overload derived by a too-high number of icons. The evaluation importantly highlighted how visual vocabulary depends on culture, therefore calling for intercultural user audiences, while it also suggested that simplification of the elements and uniformity of the design styles are critical. Nevertheless, it is not entirely clear to what extent the context of use of the icons was shown to the participants to support their interpretation. Furthermore, it could have been acknowledged that those icons that were less easily recognised (eg anonymisation, user tracking, etc.) depict less familiar and concrete concepts than those that were considered 'intuitive and easy to understand'[82] (eg medical data, deletion, etc.). Since context, concreteness and familiarity are key, as argued earlier, it cannot be expected that all symbols can be interpreted with the same ease, regardless of these dimensions.

One of the unique attempts to consider, during their conception and design, the context where the icons would appear is represented by the table included in the 2013's Draft report

of the LIBE Committee on the Regulation proposal.[83] Such table contains six icons *vis-à-vis* their verbal explanation. In this case, however, it is the prescriptive character of the specific context (ie the table) that limits their possible use (eg on small screens), thus constituting a drawback rather than a support for successful implementation. A user study[84] highlighted how the convoluted combination of symbols in the various table columns hindered the comprehension of the icons' meaning. Even such a study, however, has limited ecological validity, because it investigated the icons' meaning in isolation, even though they were explicitly designed to appear next to their textual explanations.

D. Context of Use and Function of the Data Protection Icon Set

To orientate the design of the icon set, a reflection on the envisaged context of use and the ensuing function of the icons appears to be crucial. They are meant to appear in combination with text and provide a meaningful overview of the intended processing – but neither the GDPR nor WP29 have further specified the goal and the context of implementation of the icons. Thus, many questions remain open, starting from defining 'meaningful' and translating the definition into functional requirements, especially considering that what is meaningful for one user might not be meaningful for another. Besides, it is unclear what function the icons should assume and whether it should be the same throughout the different layers of privacy policies, in consent requests, in privacy dashboards, etc. (ie in all those cases when information about the processing must be presented to the data subject).

Similarly to the Primelife project's final recommendations,[85] we also share the belief that, to reach global acceptance, icons should have a headline function, rather than making a statement about the fairness or riskiness of processing. It can be argued that it would be more meaningful to provide individuals (data subjects and supervisory authorities alike) with an obvious visual summary of the risky or unlawful practices conducted on personal data, to support their decision-making (eg whether to use a certain service or head elsewhere).[86] However, it can be challenging to determine *a priori* criteria to take a decision about the lawfulness or the riskiness of certain practices outside a specific context.[87] Moreover, the adoption of icons that clearly illustrate whether the data practices of an organisation are lawful might be opposed by many data controllers, since the GDPR does not impose such an obligation upon them. This solution would appear more realistic if the role of assigning such icons to the data processing practices of a certain organisation was played by a third party, such as auditors or consumer associations.

Although such solutions might be promising and could be investigated in future studies, in the present research, graphical symbols do not provide a judgement on the lawfulness or the riskiness of processing practices and leave to the individuals the freedom to evaluate for themselves whether a certain organisation's data practices satisfy their privacy expectations. Besides, depicting single concepts, instead of statements about concepts, is the most suitable integration with an ontological formalisation of legal knowledge.

For such reasons, DaPIS envisions graphical symbols as 'companion icons' (ie icons that represent the meaning or the function of the text section they accompany).[88] In this view,

they act as information markers in documents to support text navigation, information finding and memorisation (see Figure 3.1). The motivation supporting this functional choice lies in the fact that legal icons have limited self-explanatory nature. When they convey abstract meanings, such as data practices, they might not be universally understood if they are not accompanied by some sort of textual explanation.[89] Moreover, this type of visual element cannot convey subtle and nuanced meanings:[90] they can rather give salience to certain elements that would be otherwise lost in lengthy and undifferentiated texts. This is why it is wrong to expect that these tiny graphical elements can and will substitute the legal text completely, as it is sometimes feared.[91] However, they can accompany the text to enhance the effectiveness of communication by combining verbal and nonverbal elements. In this context, icons help readers to skim the document, identify information quickly and efficiently, and even compare it across separate documents. As the icons' use spread in a coherent way across more organisations, they will become more and more recognisable.

Although the icons are not meant to appear in isolation, it is fundamental to evaluate their ability to convey the correct meaning. This matter has great relevance if individuals take legally binding decisions based on the visualisations, such as entering into a contract with a service provider or giving consent to certain data practices. Misunderstanding the icons or oversimplification of privacy terms might cause liability issues.[92] Usability tests on existing data protection icons[93] show that 'critical confusions',[94] namely interpretations opposite to the intended meaning, are possible due to multiple reasons: misalignment between designers' intentions and users' expectations on the icon meaning and differences in individuals' level of education, age and cultural background. This is why user-centric methods, drawn from design principles, can be necessarily applied.

Figure 3.1 A possible 'visual layer' for the Blablacar privacy policy's section about data subjects' rights, with visual structure and companion icons accompanying the different paragraphs. The original text of the document was not changed



What are your rights in respect of your personal data?

Your right of data access



8.1. You are entitled to receive a copy of your personal data that is in our possession (your right of data access).

Your right to erasure and rectification



8.2 You may request the deletion of personal data or the correction of inaccurate personal data (your right to erasure and rectification). Please note that we may keep certain information concerning you, as required by law, or when we have a legal basis to do so (e.g., our legitimate interest to keep the platform safe and secure for other users).

Your right to object to processing



8.3 You have the right to object at any time (i) to the processing of your personal data for the purpose of direct marketing, or (ii) to the processing of your personal data for other purposes on grounds relating to your particular situation (your right to object to processing). Please note that in the latter case, this right only applies if the processing of your personal data is based on our legitimate interest.

Your right to restriction to processing



8.4 You have the right to restrict the processing of your personal data (your right to restriction of processing). Please note that this only applies if (i) you contested the accuracy of your personal data and we are verifying the accuracy of the personal data, (ii) you exercised your right to object and we are still considering, as foreseen by the applicable law, whether our legitimate grounds to process your personal data in that case override your interests, rights and freedoms; or (iii) your personal data has been processed by us in an unlawful way but you either oppose the erasure of the personal data or want us to keep your personal data in order to establish, exercise or defend a legal claim.

Your right to data portability



8.5 You have the right to receive and/or have us transfer to another data controller a subset of personal data, that concern you and that you provided us with, and which we process for the performance of our contract or because you previously consented to it, in a structured, commonly used and machine-readable format (your right to data portability).

Data Protection Officer

8.6 To exercise your rights, please contact the Group Data Protection Officer (see under Article 13).

Your right to make a complaint to the relevant data protection authority



8.7. You also have the right to make a complaint to the relevant data protection supervisory authority or to seek a remedy through the courts if you believe that your rights have been breached.

E. Legal Design

Following its human-centred nature, Legal Design assumes that the 'users of the law'[95] are not only legal experts, but also laypeople. Therefore, when useful for its goals, it favours participatory design methods:[96] the design process starts from an analysis of the needs and abilities of the intended users of an artefact (ie the icons and the privacy policies) that are involved at every stage of the design, from the conceptual phase until the evaluation. One of the legal design research areas focuses on graphic communication tools,[97] but does not aspire to become a prescriptive theory that generates 'a single 'right' […] image or layout'.[98] Rather, it can be conceived as a creative and iterative process which provides indications about the chances of suitable use of a certain element (eg a visualisation, given information type and goal of the design). Multi-stakeholder collaborations are encouraged since they leverage the multiple skills and knowledge of the different stakeholders involved; this reciprocal understanding reduces the chances of personal bias.[99]

VI. Design and Evaluation of DaPIS

A. Methodology for the Design of DaPIS

For the creation of DaPIS, a series of design workshops were held in July 2017, March 2018 and July 2018[100] and followed the (legal) design cycle.[101] The risk of misalignments between designers' intentions and the sense-making activity of individuals orientated the research towards participatory design methods for the creation of the icon set. Interdisciplinarity was a critical element: academics and professionals with legal and technical backgrounds interpreted, explained and exemplified the data protection concepts to the other participants; graphic designers and other professionals from visual disciplines contributed with techniques and tools to produce functional visualisations for the intended audience and the intended medium; lastly, laypeople added non-expert views and knowledge to the design process (eg about the visual conventions with which they were familiar).

The systematic formalisation of knowledge described in section IV provided the conceptual framework for the creation of the visualisations. The existing visual vocabulary for technical, legal and data protection matters (see section V.B.) was re-adapted to a certain extent, but was revealed as insufficient: for many concepts, new symbols had to be created. The design followed iterative cycles: during each workshop, initial icon prototypes were proposed, discussed and refined in subsequent phases, so that feedback from other participants, but also from externals, was collected at every stage of the design. In this way, the shortcomings and strengths of the proposed ideas were identified before the actual creation of high-fidelity icons and chances of failure at later stages (eg during the evaluation phase) were minimised.

Not only did each workshop follow an iterative cycle, but iterative was also the design cycle overall: whereas the first design workshop explored the best suited visual means to render complex data protection notions, subsequent workshops focused on more specific aspects related to the usability of the graphical symbols, harmonising the design style of the set and the digital rendering of the prototypes. Furthermore, three user studies,[102] each following one of these phases, were conducted to determine the comprehensibility and legibility of the icons. Based on the results after each user study, icons were vetted and refined in the subsequent workshops and further evaluated if necessary.

Given the previous research on graphical symbols, it was not surprising that concepts with a higher degree of concreteness (eg 'contract'), for which an exemplification could be easily provided (eg 'research purposes'), or that could rely on established visual convention (eg the bin to signify erasure in the 'right to erasure' icon) were more quickly and effortlessly visualised by the participants. Conversely, abstract or general concepts such as 'rights', 'processing purposes', 'service enhancement' and 'service provision' were the object of thoughtful consideration and even intense debate. Decisions that appeared arbitrary to some group members had eventually to be taken.

One of the major challenges that repeatedly emerged during the workshops was represented by the striking of a tentative balance among the priorities of the different stakeholders. On the one hand, legal experts warned of the existing risks of oversimplification in the visualisation of data protection concepts. On the other hand, icons containing few details had to be preferred to achieve ease of recognition and allow icons' usability in multiple contexts (ie small screens).

The participants were explicitly made aware that they should pay attention to balancing the simplicity of representation, the distinctiveness of the icons and the coherence of the elements across the icon set.[103] For instance, an upward-facing hand was chosen to indicate the class of data subjects' rights. The metaphor underlying the hand represents the concept of being in control of the element located above it. This palm recurs in every data subject's right as common denominator (ie the root) among concepts belonging to the same class, but the meaning of the icon as a whole is specified by the element held by the hand (ie the determinant): eg a bin for the right to erasure, a pencil for the right to rectification, etc (see Figure 3.2a).

B. Methodology for the Evaluation of DaPIS

Evaluation of the icons is crucial, given that the goal is EU standardisation. However, as illustrated in Section V.C., only very few assessments have been carried out on data protection icon sets and even those show their limitations. That said, there is no good standard evaluation method that can be proposed for this specific context without any vetting, since legal icons have the peculiar characteristics explored in section V.B. In this research, we have proposed an evaluation methodology which follows a two-step approach.[104] Firstly, icons are evaluated as stand-alone elements (ie according to classical dimensions such as comprehensibility and legibility). Secondly, a complementary evaluation concerns the extent

to which the icons can indicate the desired function in context (ie whether they support the navigation through large amounts of information and increase speed and accuracy of comprehension). This chapter only covers the first phase of evaluation, while recommendations about the second phase will be provided in the last section.

The three user studies conducted on DaPIS were fundamental to confirming or rejecting the hypotheses formulated during the workshops. On the one hand, the first user study[105] confirmed that laypeople have a low familiarity with many data protection concepts, apart from those that are more commonly known, such as anonymisation, marketing or transfer outside the EU. On the other hand, this user test also disconfirmed the hypothesis championed by the legal experts: namely, that the more detailed the graphical representation, the easier the icon interpretation. The recognised excessive complexity guided the following icon (re)design towards simplicity and usability goals.

This observation also brought to the adoption of visual metaphors for some concepts. Indeed, the first exploratory workshop produced pictograms representing concepts in a literal manner (e.g. the right to data portability, see Figure 3.2a). However, despite their concreteness and their arguable informational value, the prototypes are not suitable for small-dimension screens and were judged too complex during the evaluation phase. On the contrary, a metaphor in which one idea is understood in terms of another is well suited to convey meaning through minimal elements. For these reasons, for instance, a folder in the shape of a suitcase was proposed to more compactly recall the right to data portability (see Figure 3.2b). Thus, many explanatory details of the first icon were lost but, if icons need to be usable and scalable elements, certain specifications must be left to the written privacy terms that they complement.

Whereas this first user study was exploratory in nature, the second[106] focused on classical measures to evaluate graphical symbols. Firstly, the icons' legibility was investigated, defined as the ease of recognition of the elements composing an icon. This dimension determines the ease of recognition of the icon as a whole and is important because, if some elements are not easily visible (eg due to their size) or recognisable (eg due to the way they are designed), they can hinder the comprehensibility of its meaning. Moreover, low legibility rates can also make it hard to distinguish one icon from another.

Figure 3.2a The first icon prototype for the right to data portability, that literally depicts the concept's definition

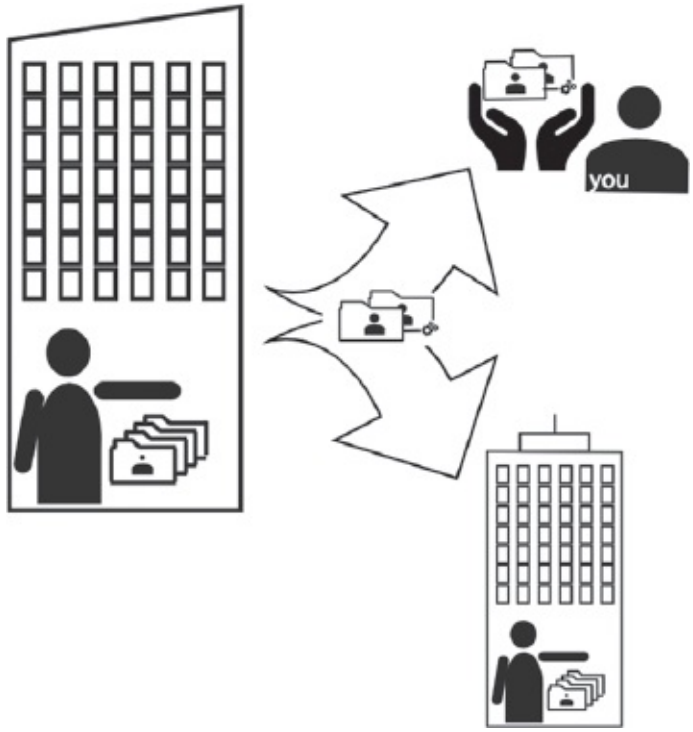


Figure 3.2b The redesign of the icon through a metaphor



The second evaluation dimension was represented by ease of recognition, which is also considered 'the most important single index of a symbol's effectiveness'.[107] However, as recalled earlier, standardised evaluation methods[108] which employ quantitative measures such as hit rate (number of correct associations between icon and referent) are ineligible here because of (a) the lack of familiarity with the icons' referents and (b) their abstractness. In the user studies described in this chapter, each icon was presented next to its definition: instead of measuring efficiency of association between concept and icon, the primary focus was placed on the explicit interpretation of the visuals. Users could provide a subjective rate (on a 1 to 5 Likert scale) to express their degree of agreement with the iconographical choice that had been made for a certain concept. The adoption of such a method had three main goals: firstly, to find out through the uniformity of rates (or, on the contrary, through their variation) whether an icon was considered a good fit overall. Secondly, to clarify the difference between poor rates caused by icons' representation or design, and poor rates derived by lack of understanding of the underlying concept. Finally, to avoid interpretation strategies based on the exclusion of previous associations, since such methods hide the level of subjective

certainty about an association: in the first user study, the icons selected and associated to their meaning first were mostly those that the data subjects could more easily recognise (eg copying).

Lastly, an attempt was made to establish the alignment between users' and designers' mental models: since the interpretation of a user might not correspond to the intended meaning embedded by a designer in a symbol, the participants were explicitly asked to explain whether they could grasp the rationale behind the iconographical choices made during the design phase. This was meant to find out whether, even if not immediately evident, the meaning of the icons could be divined upon reflection.

To enhance the ecological validity of the testing scenario, during the study, the participants were provided a visualised privacy policy showing both the icons' intended context and the entire set of icons. Not surprisingly, the icons that scored best (eg right to information, right to erasure, security purposes, scientific purposes, etc.) either represent concrete objects or familiar concepts or are based on widespread representations.[109] Conversely, the concepts behind the icons that scored worst (eg purposes of provision of a service, purposes of enhancement of the service, public interest), are vague, general, unknown or abstract. In those cases where the association between icon and referent was deemed more appropriate, a general tendency shows that the users' interpretation more frequently coincided with the reason behind the design choice. These considerations and some pitfalls in legibility caused further vetting of the icons, that were lastly evaluated in a third user study.[110]

C. The Final DaPIS

According to the results discussed in the previous pages and the subsequent redesign, an icon set composed of 37 elements was created and is illustrated in Annex 1.[111] It can be assumed that many of these elements can be adopted, although a few icons still require further research, since the user studies did not produce satisfactory results. The user studies described in the last section can be indicative but not conclusive, given the low number of participants and their socio-demographics, which were not representative of the EU population. Yet, the empirical approach described in this chapter has shed light on many design pitfalls, while participatory design has proved valuable to represent the many stakeholders that will be impacted by the use of the icon set. That said, creating data protection icons that should function as standard for the whole European Union might prove difficult, even impossible, considering that there is no 'average user' to design for: European citizens have different levels of (technical and legal) knowledge, expectations and privacy concerns.

VII. Future Research

Since the main obstacle to ease of recognition is lack of familiarity, it can be expected that training would increase recognition rates and determine easier icon recall. Thus, comprehension tests should be carried out as a longitudinal study spanning a period of time, rather than as a one-time only recognition test.[112] It would also be important to determine the icons' learning ease because it is reasonable to expect that individuals will learn to recognise the icons over time, as any new (visual or verbal) language. The function of DaPIS in context should also be tested,[113] namely in an online, interactive interface where the icons complement the privacy policy and act as navigation cues. In this context, an association task between symbol and referent to assess the icons' comprehensibility would be meaningful if carried out as an information-finding task, thus reproducing a realistic user task. Such a setting would provide higher ecological validity to the study and possibly determine higher icons' recognition rates.

Despite the necessity of increasing familiarity, research must be devoted to the cognitive overload that a numerous icon set might cause, especially at first exposure. In this respect, it would be meaningful to experiment whether the selection of a limited number of icons would be more meaningful than the entire icon language. In one possible scenario, only risky practices or practices that would have a significant impact on the individual would be displayed (eg the transfer of data outside of the EU and the existence of automated decision-making). Such selection of icons would thus compose the first layer of a layered approach, where a compact array of icons summarises the most relevant data practices, as long as the selection is solidly grounded in methodology.

Another dimension that must still be scrutinised is the extent to which each icon is discernible from the others of the set; this is a crucial index for ease of recognition. The icons are part of a set and present common elements, therefore the less they overlap in terms of similarity, the more easily they can be memorised. Yet, if the icons are too diverse, they might cause information overload for individuals. In other words, their design should be sufficiently consistent to identify them as a family of icons, but also sufficiently distinctive to distinguish each element easily from the others. This could be carried out as a hit-rate task with multiple answers where all the icons under the same conceptual category (eg rights) or having similar meanings (eg consent, right to withdraw consent, etc.) are displayed together.

VIII. Conclusions

The research described in this chapter is not finished because it has not yet reached conclusive results. Quite the contrary: it is intended to pave the way for further empirically grounded and methodologically motivated investigations into the domain of data protection iconography. What seems beyond doubt is that it will be almost impossible to produce an icon set that will be considered perfectly representative of data protection concepts (ie that is highly semantically transparent) and which will be effortlessly recognised by everybody. User research can give important insights as to what concerns legibility, while alternatives for those symbols that scored worst should be sought. Nevertheless, very high rates for ease of

recognition will never be reached for unfamiliar concepts and unfamiliar icons, until their widespread adoption increases their familiarity. One path to follow might be standardisation open to versioning: after one icon set has been publicly discussed and adopted, empirical data on its use in real-world scenarios should be gathered and employed to further vet the set, considering also the needs of evolving societies and regulations. A fundamental step towards this goal is to initiate a multi-stakeholder discussion and collect multiple approaches and results from other research.[114]

In conclusion, we advance a few general recommendations. Educating data subjects about data protection and privacy-conscious behaviour[115] is necessary to learn the concepts behind the symbols, while the standardisation and consistent implementation of icons by all relevant stakeholders would reduce the margins for free interpretation. Whereas researchers from many disciplines[116] can offer valuable insight on the further development and evaluation of data protection icons, it must be a goal of the regulators to find means and resources to carry out data protection education campaigns for European citizens[117] and standardisation. Every segment of society[118] from each European country should be possibly included: while this is ambitious, it is a necessary step to produce icons that can be safely adopted at the EU level.

Throughout the phases of creation and evaluation of the icons, there was constant opposition between simplicity and preciseness of representation. Whereas the former is a fundamental feature to ensure usability and scalability of the visual elements to any dimension, the latter is important to convey the exact meaning of the corresponding concept. It is challenging to determine the extent to which a visual representation can be simplified and reduced to a few pixels without losing those traits that are necessary to convey its meaning. However, a trade-off must be struck, even if it is an arbitrary choice. Besides, although to a certain extent icons can convey unknown notions to data subjects, the focus should be on other typologies of visual means that are more effective to reach this goal: pictograms, comics, infographics are obvious candidates, while animated gifs, videos and timelines can better convey movements and time sequences.[119]

Although they can contribute to implement transparency to a certain extent, it is unrealistic to expect that icons will be a universal language solving all the hurdles posed by traditional privacy policies. The language of these documents is typically vague and complex, while the amount of information provided is usually excessive for data subjects. Empirical research shows that the provision of detailed privacy information while the user is executing a different primary task is only seen as a nuisance. Nevertheless, interdisciplinary studies can shed light on many overseen aspects of transparency with the aim of providing sufficient necessary and comprehensible information to empower data subjects to have more conscience and control over the flow of their personal data. Creative and original ways of communicating data practices are spreading, although they constitute only a minority,[120] but the GDPR’s transparency obligation has provided a considerable incentive to innovation and empirically based experimentation in this regard.

Acknowledgements

The research described in this chapter was supported by the EACEA, financing the Joint International Doctoral Degree in Law, Science and Technology (LAST-JD) and by the Marie Sklodowska-Curie Mining and Reasoning with Legal Texts (MIREL) project. The authors would like to thank all those who have taken part in this project in various degrees: Margaret Hagan, Legal Design Lab, Stanford University; Professor Danilo Danisi and his students, Accademia di Belle Arti di Bologna; Chiara Cavazzuti, Accademia di Belle Arti di Firenze; and Miroslav Kurdov, Sketchlex. All the participants in the 'Law & Design for Privacy' workshops and in the user studies, and the anonymous reviewers are also gratefully acknowledged.

References

Acquisti, Alessandro, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon et al 'Nudges for privacy and security: Understanding and assisting users' choices online' (2017) 50(3) *ACM Computing Surveys* 44.

Article 29 Data Protection Working Party, Guidelines on Transparency under Regulation 2016/679, 17/EN WP260 (2018).

Article 29 Data Protection Working Party, Opinion 10/2004 on More Harmonised Information Provision, 2004. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp100_en.pdf (Last accessed 1 October 2018).

Asprey, Michele M *Plain Language for Lawyers* (Federation Press, 2003).

Barton, Thoma, Helena Haapio, Stefania Passera and James G Hazard 'Successful Contracts: Integrating Design and Technology' in *Legal Tech, Smart Contracts and Blockchain*, eds M Corrales M Fenwick, H. Haapio (Springer, 2019).

Ben-Shahar, Omri, and Carl E Schneider *More than You Wanted to Know: The Failure of Mandated Disclosure* (Princeton University Press, 2014).

Berger-Walliser, Gerlinde, Thomas D Barton, and Helena Haapio 'From Visualisation to Legal Design: A Collaborative and Creative Process' (2017) 54(2) *American Business Law Journal* 347–392.

Bhatia, Jaspreet, Travis D Breaux, Joel R Reidenberg, and Thomas B Norton 'A Theory of Vagueness and Privacy Risk Perception' in *2016 IEEE 24th International Requirements Engineering Conference (RE)*, pp 26–35.

Boehme-Neßler, Volker *Pictorial Law: Modern Law and the Power of Pictures* (Springer Science & Business Media, 2010).

Brunschwig, Colette *Visualisierung von Rechtsnormen: Legal Design* (Schulthess, 2001).

Butt, Peter 'Legalese Versus Plain Language' (2012) 35 *Amicus Curiae 2001* 28–32.

Caire, Patrice, Nicolas Genon, Patrick Heymans and Daniel L Moody 'Visual Notation Design 2.0: Towards User Comprehensible Requirements Engineering Notations' in *2013 21st IEEE International Requirements Engineering Conference* (RE), pp 115–124.

Calo, Ryan 'Against Notice Skepticism in Privacy (and Elsewhere)' (2011) 87 *Notre Dame Law Rev*iew 1027.

Carolan, Eoin 'The Continuing Problems with Online Consent under the EU's Emerging Data Protection Principles' (2016) 32(3) *Computer Law & Security Review* 462–473.

Dewar, Robert 'Design and Evaluation of Public Information Symbols' Visual Information for Everyday Use: Design and Research Perspectives (1999): 285–303.

Efroni, Zohar et al, 'Privacy Icons: A Risk-based Approach to Visualisation of Data Processing' (2019) 5(3) *European Data Protection Law Review* 352–366. DOI: https://doi.org/10.21552/edpl/2019/3/9.

Esayas, Samson, Tobias Mahler and Kevin McGillivray. 'Is a Picture Worth a Thousand Terms? Visualising Contract Terms and Data Protection Requirements for Cloud Computing Users' in *International Conference on Web Engineering*, (Springer, 2016) pp 39–56.

European Commission, Special Eurobarometer 487a, The General Data Protection Regulation Report. Available at: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2222

(last accessed: 21 July 2019).
European Commission, Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union. COM(2010) 609 final, 2010.
European Commission. Flash Eurobarometer 443, ePrivacy Report. Available at: https://ec.europa.eu/digital-single-market/en/news/eurobarometer-eprivacy, 2016 (last accessed 2 July 2018).
European Commission. Special Eurobarometer 431, Data Protection Report. Available at: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf, 2015 (last accessed 2 July 2018).
European Data Protection Supervisor, Opinion 4/2015 Towards a New Digital Ethics, 2015.
European Parliament and Council of European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, pp 1–88, 2016.
European Parliament. Committee on Civil Liberties, Justice and Home Affairs 'Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [COM(2012)0011 – C7-0025/2012–2012/0011 (COD)]', 2013.
Fabian, Benjamin, Tatiana Ermakova, and Tino Lentz. 'Large-scale Readability Analysis of Privacy Policies' in *Proceedings of the International Conference on Web Intelligence* (ACM, 2017) pp 18–25.
Fischer-Hübner, S, E Wästlund, and H Zwingelberg 'UI Prototypes: Policy Administration and Presentation version 1. Deliverable D4. 3.1 of the EC FP7 project PrimeLife' (2009).
Fuster, Gloria González. 'How Uninformed is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection' (2014) 19 *IDP: revista de Internet, derecho y política= revista d'Internet, dret i política* 92–104.
Gluck, Joshua, Florian Schaub, Amy Friedman, Hana Habib, Norman Sadeh, Lorrie Faith Cranor, and Yuvraj Agarwal. 'How Short is Too Short? Implications of Length and Framing on the Effectiveness of Privacy Notices' in *Twelfth Symposium on Usable Privacy and Security* (SOUPS 2016), pp 321–340.
Gomez, Joshua, Travis Pinnick and Ashkan Soltani (2009) 'Privacy Coding Methodology' Available at: http://knowprivacy.org/policies_methodology.html.
Graf, Cornelia, Christina Hochleitner, Peter Wolkerstorfer, Julio Angulo, Simone Fischer-Hübner, and Erik Wästlund 'Final HCI Research Report.' Primelife Project Deliverable D 4, 2011.
Gruber, Thomas R 'A Translation Approach to Portable Ontology Specifications' (1993) 5(2) *Knowledge Acquisition* 199–220.
Haapio, Helena, Daniela Plewe and Robert deRooy (2017) 'Contract Continuum: From Text to Images, Comics, and Code' in *Trends und Communities der Rechtsinformatik-Trends and Communities of Legal Informatics*: *Tagungsband des 20. Internationalen Rechtsinformatik Symposions IRIS 2017 Proceedings of the 20th International Legal Informatics Symposium*.
Haapio, Helena, Margaret Hagan, Monica Palmirani and Arianna Rossi 'Legal Design Patterns for Privacy' in *Data Protection/LegalTech. Proceedings of the 21th International Legal Informatics Symposium IRIS 2018*, pp 445–450.
Hagan, Margaret 'Law by Design'. Available at: www.lawbydesign.co (last accessed 19 March 2019).
Hansen, Marit 'Putting Privacy Pictograms into Practice – A European Perspective' (2009) 154 *GI Jahrestagung* 1–703.
Harkous, Hamza, Kassem Fawaz, Rémi Lebret, Florian Schaub, Kang G Shin, and Karl Aberer (2018) 'Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning' in *27th (USENIX) Security Symposium Security 2018*, pp 531–548.
Hartzog, Woodrow 'Website Design as Contract' (2010) 60 *Am UL Rev* 1635.
Hartzog, Woodrow *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press, 2018).
Hicks, Jon *The Icon Handbook* (Five Simple Steps, 2011).
Holtz, Leif-Erik, Harald Zwingelberg and Marit Hansen 'Privacy Policy Icons' in *Privacy and Identity Management for Life*, pp. 279–285 (Springer, Heidelberg, 2011).
Holtz, Leif-Erik, Katharina Nocun and Marit Hansen (2010) 'Towards Displaying Privacy Information with Icons' in *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life* (Springer, Heidelberg, 2010) pp 338–348.
Iannella, Rennato, Adam Finden and Stacked Creations (2010) 'Privacy Awareness: Icons and Expression for Social Networks' in *Proceedings of the 8th Virtual Goods Workshop* and the *6th ODRL Workshop*: 1–15.
Isherwood, Sarah J, Siné JP McDougall and Martin B Curry 'Icon Identification in Context: The Changing Role of Icon

Characteristics with User Experience' (2007) 49(3) *Human Factors* 465–476.
ISO 9186-1:2014. Graphical symbols – Test methods – Part 1: Method for testing comprehensibility.
ISO 9186-3:2014. Graphical symbols – Test methods Part 3: Method for testing symbol referent association.
Jensen, Carlos and Colin Potts 'Privacy Policies as Decision-making Tools: An Evaluation of Online Privacy Notices' in *Proceedings of the SIGCHI conference on Human Factors in Computing Systems* (ACM, 2004) pp 471–478.
Joint Research Center (2018) 'DigComp into Action. Get Inspired Make It Happen'. A User Guide to the European Digital Competence Framework, 7.
Lusoli, Wainer, Margherita Bacigalupo, Francisco Lupiáñez-Villanueva, Norberto Nuno Gomes de Andrade, Shara Monteleone, and Ioannis Maghiros. 'Pan-European Survey of Practices, Attitudes and Policy Preferences as regards Personal Identity Data Management' (2012) JRC Scientific and Policy Reports, Seville.
Malamed, Connie (2009) *Visual Language for Designers: Principles for Creating Graphics that People Understand*. Rockport Publishers.
Mantelero, Alessandro 'The Future of Consumer Data Protection in the EU Re-thinking the 'Notice and Consent' Paradigm in the New Era of Predictive Analytics' (2014) 30(6) *Computer Law & Security Review* 643–660.
McDonald, Aleecia M and Lorrie Faith Cranor 'The Cost of Reading Privacy Policies' (2008) 4 *ISJLP* 543.
Mehldau, Matthias Iconset for Data-Privacy Declarations v 0.1. Available at: https://netzpolitik.org/wp-upload/data-privacy-icons-v01.pdf.
Milne, George R and Mary J Culnan 'Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices' (2004) 18(3) *Journal of Interactive Marketing* 15–29.
Mondschein, Christopher F 'Some Iconoclastic Thoughts on the Effectiveness of Simplified Notices and Icons for Informing Individuals as Proposed in Article 12 (1) and (7) GDPR' (2016) 2 *European Data Protection Law Review* 507.
Moskowitz, Ben and Aza Raskin 'Privacy Icons.' Available at: https://wiki.mozilla.org/Privacy_Icons, 2011.
Nissenbaum, Helen 'A Contextual Approach to Privacy Online' (2011) 140(4) *Daedalus* 32–48.
Obar, Jonathan A and Anne Oeldorf-Hirsch 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services' (2018) *Information, Communication & Society* 1–20.
Oehler, Andreas and Stefan Wendt 'Good Consumer Information: The Information Paradigm at its (Dead) End?' (2017) 40(2) *Journal of Consumer Policy* 179–191.
Palmirani, Monica and Fabio Vitali 'Akoma-Ntoso for Legal Documents' in Legislative XML for the Semantic Web (Springer, Dordrecht, 2011) pp 75–100.
Palmirani, Monica, Michele Martoni, Arianna Rossi, Cesare Bartolini and Livio Robaldo (2018) 'PrOnto: Privacy Ontology for Legal Reasoning' in *International Conference on Electronic Government and the Information Systems Perspective* (Springer, 2018) pp 139–152.
Palmirani, Monica, Michele Martoni, Arianna Rossi, Cesare Bartolini and Livio Robaldo 'Legal Ontology for Modelling GDPR Concepts and Norms' *Legal Knowledge and Information Systems: JURIX 2018: The Thirty-first Annual Conference*. Vol 313 (IOS Press, 2018).
Passera, Stefania, *Beyond the Wall of Contract Text. Visualising Contracts to Foster Understanding and Collaboration within and Across Organisations* (Aalto University, 2017).
Passera, Stefania 'Beyond the Wall of Text: How Information Design Can Make Contracts User-friendly' in *International Conference of Design, User Experience, and Usability* (Springer, 2015) pp 341–352.
Perry-Kessaris, Amanda 'Legal Design for Practice, Activism, Policy and Research' (2018) 46 *Journal of Law and Society* 185–210.
Pettersson, John Sören. 'A Brief Evaluation of Icons in the First Reading of the European Parliament on COM (2012) 0011' in *IFIP International Summer School on Privacy and Identity Management*, (Springer, 2014) pp 125–135.
Pollach, Irene 'A Typology of Communicative Strategies in Online Privacy Policies: Ethics, Power and Informed Consent' (2005) 63(3) *Journal of Business Ethics* 221.
PrivacyTech 'Privacy Icons'. Available at: www.privacytech.fr/privacy-icons/.
Proctor, Robert W, M Athar Ali and Kim-Phuong L Vu 'Examining usability of Web Privacy Policies' (2008) 24(3) *International Journal of Human – Computer Interaction* 307–328.
Reeder, Robert W, Patrick Gage Kelley, Aleecia M McDonald and Lorrie Faith Cranor 'A User Study of the Expandable Grid Applied to P3P Privacy Policy Visualisation' in *Proceedings of the 7th ACM Workshop on Privacy in the Electronic Society* (ACM, 2008) pp 45–54.
Reidenberg, Joel R, Jaspreet Bhatia, Travis D Breaux and Thomas B Norton 'Ambiguity in Privacy Policies and the Impact of Regulation' (2016) 45(S2) *The Journal of Legal Studies* S163–S190.
Robinson, Neil, Hans Graux, Maarten Botterman, and Lorenzo Valeri 'Review of EU Data Protection Directive: Summary' Information Commissioner's Office (2009).

Rossi, Arianna 'Legal Design for the General Data Protection Regulation. A Methodology for the Visualisation and Communication of Legal Concepts' PhD thesis, Alma Mater Studiorum Università di Bologna, PhD in Law, Science and Technology 31 Ciclo (2019). Online at: http://amsdottorato.unibo.it/9060/.

Rossi, Arianna and Monica Palmirani 'A Visualisation Approach for Adaptive Consent in the European Data Protection Framework' in *2017 Conference for E-Democracy and Open Government* (IEEE, 2017) pp 159–170.

Rossi, Arianna and Monica Palmirani, 'DaPIS: An Ontology-Based Data Protection Icon Set' in G Peruginelli and S Faro (eds), *Knowledge of the Law in the Big Data Age. Frontiers in Artificial Intelligence and Applications No 317* (IOS Press, 2019).

Rossi, Arianna, Rossana Ducato, Helena Haapio, Stefania Passera and Monica Palmirani 'Legal Design Patterns: Towards A New Language for Legal Information Design' in *Internet of Things. Proceedings of the 22nd International Legal Infomatics Symposium IRIS* (2019) 517–526.

Rossi, Arianna, Rossana Ducato, Helena Haapio and Stefania Passera 'When Design Met Law: Design Patterns for Information Transparency' (2019) 122 *Droit de la consommation* 79–121.

Rundle, Mary C 'International Personal Data Protection and Digital Identity Management Tools' (2006) The Berkman Center for Internet & Society Research Publication Series.

Sadeh, Norman, Alessandro Acquisti, Travis D Breaux, Lorrie Faith Cranor, Aleecia M McDonald, Joel R Reidenberg, Noah A Smith et al (2013) 'The Usable Privacy Policy Project'. Technical Report, CMU-ISR-13-119.

Sartor, Giovanni, Monica Palmirani, Enrico Francesconi and Maria Angela Biasiotti (eds) Legislative XML for the Semantic Web: Principles, Models, Standards For Document Management. Vol 4 (Springer Science & Business Media, 2011).

Schaub, Florian, Rebecca Balebako, Adam L Durity and Lorrie Faith Cranor 'A Design Space for Effective Privacy Notices' in *Eleventh Symposium on Usable Privacy and Security* (SOUPS 2015), pp 1–17.

Schuler, Douglas and Aki Namioka, eds *Participatory Design: Principles and Practices* (CRC Press, 1993).

Sloan, Robert H and Richard Warner 'Beyond Notice and Choice: Privacy, Norms and Consent' (2014) 14 *Journal of High Tech Law* 370.

Specht, Louise und Bienemann, 'Informationsvermittlung durch standardisierte Bildsymbole – Ein Weg aus dem Privacy Paradox?' in Louisa Specht, Nikola Werry and Susanne Werry (eds) Handbuch *Datenrecht in der Digitalisierung* (forthcoming 2019).

TRUSTe, 'TRUSTe and Disconnect Introduce Visual Icons to Help Consumers Understand Privacy Policies'. Available at: www.truste.com/blog/2014/06/23/truste-disconnect-introduce-visual-icons-to-help-consumers-understand/-privacy-policies/.

Waller, Robert, Jenny Waller, Helena Haapio, Gary Crag and Sandi Morrisseau 'Cooperation Through Clarity: Designing Simplified Contracts' (2016) 1–2 *Journal of Strategic Contracting and Negotiation* 48–68.

Whalen, Tara and Kori M Inkpen 'Gathering Evidence: Use of Visual Security Cues in Web Browsers' in *Proceedings of Graphics Interface 2005* (Canadian Human-Computer Communications Society, 2005) pp 137–144.

Wiedenbeck, Susan 'The Use of Icons and Labels in an End User Application Program: An Empirical Study of Learning and Retention' (1999) 18(2) *Behaviour & Information Technology* 68–82.

Wogalter, Michael S 'Factors Influencing the Effectiveness of Warnings' in *Visual Information for Everyday Use* (CRC Press, 2014) pp 127–144.

Wolff, Jennifer Snow and Michael S Wogalter 'Comprehension of Pictorial Symbols: Effects of Context and Test Method' (1998) 40(2) *Human Factors* 173–186.

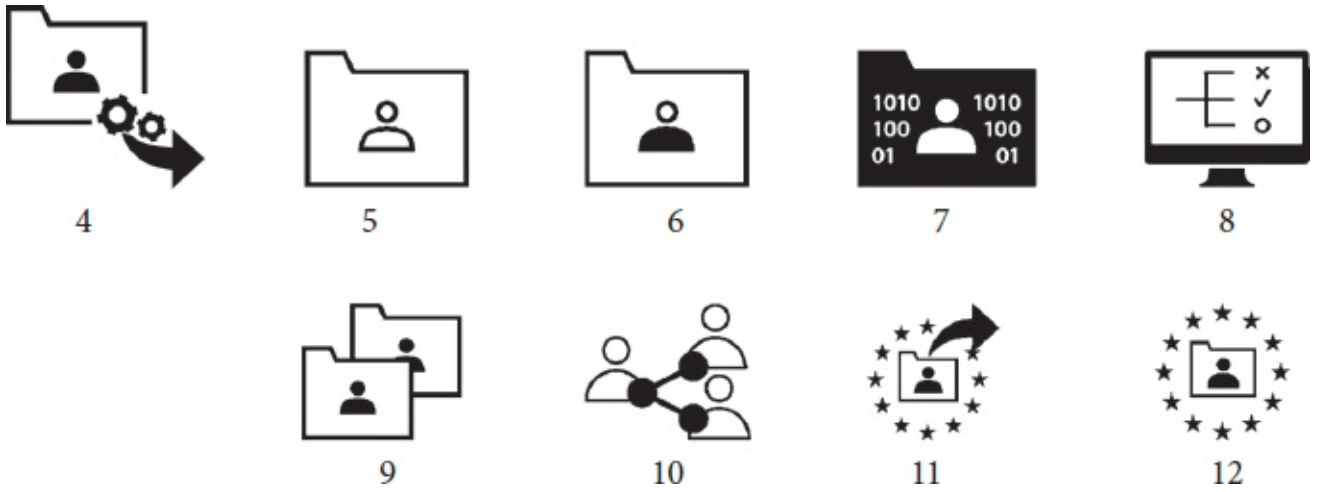
Zuiderveen Borgesius, Frederik 'Consent to Behavioural Targeting in European Law – What Are the Policy Implications of Insights from Behavioural Economics?' Amsterdam Law School Research Paper 2013–43 (2013).

Annex 1

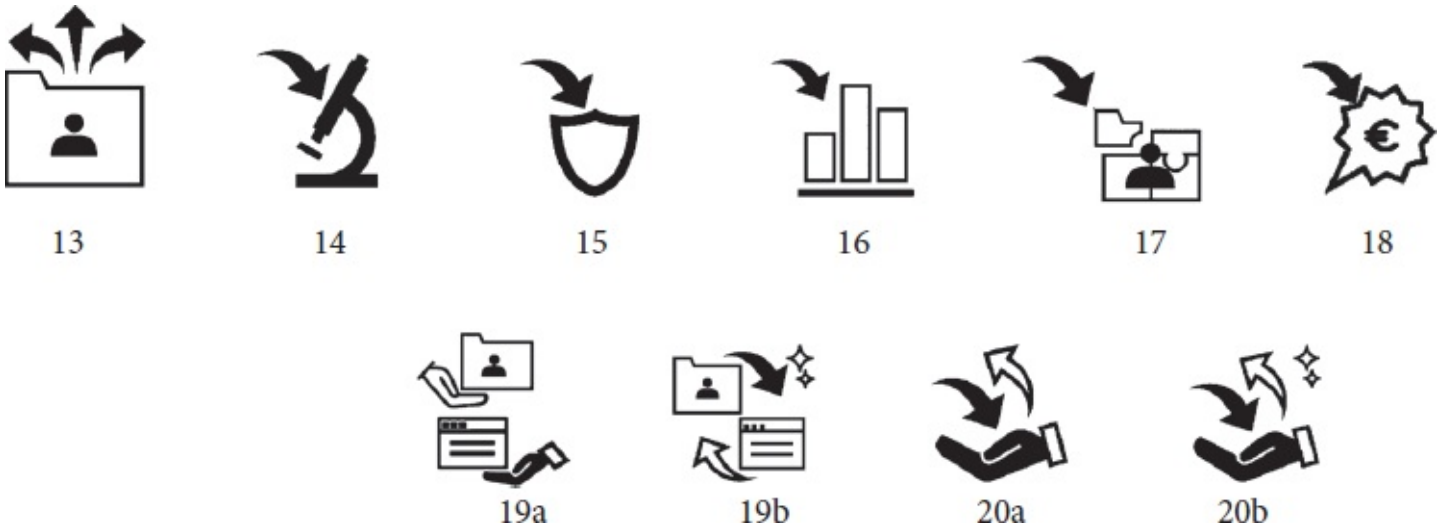
Agents and roles: (1) Data subject; (2) Data controller; (3) Supervisory authority



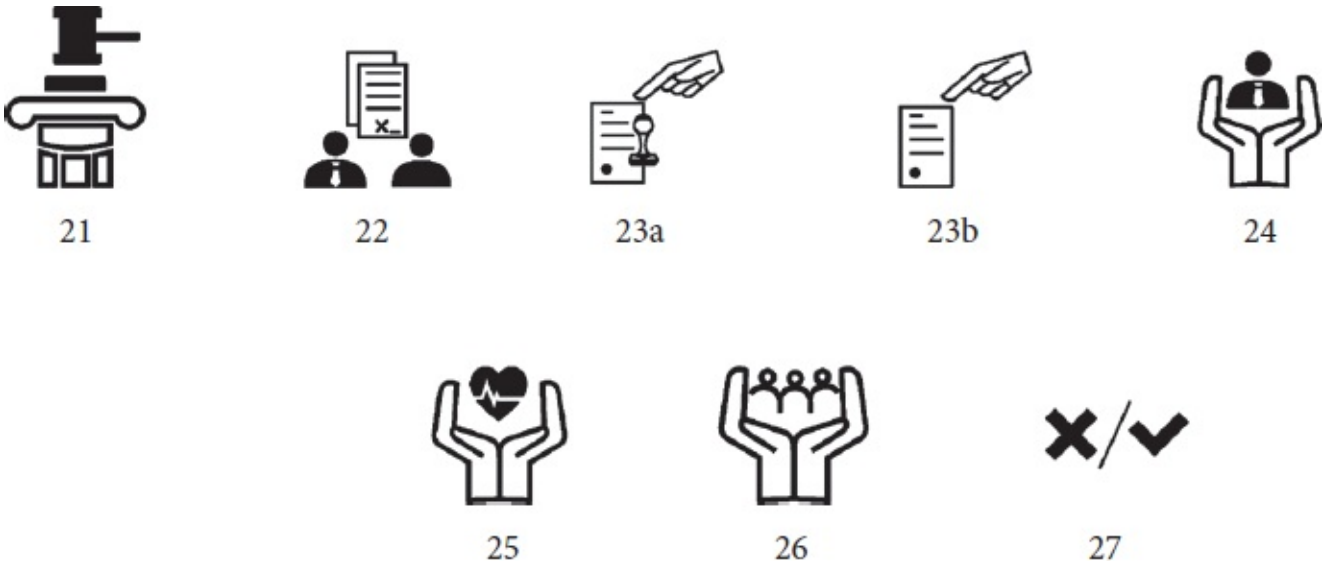
Processing operations: (4) Processing personal data; (5) Anonymization; (6) Pseudonymization; (7) Encryption*; (8) Automated decision-making; (9) Copying; (10) Data Sharing with third parties; (11) Transfer of data to third countries; (12) Storage of data inside the EU



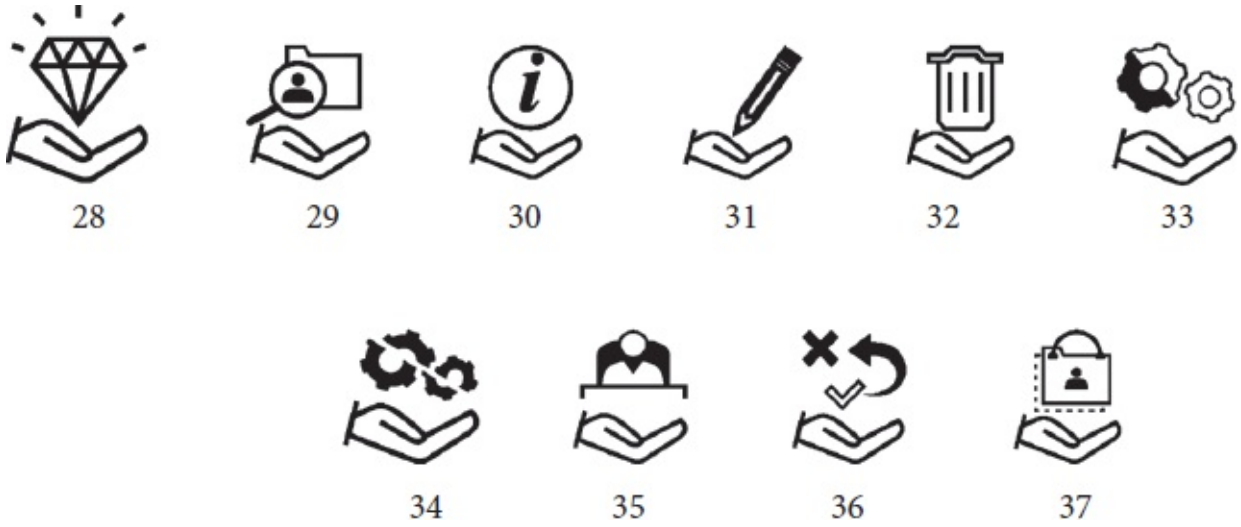
Purposes of processing: (13) Processing purposes; (14) Research purposes; (15) Security purposes; (16) Statistical purposes; (17) Profiling purposes; (18) Marketing purposes; (19a) Purposes of provision of the service – alternative a*; (19b) Purposes of service enhancement – alt. a*; (20a) Purposes of provision of the service – alt. b*; (20b) Purposes of service enhancement – alt. b*



Legal bases: (21) Legal bases; (22) Contract; (23a) Legal obligation – alt. a*; (23b) Legal obligation – alt. b*; (24) Legitimate interest; (25) Vital interest; (26) Public interest; (27) Consent



Rights of the data subject: (28) Rights; (29) Right of access; (30) Right to be informed; (31) Right to rectification; (32) Right to erasure; (33) Right to restrict processing*; (34) Right to object to processing*; (35) Right to lodge a complaint to a supervisory authority; (36) Right to withdraw consent; (37) Right to data portability



* For the icons with this symbol, research about possible alternatives that can better convey the meaning should be carried out.

---

[1] SnT, University of Luxembourg. The author performed this work while at CIRSFID, University of Bologna and ICR, University of Luxembourg.

[2] CIRSFID, Università di Bologna.

[3] For an historical evolution of the information paradigm and the reasons behind its origins in the 1960s, see generally Gloria González Fulster, 'How Uninformed is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection' (2014) 19 *IDP: revista de Internet, derecho y política= revista d'Internet, dret i política* 92–104; Alessandro Mantelero, 'The Future of Consumer Data Protection in the EU Re-thinking the 'Notice and Consent' Paradigm in the New Era of Predictive Analytics' (2014) 30(6) *Computer Law & Security Review* 643–660. For an historical background on the regulatory tool of consent and its critical analysis, see generally Eoin Carolan, 'The Continuing Problems with Online

Consent under the EU's Emerging Data Protection Principles,' (2016) 32(3) *Computer Law & Security Review* 462–473.

[4] The provision of information is considered the bedrock for the data subject to make the choice either to engage or disengage with a service. Helen Nissenbaum, 'A Contextual Approach to Privacy Online' (2011) 140(4) *Daedalus* 34.

[5] See generally George R Milne and Mary J Culnan, 'Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices' (2004) 18(3) *Journal of Interactive Marketing* 15–29; Wainer Lusoli et al, 'Pan-European Survey of Practices, Attitudes and Policy Preferences as Regards Personal Identity Data Management' (2012) JRC Scientific and Policy Reports Seville: EC JRC Institute for Prospective Technological Studies; Jonathan A Obar and Anne Oeldorf-Hirsch, 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services' (2018) *Information, Communication & Society* 1–20.

[6] 'While transparency has been emphasised as an important practice for decades, existing privacy notices often fail to help users make informed choices. They can be lengthy or overly complex, discouraging users from reading them'. Florian Schaub et al., 'A Design Space for Effective Privacy Notices,' *Eleventh Symposium on Usable Privacy and Security* (SOUPS 2015) (2015): 1. See also Neil Robinson et al, 'Review of the European Data Protection Directive,' Rand Europe (2009): 28–33.

[7] Woodrow Hartzog, 'Website Design as Contract,' (2010) 60 *American University Law Review* 1651–1652.

[8] Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press, 2018), 47.

[9] For a through critical discussion on this assumption, see eg Robert H Sloan and Richard Warner, 'Beyond Notice and Choice: Privacy, Norms, and Consent' (2014) 14 *Journal of High Technology Law* 16–21. Not reading can also be the outcome of a rational decision, see n 18.

[10] See eg European Commission, *Special Eurobarometer 487a, The General Data Protection Regulation Report.* Available at: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2222 (last accessed: 21 June 2019): 51–55; European Commission, *Flash Eurobarometer 443, ePrivacy Report*. Available at: https://ec.europa.eu/digital-single-market/en/news/eurobarometer-eprivacy, 2016 (last accessed 2 July 2018): 2–4; European Commission. *Special Eurobarometer 431, Data Protection Report*. Available at: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf, 2015 (last accessed 2 July 2018): 18–19.

[11] Andreas Oehler and Stefan Wendt. 'Good Consumer Information: The Information Paradigm at its (Dead) End?' (2017) 40(2) *Journal of Consumer Policy* 182.

[12] Research from behavioural science has exposed many hurdles in privacy and security decision making. See generally Alessandro Acquisti et al, 'Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online' (2017) 50(3) *ACM Computing Surveys* (CSUR) 44.

[13] European Parliament and Council of European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, pp 1–88, 2016. Hereafter: GDPR.

[14] See eg Arianna Rossi et al, 'When Design Met Law: Design Patterns for Information Transparency' (2019) 122 *Droit de la consommation* 91–97.

[15] Hartzog, *Privacy's Blueprint* (n 8) 64.

[16] 'Privacy policies are written by lawyers, for lawyers, and appear to serve little useful purpose for the data subject due to their length, complexity and extensive use of legal terminology' Robinson, et al, (n 6) 29; Helena Haapio et al, 'Legal Design Patterns for Privacy' in Erich Schweighofer et al (eds), *Data Protection/LegalTech* in *Proceedings of the 21th International Legal Informatics Symposium IRIS 2018* (Editions Weblaw, Bern 2018): 446.

[17] Most privacy policies have the unique goal to discharge from liability the service provider. Hartzog, 'Website Design' (n 7) 1640–1641.

[18] In general, legal communication tends to focus on the essence and precision of the rules, but it is not aimed at responding to the needs of the people that are principally impacted by the text (ie mostly non-lawyers). Haapio et al, (n 16) 446. Within this view, privacy notices can be effective accountability mechanisms for companies and necessary auditing instruments for supervisory authorities and advocates, but 'they are just not very good at notifying users.' Hartzog, *Privacy's Blueprint* (n 8) 70. Robinson et al (n 6) 29.

[19] See generally Carlos Jensen and Colin Potts, 'Privacy policies as decision-making tools: an evaluation of online privacy notices'. *Proceedings of the SIGCHI conference on Human Factors in Computing Systems* (ACM, 2004); Robert W Proctor, M Athar Ali, and Kim-Phuong L Vu, 'Examining usability of Web Privacy Policies' (2008) 24(3) *Intl. Journal of Human–Computer Interaction* 307–328; Benjamin Fabian, Tatiana Ermakova and Tino Lentz, 'Large-scale Readability Analysis of Privacy Policies' in *Proceedings of the International Conference on Web Intelligence* (ACM, 2017): 18–25; Obar and Oeldorf-Hirsch, The Biggest Lie (n 5).

[20] Estimations of privacy policies' reading time are provided in Obar and Oeldorf-Hirsch, (n 5) at 12; Fabian, Ermakova, and Lentz (n 20) at 21–22; Aleecia M McDonald and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies' (2008) 4 *ISJLP* 543.

[21] Too much information overwhelms users, who in turn do not react reasonably, but 'skim, freeze or pick out information arbitrarily', Ryan Calo, 'Against Notice Skepticism in Privacy (and Elsewhere)' (2011) 87 *Notre Dame Law Review* 15. This evidence suggests that the information duties' basic assumption (ie providing more information rebalances information asymmetries) is flawed. Oehler and Wendt (n 11) 179.

[22] Obar and Oeldorf-Hirsch (n 5) 18. Individuals carry out a cost–benefit analysis that considers time and effort required for reading and understanding. Frederik Zuiderveen Borgesius, 'Consent to Behavioural Targeting in European Law-What are the Policy Implications of Insights from Behavioural Economics?,' *Amsterdam Law School Legal Studies Research Paper; No. 2013–43* (Amsterdam: University of Amsterdam, IViR. 2013): 31–34. DOI: 10.2139/ssrn.2300969.

[23] Eg 'We *may* collect information about you.' 'We disclose *certain* personal data with third parties.' See generally Irene Pollach, 'A Typology of Communicative Strategies in Online Privacy Policies: Ethics, Power and Informed Consent,' (2005) 62(3) *Journal of Business Ethics* 225; Joel R Reidenberg et al, 'Ambiguity in Privacy Policies and the Impact of Regulation' (2016) 45 *The Journal of Legal Studies* S163–S190.

[24] Jaspreet Bhatia et al, 'A Theory of Vagueness and Privacy Risk Perception' in *Requirements Engineering Conference (RE), 2016 IEEE 24th International*, IEEE (2016): 26.

[25] See generally Michele M Asprey, *Plain Language for Lawyers* (Federation Press, 2003); Peter Butt, 'Legalese versus Plain Language' (2012) 35 *Amicus Curiae* 2001 28–32.

[26] In late 2017, only a minority of the most trafficked sites on the web displayed visual structure. Haapio et al (n 16) 449.

[27] Stefania Passera, 'Beyond the Wall of Text: How Information Design Can Make Contracts User-friendly' *International Conference of Design, User Experience, and Usability* (Springer Cham, 2015): 342.

[28] European Data Protection Supervisor, *Opinion 4/2015 Towards a New Digital Ethics*, (2015): 4.

[29] I.e. information hierarchy and meaningful visual organization (eg divide the document in digestible paragraphs, organise the content in the relevant sections, provide informative headings and differentiate font bolds). Arianna Rossi et al, 'Legal Design Patterns: Towards a New Language for Legal Information Design,' *Internet of Things. Proceedings of the 22nd International Legal Informatics Symposium IRIS 2019* (Bern Weblaw, 2019): 517–526; Arianna Rossi et al, (n 14) 93.

[30] Passera (n 27) 343.

[31] See generally McDonald and Faith Cranor, Cost of Reading; Robert W Reeder et al, 'A User Study of the Expandable Grid Applied to P3P Privacy Policy Visualisation.' *Proceedings of the 7th ACM Workshop on Privacy in the Electronic Society* (ACM, 2008): 45–54.

[32] '[N]othing more than an unwanted impediment to the real purposes of going online' Obar and Oeldorf-Hirsch (n 5) 22.

[33] The cookie consent is the most striking example of this nuisance.

[34] '[T]here is considerable agreement that transparency-and-choice has failed.' Nissenbaum (n 4) 34.

[35] See generally Omri Ben-Shahar and Carl E Schneider. *More Than You Wanted to Know: The Failure of Mandated Disclosure* (Princeton University Press, 2014).

[36] Oehler and Wendt (n 11) 181.

[37] See generally Haapio and Passera, Contracts as Interfaces; Stefania Passera, *Beyond the Wall of Contract Text. Visualising Contracts to Foster Understanding and Collaboration Within and Across Organisations* (Aalto University, 2017); Passera, (n 27); Stefania Passera and Helena Haapio 'Transforming Contracts from Legal Rules to User-centered Communication Tools: A Human-information Interaction Challenge' (2013) 1 (3) *Communication Design Quarterly Review*

38–45; Robert Waller et al, 'Cooperation through Clarity: Designing Simplified Contracts' (2016) 2(1–2)*Journal of Strategic Contracting and Negotiation* 48–68.

[38] See generally Joshua Gluck et al, 'How Short is Too Short? Implications of Length and Framing on the Effectiveness of Privacy Notices,' *12th Symposium on Usable Privacy and Security* (SOUPS), (2016): 321–340; Norman Sadeh et al, *The Usable Privacy Policy Project*, Technical Report, CMU–ISR–13–119 (Carnegie Mellon University, 2013); Schaub et al (n 6).

[39] Despite obvious discrepancies, both in the American and European contexts mandated disclosures are recognised as central policy tool. The importance of the understandability of information provided to users is underlined in both legislations (eg for the US see the California Consumer Privacy Act), while even the critiques to privacy notices and the proposed solutions are similarly expressed on both sides of the Atlantic. This is why analogies between the two models can be drawn: best practices for good legal information design can be universally applied since they resonate with the capacity of processing information of all human beings, rather than being tied to a specific legal framework.

[40] Article 12 overtly specifies that the information to data subjects must be disclosed in a 'concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.' European Parliament and Council, *GDPR*.

[41] See generally Article 29 Data Protection Working Party, *Guidelines on Transparency under Regulation 2016/679, 17/EN WP260 rev. 01* (2018). Available at: www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2010/0609/COM_COM(2010)0609 (last accessed 1 October 2018): 5.

[42] Article 29 Data Protection Working Party, *Opinion 10/2004 on More Harmonised Information Provision*, 2004. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp100_en.pdf (last accessed 1 October 2018): 6.

[43] 'Compared to the DPD, the GDPR now includes rules on how the information must be presented to data subjects and not only which information should be presented' Christopher F. Mondschein, 'Some Iconoclastic Thoughts on the Effectiveness of Simplified Notices and Icons for Informing Individuals as Proposed in Article 12(1) and (7) GDPR' (2016) 2 *European Data Protection Law Review* 509.

[44] WP29, Guidelines Transparency, 5.

[45] Hereafter: WP29.

[46] For instance, a teenager uploading pictures on Instagram supposedly has different cognitive needs and past experiences than an adult opening a bank account.

[47] 'The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used' European Parliament and Council, *GDPR*, Recital 58. 'Importantly, the principle of transparency in the GDPR is not limited to being effected simply through language communications (whether written or oral). The GDPR provides for visualisation tools (referencing in particular, icons, certification mechanisms, and data protection seals and marks) where appropriate' WP29, Guidelines Transparency, 25. The use of visual elements to enhance the comprehensibility of the law is gaining acceptance, since adequate knowledge visualisation can support learning, reasoning and memorisation, and fight information overload. See generally M. Hagan, *Law by Design.* Available at: www.lawbydesign.co; Gerlinde Berger-Walliser, Thomas D Barton, and Helena Haapio, 'From Visualisation to Legal Design: A Collaborative and Creative Process.' *American Business Law Journal* 54(2) (2017): 347–392; Volker Boehme-Neßler, *Pictorial Law: Modern Law and the Power of Pictures* (Springer Science & Business Media, 2010); C.R. Brunschwig, *Visualisierung von Rechtsnormen – Legal Design [Visualisation of Legal Norms]*, PhD diss., Doctoral Thesis (Zürcher Studien zur Rechtsgeschichte, 2001); Haapio and Passera, Contracts as Interfaces (n 37).

[48] WP29, Guidelines Transparency, 25.

[49] '1. In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission. 2. In particular, delegated acts should be adopted in respect of criteria and requirements for certification mechanisms, information to be presented by standardised icons and procedures for providing such icons. 3. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level.' European Parliament and Council, *GDPR*, Recital 166.

[50] WP29, Guidelines Transparency, 26.

[51] In general, empirical research ('user testing' WP29, Guidelines Transparency, 14) must demonstrate the intelligibility and effectiveness of a specific privacy notice.

[52] Helena Haapio, Daniela Plewe, and Robert deRooy. 'Contract Continuum: From Text to Images, Comics, and Code,' *Trend and Communities of Legal Informatics. Proceedings of the 20th International Legal Informatics Symposium IRIS 2017* (2017): 4.

[53] See generally Thomas D Barton et al, 'Successful Contracts: Integrating Design and Technology,' in *Legal Tech, Smart Contracts and Blockchain*, eds M Corrales, M Fenwick, H Haapio (Springer, 2019).

[54] Recital 21 of Directive 2013/37/EU17.

[55] Such heterogeneous information contained in legal documents can be formally represented through a multi-layered architecture: (1) the textual layer provides the representation of the document's original content; (2) the structural layer provides a hierarchical organisation of the text; (3) the metadata layer connects document's information with external ontological resources; (4) the ontological layer is the formal model of the concepts mentioned in the document; (5) the logical layer provides the legal interpretation and modelling of the legal meaning of the text, and the transformation of the norms into legal rules to allow legal reasoning. Monica Palmirani and Fabio Vitali, 'Akoma-Ntoso for Legal Documents' *Legislative XML for the Semantic Web* (Springer, Dordrecht, 2011): 78–79.

[56] Akoma Ntoso (www.akomantoso.org) has been adopted by OASIS (www.oasis-open.org) as legal open XML standard for legislative, judiciary and legal documents.

[57] The W3C Web Ontology Language (OWL) is a computational logic-based language that can represent rich and complex knowledge in documents that are known as ontologies. OWL is part of the W3C's Semantic Web technology stack (www.w3.org/OWL/).

[58] A classical definition in artificial intelligence research characterises ontologies as an explicit, formal specification of a shared conceptualisation. Thomas R Gruber, 'A Translation Approach to Portable Ontology Specifications' (1993) 5(2) *Knowledge Acquisition* 199–220. Ontologies are massively adopted in the Semantic Web to support the uniform description, retrieval and sharing of legal knowledge through the definition of legal concepts and their linguistic realisation.

[59] The first layer should 'include the details of the purposes of processing, the identity of controller and a description of the data subject's rights [… It] should also contain information on the processing which has the most impact on the data subject and processing which could surprise them'. WP29, *Guidelines Transparency*, 18. The display of the first layer might be helpful especially in those occasions when the user is carrying out a task (eg a ticket purchase) and the reading of the privacy terms would be regarded as a nuisance.

[60] The idea is further explored in Arianna Rossi and Monica Palmirani, 'DaPIS: An Ontology-Based Data Protection Icon Set' in G Peruginelli and S Faro (eds), *Knowledge of the Law in the Big Data Age. Frontiers in Artificial Intelligence and Applications* no 317 (IOS Press, 2019).

[61] See Section II.

[62] For a thorough description of the ontology, its goals and the methodology to build it, see generally Monica Palmirani et al, 'PrOnto: Privacy Ontology for Legal Reasoning' *International Conference on Electronic Government and the Information Systems Perspective* (Springer, Cham, 2018): 139–152; Monica Palmirani et al 'Legal Ontology for Modelling GDPR Concepts and Norms' *Legal Knowledge and Information Systems: JURIX 2018: The Thirty-first Annual Conference*. Vol 313. IOS Press, 2018.

[63] Rossi and Palmirani (n 60) s 3.2.2.

[64] Legal Design is an interdisciplinary research defined as 'the application of human-centered design to the world of law, to make legal systems and services more human-centered, usable, and satisfying'. Hagan (n 47) Ch 1. On the application of design methods to the legal domain, see generally Berger-Walliser et al (n 47); Brunschwig, *Visualisierung*. A 'Legal Design Manifesto' describing approaches, goals and methods of legal design has been recently published (www.legaldesignalliance.org/). See also Amanda Perry-Kessaris, 'Legal Design for Practice, Activism, Policy and Research,' 46(2) *Journal of Law and Society* 185–210.

[65] Connie Malamed, *Visual Language for Designers: Principles for Creating Graphics that People Understand* (Rockport Publishers, 2009): 119.

[66] Sarah J Ishwerwood, Siné JP McDougall, and Martin B Curry, 'Icon Identification in Context: The Changing Role of

Icon Characteristics with User Experience' (2007) 49(3) *Human Factors* 465. For a critical examination of the supposed universality of icons, see generally Robert Dewar, 'Design and Evaluation of Public Information Symbols' (1999) *Visual information for Everyday Use: Design and Research Perspectives* 285–303.

67 Isherwood et al (n 66) 467.

68 Ibid at 467.

69 Malamed (n 65) *Visual Language*, 118. For new exposures, ease of identification also depends on the icon's concreteness, which is the extent to which real objects, materials, or people are depicted (Isherwood, (n 66) 466). This effect diminishes as users gain experience over the icons, though.

70 Jon Hicks, *The Icon Handbook* (Five Simple Steps, 2011): 22.

71 Isherwood et al (n 66) 466.

72 Dewar, (n 66), 49–50.

73 Hicks (n 70) 95.

74 The highway code represents the most successful example of an internationally established legal visual language. Yet, the supposed universality of traffic signs derives from constant use, international standardisation of the norms, and explicit education of the drivers.

75 However, these symbols express great variety across applications (eg browser types) and no standard exists. See eg Tara Whalen and Kori M Inkpen, 'Gathering Evidence: Use of Visual Security Cues in Web Browsers' *Proceedings of Graphics Interface 2005* (Canadian Human-Computer Communications Society, 2005): 143–144.

76 See especially *ISO 9186-1:2014. Graphical symbols – Test methods – Part 1: Method for Testing Comprehensibility*.

77 Wolff et al suggest that without such precautions, low recognition scores would falsely indicate that more design and test work is necessary. See Wolff, Jennifer Snow, and Michael S Wogalter 'Comprehension of Pictorial Symbols: Effects of Context and Test Method' (1998) 40(2) *Human Factors*: 173–186.

78 In order of publication: Mary C Rundle 'International Personal Data Protection and Digital Identity Management Tools.' *The Berkman Center for Internet & Society Research Publication Series* (2006); M Mehldau, *Iconset for Data-Privacy Declarations v 0.1*. Available at: https://netzpolitik.org/wp-upload/data-privacy-icons-v01.pdf; Joshua Gomez, Travis Pinnick and Ashkan Soltani, *Privacy Coding Methodology*. Available at: http://knowprivacy.org/policies_methodology.html) (2009); Renato Iannella, Adam Finden and Stacked Creations. 'Privacy Awareness: Icons and Expression for Social Networks' in *Proceedings of the 8th Virtual Goods Workshop and the 6th ODRL Workshop*, 2010: 1–15; Ben Moskowitz and Aza Raskin, Privacy Icons. Available at: https://wiki.mozilla.org/Privacy_Icons (2011); Cornelia Graf et al, 'Final HCI Research Report.' *Primelife Project Deliverable D* 4 (2011); European Parliament. Committee on Civil Liberties, Justice and Home Affairs, *Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) [COM(2012)0011 – C7-0025/2012 – 2012/0011 (COD)]* (2013); TRUSTe, '*TRUSTe and Disconnect Introduce Visual Icons to Help Consumers Understand Privacy Policies*'. Available at: www.truste.com/blog/2014/06/23/truste-disconnect-introduce-visual-icons-to-help-consumers-understand/-privacy-policies/) (2014); PrivacyTech '*Privacy Icons'*. Available at: www.privacytech.fr/privacy-icons/ (2017); L Specht und Bienemann, 'Informationsvermittlung durch standardisierte Bildsymbole – Ein Wegaus dem Privacy Paradox?' in Louisa Specht, Nikola Werry and Susanne Werry (eds) *Handbuch Datenrecht in der Digitalisierung* (forthcoming).

79 For a literature review of existing data protection icon sets, see Arianna Rossi and Monica Palmirani, 'A Visualisation Approach for Adaptive Consent in the European Data Protection Framework' *Conference for E-Democracy and Open Government (CeDEM)* (IEEE, 2017): 159–170.

80 See generally Graf (n 78).

81 Simone Fischer Hübner and Harald Zwingelberg 'UI Prototypes: Policy Administration and Presentation-Version 2'. (2010): 19–28; Graf (n 78) 50–60; Leif-Erik Holtz, Katharina Nocun, and Marit Hansen 'Towards Displaying Privacy Information with Icons,' *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life*, (Springer, Berlin, Heidelberg, 2010): 338–348.

82 Leif-Erik Holtz, Harald Zwingelberg and Marit Hansen, 'Privacy Policy Icons,' *Privacy and Identity Management for Life* (Springer, 2011): 283.

83 European Parliament, *Draft Report*, Annex 1. The display of such icons would have constituted a legal obligation for

websites, were the amendments approved. Trace of this proposition can be found in the GDPR's call for icons.

84 John Sören Pettersson, 'A Brief Evaluation of Icons in the First Reading of the European Parliament on COM (2012) 0011' *IFIP International Summer School on Privacy and Identity Management* (Springer, 2014): 125–135.

85 Graf (n 78) 54–55.

86 This is the approach proposed in Zohar Efroni et al, 'Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing' (2019) 5(3) *European Data Protection Law Review* 352–366.

87 But see Hamza Harkous et al, 'Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning,' *arXiv preprint arXiv:1802.02561* (2018). In this respect, one viable solution for the EU context would concern the exploration of the levels of risk entailed in DPIAs.

88 See eg the 'companion icons' pattern in Haapio and Passera, Contracts as Interfaces (n 37); Rossi et al, Towards New Language (n 29).

89 See generally Susan Wiedenbeck, 'The Use of Icons and Labels in an End User Application Program: An Empirical Study of Learning and Retention' (1999) 18(2) *Behaviour & Information Technology* 68–82.

90 In the interpretation of the WP29 (Guidelines Transparency, 25), the icons are meant to enhance transparency by reducing the extreme amount of information and, upon standardisation, to be used across the continent as universal shorthand for that information. However, reducing the complexity and the potentially infinite combinations of linguistic terms into a limited set of icons is impossible and non-functional.

91 Samson Esayas, Tobias Mahler and Kevin McGillivray, 'Is a Picture Worth a Thousand Terms? Visualising Contract Terms and Data Protection Requirements for Cloud Computing Users' *International Conference on Web Engineering* (Springer, 2016): 42; Berger-Walliser et al (n 47).

92 Marit Hansen, 'Putting Privacy Pictograms into Practice-a European Perspective' (2009) *GI Jahrestagung* 154.

93 See generally Holtz, Nocum and Hansen (n 81); Pettersson (n 84); Iannella and Finden (n 78).

94 Michael S Wogalter, 'Factors Influencing the Effectiveness of Warnings' In *Visual Information for Everyday Use* (CRC Press, 2014): 102.

95 See also Sc II.

96 On participatory design, see generally Douglas Schuler and Aki Namioka, *Participatory Design: Principles and Practices* (CRC Press, 1993). Research has established that people tend to project their own beliefs and assumptions on others. User research, as a collaborative exploration between designer and user, provides a definition of the problem and of the potential areas of intervention, and steers the generation of ideas and solutions. Berger-Walliser et al (n 47) 13–14.

97 Berger-Walliser et al (n 47) 6.

98 Ibid at 22.

99 Ibid at 14. Indeed, previous research has found that it is arduous for experts to think like non-experts and, thus, symbols created by the target audience are more likely to be correctly interpreted by other members of the target audience, since they share similar mental models and cognitive profiles. See eg Patrice Caire et al, 'Visual Notation Design 2.0: Towards User Comprehensible Requirements Engineering Notations' *Requirements Engineering Conference (RE), 2013 21st IEEE International* (IEEE, 2013): 115.

100 The first workshop was organised at the Legal Design Lab, Stanford University (US) in July 2017 and developed the first prototypes of the icon set. Three further workshops were held at CIRSFID, Università di Bologna (IT) in March 2018 with the Accademia di Belle Arti di Bologna. One last workshop was organised at CIRSFID in July 2018 with the Accademia di Belle Arti di Bologna. Further details can be found in Rossi and Palmirani (n 60) and in Arianna Rossi, 'Legal Design for the General Data Protection Regulation. A Methodology for the Visualisation and Communication of Legal Concepts' PhD thesis, Alma Mater Studiorum Università di Bologna, PhD in Law, Science and Technology 31 Ciclo, (2019).

101 Hagan (n 47).

102 See next section.

103 See additional examples in Rossi and Palmirani (n 60).

104 This approach has been more thoroughly detailed in Rossi, Legal Design (n 47).

105 Sixteen individuals participated in this study, held in Stanford in August 2017. The participants' age was diverse,

while their provenance was more uniform.

106 Sixteen people participated in this in-person observations and interviews that took place in Bologna, in March 2018. The participants' ages ranged from 20 to 29 years old and the great majority were university students, indicating a high educational background. Three quarters (n=12) of the subjects described themselves as having intermediate digital skills, while half of the participants (n=8) claimed to have basic legal competence.

107 Dewar (n 66), 292.

108 See generally ISO 9186.2014:1.

109 This is also reflected in the users' explanations: such icons were described as 'universal, immediate, instantly recognisable, clear, intuitive, unmistakable' because they were 'grounded in our culture, codified and common on application software'.

110 Ten people took part in this last user study. Their age and educational level is comparable to the second study participants. Their origin was, however, more composite and the study was carried out online.

111 The icon set is available at: http://gdprbydesign.cirsfid.unibo.it/dapis-2/.

112 A helpful evaluation framework for graphical symbols whose referents are unknown is established by the international standard ISO 9186-3:2014 that introduces two consequent phases of testing: the first part aims to make users develop familiarity with the concepts (i.e. familiarity training), while the second part tests the comprehensibility of the corresponding graphical symbols (i.e. symbol referent association test). See generally ISO 9186-3:2014. *Graphical symbols – Test Methods Part 3: Method for testing symbol referent association.* However, the fitness of this methodology for the present context must be carefully gauged: we have expressed our doubts and proposed alternatives in Rossi, *Legal Design for the GDPR*. Certain is that further research must be devoted to establish a valid evaluation framework for GDPR icons.

113 I.e. the second phase of the evaluation, as anticipated in Section V.B.

114 A first step towards this goal has consisted in the establishment of the 'Privacy Icons Forum'. Available at: www.privacyiconsforum.eu/ (last accessed: 20 June 2019).

115 As other researchers have already noted, see eg Graf (n 78) 60; Esayas et al (n 91) 54.

116 Ie law, semiotics, human-computer interaction, design, computer science, cognitive psychology, philosophy, behavioural economics.

117 Indeed, the protection of personal data and privacy is one of the fundamental digital skills of the European Digital Framework for Citizens (DigComp). Joint Research Centre, *DigComp into Action. Get inspired make it happen. A user guide to the European Digital Competence Framework* (2018): 7.

118 The user studies described in this research had young highly educated participants. However, to produce generalisable results, they should be diverse in terms of age, gender, educational background, profession, technical proficiency, legal knowledge and privacy awareness.

119 See generally Rossi et al (n 29); Rossi et al (n 14).

120 See generally Haapio et al (n 16).

4

‘We’re All in This Together’

Actors Cooperating in Enhancing Children’s Rights in the Digital Environment after the GDPR

DOMENICO ROSANI[1]

Abstract

When speaking of children’s activities on the internet, the public focus has so far mostly been on online risks. However, the internet plays a paramount positive role in enhancing children’s participation in society and fulfilling their rights. Despite the pivotal relevance the digital environment has for children and the difficult balance between protection and participation components in an online setting, such topics have long been neglected. Finally, the General Data Protection Regulation (GDPR) has sparked an imperative public discussion on this issue. Against this background, the goal of this chapter is to highlight the new pathways opened by the regulation to concretely support the achievement of children’s rights in the digital environment. Despite lacking involvement from experts and children in its drafting and the reprehensible age requirement to give consent to data processing, the regulation does provide important normative tools to empower children online. To this end, its practical implementation – which needs to go beyond a merely legal approach – will be decisive. This chapter follows a multi-stakeholder approach, taking into account the different actors playing an important role in this regard, such as families, educational actors and civil society, business, public authorities, academia and research institutes. The author particularly advocates a stronger evidence-based cooperation among these actors and offers a few practical suggestions to achieve this.

Keywords

Children’s rights, data protection, digital environment, multidisciplinary cooperation, General Data Protection Regulation.

I. Introduction

Children, meaning all people under 18 years of age,[2] are nowadays important actors on the internet. From a very young age, they start using online and digital resources, both alone and

together with their parents. In this connection, they give away a considerable amount of personal data, consciously or not. While the focus of the public debate has long been on the risks of the digital environment such as sexual abuse, awareness of children's privacy and data protection issues has developed only recently. However, these are crucial topics for society as a whole, due to the vulnerability of children, the sensitivity of their data and the fact that they are future voting citizens.

This chapter aims to discuss how children's digital rights are currently acknowledged and protected in the European legal system and to highlight the new opportunities opened up by the regulation to concretely support their fulfilment. In this connection, the term 'children's digital rights' refers to the protection and achievement of children's rights in the digital environment. Such a broad understanding encompasses data protection, privacy, freedom of speech and other children's rights as notably recognised by the UN Convention on the Rights of the Child (UNCRC). It is important to note that children as rights-holders enjoy both the rights generally enshrined for 'everyone' as well as those specifically devoted to them. While they need advanced protection, children are also endowed with important rights they may – at least partially – exercise on their own.

Despite the pivotal relevance the digital environment has for children and the difficult balance between protection and participation in an online setting, the topic of children's digital rights has been neglected for a long time. The General Data Protection Regulation (GDPR), the uniform body of rules protecting personal data in the European Union (EU), has sparked a long-deserved public discussion on the issue. The stance of the regulation on children has been variously criticised. To start with, despite available research evidence, the regulation has been drafted without resorting to expert advice or involving children.[3] Moreover, its provision on consent for data processing, as provided for by Article 8, has several shortcomings.[4] However, other provisions might pave innovative ways for the fulfilment of children's rights in the digital environment. Due to their vagueness and the need for further specification, the practical implementation of these provisions will be decisive in making sure children's rights online are taken seriously. Several actors are requested to take responsibility in this regard. A multidisciplinary approach, going beyond a merely legal response, is necessary.

After a brief introduction, Section II of this chapter briefly examines the impact of the internet on children's lives, moving on to scrutinise children's lack of awareness of data processing mechanisms. The positive role of the internet for the fulfilment of digital rights is thus analysed together with the main international and European law obligations affected in this regard. The fact that children's competence develops over time and must be gradually recognised when taking decisions impacting on them, is investigated in the following subparagraph, devoted to the evolving capacities of individuals during childhood. Families are pivotal environments for the fulfilment of children's digital rights. Yet, parents often struggle to maintain a balance between oversight measures and the recognition that their children need a certain amount of online privacy.

Section III takes a closer look at the General Data Protection Regulation. After a quick overview of the policy and the legal context on data protection before its enactment, which did not sufficiently consider the specificity of children, the innovations brought by the

regulation are examined. So far, the focus of the debate has mostly been on Article 8, which introduces an age requirement for children to be able to give consent to the processing of their data. However, other provisions may turn out to be decisive for the practical empowerment of children in the digital space. Among others, this is the case for the several references within the regulation to the particularity of the situation children face online, the requirement of a child-friendly language, the possibility of drawing up codes of conduct and the enhancement of supervisory authorities' tasks. Other provisions, as those on the data protection impact assessment, profiling and the right to be forgotten, are also crucial in this connection. They all have a certain vagueness and the need of further specification on how to be implemented in common.

Section IV highlights a few practical pathways to enhance children's digital rights, relying on the new opportunities provided by the GDPR. Coordinated action by different stakeholders is imperative in this regard. The paragraph initially discusses the role of educational actors and families in providing children with digital literacy, empowering them to critically scrutinise the digital world and making use of the opportunities it provides to participate in social life. The following section sets out the role of the industry, which is encouraged to take social responsibility and attentively consider children in their policies. The role of supervisory authorities, especially in fostering such positive actions, is subsequently scrutinised. The last subparagraph is devoted to the responsibility of academia and research institutes in sparking and supporting an evidence-based cooperation among such actors, in order to provide children with a safe digital environment and empower them to take advantage of the beneficial opportunities of the internet.

II. Relevant Factors to be Considered When Debating About Children's Digital Rights

A. Hyperconnected Childhood

It is everyone's common experience that children widely use information and communication technologies (ICTs) and online resources. It has been estimated that one in three internet users is below 18 years old.[5] A presence on such sites is considered to be an essential component of social life by today's teens. Surveys carried out between 2010 and 2012 showed that at that time 38 per cent of children aged between 9 and 12 had a profile on a social network site, even though the privacy policies of most of them prohibited that. For teens aged 13 to 16, the percentage rose to 77 per cent.[6] The current relevance of a social media profile is likely to have further improved. Moreover, in recent years the intrusiveness of ICTs exacerbated and 'always on' devices have become ubiquitous.[7] Children go online on more personal devices[8] and even toys have started to be connected to the internet, tracking and predicting children's behaviour.[9] In this 'hyperconnected' reality, the boundaries between online and offline reality have become rather blurred and access to the net can hardly be

mediated by families or educational actors.[10]

When interacting with technology, a considerable amount of personal data is given away, consciously or not.[11] For instance, children – similarly to adults – publish their data to register on social media, while just their online presence leads to the collection of data by the different websites. These pieces of information create additional data, predicting relevant and potentially highly sensitive aspects of the child's life. By analysing data from the websites they most frequently visit and their actions on social media (eg 'likes' or comments) technology is now able to predict personality traits, political opinions or sexual preferences with considerable accuracy.[12] The data consciously disclosed by children may contain very personal information, including their mobile number,[13] health data, geo-localisation or personal comments stored in tracking and note-taking apps.

B. Children's Lack of Awareness on Data Processing

Such an enormous dataset of information is particularly relevant with regard to marketing, where it is used for advertising and predictive purposes. Children have become important drivers of family spending, while the fact that they are future consumers makes them interesting to business.[14] Marketing is nowadays woven into a child's daily life. A case in point is the growing phenomenon of 'influencers' on social media platforms, whose advertising component can hardly be separated from genuine content. This is particularly problematic for the youngest children who are unable to differentiate between these two components.[15] Notwithstanding their ability to deal with these technologies from a technical point of view, children's understanding of privacy, their awareness of the general context in which data processing takes place and their capacity to cope with it are, to some extent, open questions.[16] As regards Europe, the multinational research network EU Kids Online has provided important pieces of evidence-based information on the use of the internet by both children and their parents' use of the internet.[17] Research on these topics has also been carried out in North America. The project 'Young Canadians in a Wired World' has supplied valuable data, although it mainly refers to findings collected during 2013.[18] Research in the United States is being carried out by the Pew Research Center.[19]

Such surveys have highlighted that children often lack awareness about risks and rights in the online environment, especially regarding marketing and data protection, as well as the potentially long-lasting impact their activities may have. The Canadian research showed that 68 per cent of children aged 10 to 17 agreed with the statement: 'If a website has a privacy policy, that means it will not share my personal information with others.' However, this statement is false and was consciously used to test the (lack of) understanding of privacy policies by the students who were interviewed. Roughly a third of the students were unaware of the considerable attention devoted by the business to the information they posted online.[20] What is more, as developmental psychology has shown, adolescents generally struggle with long-term perspective.[21] However, one of the properties of online public spaces is precisely the indefinite persistence of the content,[22] which does not disappear after a certain period of

time.

A lack of critical understanding of how the digital environment works may lead to serious repercussions at both a societal level and more personally. Techniques, such as targeted advertising and profiling, result only make certain types of content visible to certain people. Such automatic techniques of data processing apply a 'profile' to each user, to take decisions for them or to analyse or predict their personal preferences and behaviour. Besides their marketing component, these methods may seriously affect an individual's capacity to access well-balanced information or improperly shape their preferences.[23] For instance, online searches for a certain political party may easily provide people with a disproportionate amount of news items regarding the corresponding political spectrum. Such a situation may contribute to a growing polarisation of the population and a reduction of the overall democratic character of societies, which is grounded in an objective debate by informed citizens. From an educational point of view, receiving unbalanced data and information may exacerbate the child's initial preferences, adversely impacting on their autonomy and their right to development.[24]

Finally, an unconscious and unquestioning acceptance of such data-processing methods could easily result in an uncritical acceptance of the consequent reduction of privacy or an increasing recourse to surveillance by both states and companies. The claim of protecting children could indeed cover dangerous aims, such as repressive policies by censorious governments.[25] The fact that children are future voting citizens urges a critical discussion of such topics, as well as the crucial relationship between privacy and democracy. However, the risks for the protection of one's data in relation to the widespread use of ICTs should not overshadow the extraordinary positive impact of technological developments.

C. The Internet as a Paramount Space for Children's Rights

As highlighted by research,[26] positive chances and threats go hand-in-hand in the online environment. Making use of digital opportunities may increase the risks children are exposed to, while efforts to reduce these risks could restrict a child's opportunities. Indeed, access to the internet is of critical relevance for today's children. The digital environment enables children to acquire enormous knowledge and to gain information. An extraordinary amount of data is available to every person in a way that was unimaginable only a few years ago. Such a potential access to information may have an enormous, positive impact on equality. At least theoretically, such a body of knowledge is equally accessible in low-income and high-income families, as long as there is a functioning internet connection.

Additionally, ICTs are nowadays pivotal for the development of the child's personality. They pave innovative ways to interact with peers and like-minded people. The digital environment allows children to enjoy privacy, to communicate and to search for information away from the prying eyes of adults.[27] Moreover, the absence of the constraints of face-to-face communication, such as judgements based on one's appearance, allow children to express themselves more freely.[28] Research by the Pew Research Center has shown that US teens consider the digital environment as a momentous space in which to connect with

people, helping them interact with individuals from diverse backgrounds or find different points of view.[29]

Thus, unprecedented opportunities for children to participate in societal life, increasing the overall democratic character of communities, have been launched. Indeed, ICTs allow children to show their support for causes or issues they care about, giving them a voice in the public debate.[30] They can meet up with people who share their opinions, regardless of frontiers and status, allying and making their voices heard. A case in point is the aftermath of the school shooting at the Marjory Stoneman Douglas High School, Florida, in 2018. Teenage survivors, mostly through the internet, founded the 'Never Again' movement, advocating for tighter gun regulation and becoming – according to *Time* magazine – 'the central organizers of what may turn out to be the most powerful grassroots gun-reform movement in nearly two decades'.[31] Moreover, digital services support children to become aware of, claim and enact their rights.[32] A well-connected childhood may therefore have momentous consequences for society as a whole, improving its democratic character and fostering equality. Both the UN Convention on the Rights of the Child (UN CRC) and the EU Charter of Fundamental Rights may relate in different ways to children's experience of the digital environment.

D. Legal Obligations Protecting Children's Digital Rights

On the level of international obligations, it is worth remembering that the UNCRC has been ratified by all EU Member States and is therefore legally binding for them as well as for the EU as a general principle of Union law.[33] At the same time, the EU Charter of Fundamental Rights devotes its Article 24 to 'the rights of the child' and reads as follows: Children 'may express their views freely', which 'shall be taken into consideration on matters which concern them in accordance with their age and maturity'. Moreover, 'in all actions relating to children […] the child's best interests must be a primary consideration'. The Charter, carrying the same legal status as the Treaties the Union is based upon, must be fully respected by the EU as well as by Member States when implementing Union law.

The four principles of the UNCRC[34] offer a straightforward dimension for analysing how children's rights – with them being rights-holders, not only objects of protection – are affected by ICTs. Unless specified differently, the numbers of the articles relate to UNCRC's provisions. First, the principle of non-discrimination (arising from Article 2) may be at risk because of implicit discrimination inherent in the underlying data processing. The classification of individuals carried out in this framework may reinforce social differences, for instance providing only certain types of information according to one's social status or gender or targeting individuals belonging to minority groups with enhanced surveillance.[35] The right to receive protection from economic (Article 32) and sexual exploitation (Article 34) are also affected.

Secondly, the right to life, survival and development (Article 6) entails an obligation to guarantee the child's optimal development. Such a broad concept involves a right to informational self-determination, a right to private spaces in which to develop one's identity

and to receive knowledge and instruments to strengthen children's position in society.[36] Specific rights affected in this regard are those to identity (Article 8) and privacy (Article 16); the right to have access to information and media (Article 17); the right to education (Articles 28 and 29); and the freedom of expression, thought and association (Articles 13 to 15) and play (Article 31). It should be noted that the content shall not attain any qualitative requirement to qualify as 'information and ideas' in the meaning of Article 13. Significantly, this provision – as the whole UNCRC – needs to be interpreted in a child-centred way, reflecting the peculiar ways in which children may express themselves.[37] As seen, Article 24 of the EU Charter of Fundamental Rights specifies that children 'may express their views freely'.

Thirdly, the right to be heard (Article 12) asks for the views of the children to be taken into account 'in all matters affecting the child'. This concerns both the consideration of the child's opinions when deciding about one's individual future, as well as consultations with children in light of forthcoming law or policy reforms.[38] In contrast to the freedom of expression, children's right to be heard requires the expression being addressed to a recipient.[39] The EU Charter of Fundamental Rights asks for these views to be taken into consideration on matters which concern the child in accordance with their age and maturity.

Fourthly, the principle of the best interests of the child (Article 3) must be implemented in a tailor-made way, differentiating in light of the specific situation children face. Such an obligation concerns individual decisions as well as the case of collective decisions, such as those by the legislator.[40] According to the EU Charter of Fundamental Rights, '[i]n all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration'. The flexibility of this concept both allows and requires relating with the actual capacities of the child, which are under development during childhood and therefore constantly in the making.

E. The Child's Evolving Capacities: A Sensitive Balance between Oversight and Privacy within Families

The more a child knows, has experienced and understands, the more their views must be taken into consideration. With the passing of time, their parents or the persons carrying legal responsibility for the child (hereinafter, simply: the parents) will have to transform 'guidance' and 'direction' into 'advice' and 'reminders'.[41] To acknowledge that people should be able to decide on their own marks the shift from a paternalistic to a rights-based approach. Decisions on what sphere of autonomy should be granted to children must thus consider the whole picture, taking into account the risks at stake and the actual capacities of the children concerned. Adolescents, for instance, are more likely to make bad decisions in emotionally charged situations, putting more weight on the potential benefits than on the risks.[42] However, individual children could be able to take well-balanced decisions at a younger age, once they have been provided with appropriate information, enabling them to critically understand the situation they are in. As well as in the UNCRC, the concepts of the 'evolving capacities of the child' and of their 'best interests' are recognised by the EU Charter of

Fundamental Rights. As seen, Article 24 requires the views of the child to be taken into consideration on matters which concern them ‘in accordance with their age and maturity’.

These evolving capacities are strictly intertwined with the topic of age requirements. While age thresholds allow the legal answer to be differentiated according to one’s age, they still may be critical in light of the child’s evolving capacities and best interests. They simply assume that a person of a certain age can take certain decisions, while younger ones cannot. However, every child develops at a different pace. Some could cope with a certain situation at a younger age, while older ones might not. The situation has therefore been described as ‘individualized versus average child dilemma’.[43] Despite this, age thresholds can hardly be avoided in modern legal systems. The law must provide for an abstract and generally applicable rule, in a way foreseeable by other social actors. However, an assessment of a child’s maturity on a case-by-case basis is sometimes requested for particularly relevant undertakings, such as medical treatment.[44] As the next paragraphs will show, the recognition of the child’s evolving capacities and therefore the setting of age requirements has been among the most controversial topics of the GDPR.

In the case of children who are under age, their parents are called upon to give consent in their place. In order to give an ‘informed consent’ for the processing of their children’s data, parents must be aware of all aspects at stake. Among other information, the adults must be aware of the identity of the involved subjects, the purpose of data processing and the categories of personal data concerned. Moreover, they could be interested in keeping an eye on the child’s activities, to ensure they follow the paths they have agreed upon. With the internet being a risky and complicated environment, parents may understandably be worried about their offspring’s actions. However, privacy plays a crucial role in a child’s development. Children need their own space where they are able to share thoughts, opinions and to unfold their personality without being constantly controlled by adults. Private spaces are paramount, especially for the development of the child’s sexual identity.[45] The digital environment is nowadays of momentous relevance for access both to information one would not want one’s parents to know about (eg on sexuality) and to digital spaces where interaction with peers is possible. The mere fact that parents do not legally need to keep controlling the child, once they have provided their consent and the child can from then on enjoy the privacy it longs for, is not decisive. Indeed, privacy also means the capacity to go to places your parents do not know about.[46]

However, parents’ fear that their children could act in an improper way seems to exacerbate as soon as the digital environment is concerned. Research has shown that parents are more comfortable with the child’s capacity of judgement in the offline world, rather than in the online one. Similar fears are particularly common during adolescence.[47] In this regard, various country-related attitudes are to be found in Europe as a whole as well as within the different countries.[48] Such a situation is likely to lead to enhanced surveillance measures by parents, both hierarchical (parents towards children, for instance asking for their offspring’s passwords) and hybrid (parents recruiting siblings and cousins to monitor a child).[49] A gender component has been observed in the past, too, since parents of girls were more likely to keep an eye on their actions.[50] To this end, parental control tools have been developed.

They restrict the content children can have access to, the time they spend online, activities they are allowed to carry out or monitoring and tracking what they do.[51] However, no decisive evidence was found as to the effectiveness of such tools in significantly reducing online risks.[52]

Additionally, parents' hyper-vigilance may over-state the risks children are exposed to and their capacity to cope with them. Research has shown that the awareness of rare risks such as 'stranger danger' was influenced by the sensationalist tone of the media.[53] At the same time, surveys have been underlining the growing resilience of children towards predation, bullying and offensive content they may encounter in the net.[54] Enhanced surveillance may interfere with the child's learning process to manage risky situations and become resilient.[55] The more children use the internet, the more digital skills they will gain.[56] Legal and ethical challenges also arise from the fact that parents monitoring their children may easily stumble on information about their children's peers and friends.[57]

Ultimately, parents' surveillance is likely to teach the wrong educational lesson, conveying to children the message that grown-ups do not trust them – and do not have to be trusted, because they exaggerate risks and ally with family members to spy on the child.[58] Over-surveillance does not, therefore, encourage prosocial behaviour by children. Generally, over-protective parenting has been found to negatively affect the child development.[59] Teens not subject to such an enhanced monitoring are more likely to share aspects of their online lives and resort to their parents when they need help. Conversely, the fact that children share information about their online activities also increases parents' trust in their child.[60] Given that surveillance and trust are intertwined topics, it is imperative to address them together. Authoritative advice to parents encourages children to think less about the risk, focusing instead on the many opportunities and benefits of the internet.[61]

III. Children's Digital Rights under the General Data Protection Regulation (GDPR)

A. European Legal and Policy State of the Art before the GDPR

The wider European public discussion has traditionally approached the topic of children's interaction in the digital spaces from a rather negative perspective.[62] When not completely ignored, children's behaviour online has often been linked to dangerous aspects, especially child abuse.[63] The 'risk and safety' paradigm has been dominating research, policy and practice for years.[64] At the same time, children's vulnerability as regards data protection has widely been ignored. The EU Data Protection Directive 1995, the Directive on Privacy and Electronic Communications 2002 and the Data Retention Directive 2006 carefully avoided mentioning children.[65] They therefore applied the same to both adults and children. However, an 'age-blind' approach is less neutral than it might seem, since it is implicitly based on an

adult as a subject of rights. A child's needs and vulnerabilities, however, are crucially different from those of a standard adult. Whenever children were considered, they constituted the exception to the (adult) rule. As noted by some scholars,[66] such an 'exceptionalist strategy' implicitly sees the child as introducing complications into a system modelled on an 'adult, able-bodied, English-speaking, privileged' user. Several explanations could be provided, ranging from the limited intrusiveness ICTs had until recent years in children's lives, to the fact that for a long time the European project has been mostly driven by economic considerations. Children's rights have only recently been expressly recognised in the European legal system. The 'protection of the rights of the child' only explicitly became a goal of the EU in 2009, when it was introduced into Article 3 of the Treaty on European Union. The Charter of Fundamental Rights, proclaimed in 2000, was elevated to primary EU law only in 2009.

At the policy level, in recent years, there has been a shift from a 'problematic' to a more 'proactive' approach to the digital environment.[67] The focus, originally lying on creating a 'safer' internet (eg the Safer internet Plus Programme 2005–2008 and the Safer Internet Programme 2009–2013), now lies on the provision of a 'better' internet (see the European Strategy for a Better Internet for Children).[68] As an example, the European Strategy specifically addressed the necessity of developing quality content for young people, stimulating the production of creative and education online materials by private and public actors. Other relevant policy documents, such as the EU Agenda for the Rights of the Child,[69] also recognise the positive aspects of digital innovation. As a consequence of a similar shift in perspective, there has been a noticeable increase in the discussion about children's rights.[70] The General Data Protection Regulation has added further momentum to this discussion.

B. The Regulation as an Attempt to Protect Children's Digital Rights (Without Involving Children)

An attempt to strike an adequate balance between the need for protection and children's rights at the legal level in the framework of personal data has finally been given by the General Data Protection Regulation, which came into force in May 2018. Its overall aim is to protect the fundamental rights and freedoms of natural persons, providing for a greater degree of control over one's personal data, in a uniform way throughout the European Union. The Regulation recognised that children deserve particular attention: it introduced a specific rule on consent for processing their personal data and provided for other rights and safeguards. However, the GDPR's stance on children has been widely criticised as 'limiting opportunities' and 'paternalistic'.[71] From a procedural perspective, critics particularly underline the fact that the Regulation has been drafted without an extensive consultation with children.[72] In wider terms, the GDPR has rarely been scrutinised with regards to children's data and did not rely on empirical evidence, due to the lack of confrontation between lawmakers and educational scientists throughout the whole legislative procedure.[73]

Paradigmatic for the lack of an evidence-based procedure is the setting of an age threshold for the child to consent to their data processing, which has proven to be highly problematic.

C. The Non-Evidence-Based Age Requirement of Article 8 of the GDPR

So far, the most discussed provision of the GDPR as regards children has been Article 8, which lays out the conditions for children to be able to consent to their personal data being processed in the case of an 'offer of information society services'. Such an offer is described as a service provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services (Article 4 of the GDPR, referring to Directive 2015/1535). This is a very broad scope, which is likely to involve social media as well as online gaming, instant messaging and e-mail accounts.[74] When the offer is made 'directly to a child' and the data processing relies, for its lawfulness, on the consent of the data subject themselves, the child must be at least 16 years old. Already the provision that the offer has to 'directly' address the child has sparked some hesitation, as some were doubtful if it covers offers aimed only at children, or also at 'dual-use' services, addressing both children and adults.[75] As stated in the interpretative guidelines provided by the Article 29 Working Party – the European advisory body on data protection issues, now replaced by the European Data Protection Board – only those services aimed at persons aged 18 or over should be excluded.[76] Member States can set a lower age of consent, but not below 13. Some countries have already taken positions in this regard.[77] So far, the majority of Member States have decided for, or have left, the higher threshold. Seven countries have lowered it to 13 years and five others to 14. Only France seems to have chosen to set the age requirement at 15, although a few other countries are considering it. In specific circumstances, some States already allow children to give consent at a younger age. Issues of legal coherency throughout the system are frequently invoked by Member States to justify the setting of a lower age threshold.[78]

The age requirement initially set by the Commission was 13.[79] Such a threshold would have reflected the United States standard,[80] avoiding an 'undue and unrealistic burden' for the business sector.[81] Around the end of the legislative procedure, the European threshold was suddenly increased to 16 by the Council, raising concerns from civil society and scholars.[82] Neither evidence nor expert advice was advanced,[83] nor were children consulted[84] to justify or support both the case for setting 13 as the threshold and the new age requirement. The 'opening clause', allowing States to opt for a lower age, was introduced a few weeks later in the framework of the trilogue,[85] because of the intensely negative reaction to the higher threshold.[86] However, such a clause is likely to jeopardise the standards in place in the different Member States, endangering the overall harmonisation aim of the regulation. Additionally, an age threshold at 16 does not provide for a protective environment for children between the ages of 16 and 18, which would likely be on a collision course with the UNCRC. The Convention defines as a child: 'every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier'.[87] An

exception from the rule of consent is made for preventive or counselling services offered directly to a child (recital no 38), for parents and the child could have conflicting interests or the child's privacy outweighs other considerations. However, this exception is provided only in the recital; it is not mentioned in the actual provisions of the Regulation, which makes its status uncertain.[88] It is worth remembering that recitals are interpretative tools, setting out the reasons and the goals of a certain piece of legislation. Although they could help in resolving ambiguities in the interpretation of the legal text they relate to, they are not equipped with autonomous legal effects unless drafted in clearly normative terms. Potentially, Article 8 could be interpreted restrictively, to exempt from its scope of application the services mentioned in the recital.

Underage children need the 'consent or authorisation' of the holder of parental responsibility. 'Reasonable efforts […] taking into consideration available technology' must be made to verify 'that consent is given or authorised by the holder of parental responsibility' (Article 8). While these requirements closely recall those set by the US federal legislator,[89] the feasibility of similar age verification is rather doubtful.

D. An Age Threshold Can Hardly be Implemented in the Digital Space

The debate following the enactment of the GDPR has raised the question of how to effectively implement an age threshold in the digital environment.[90] The Commission's empowerment to adopt delegated acts 'for the purpose of further specifying the criteria and requirements for the methods to obtain verifiable consent' was not reproduced in the final version of the regulation. The GDPR contains only a paragraph asking those who determine the purposes and means of the data processing (a so-called 'controller') to 'make reasonable efforts to verify […] that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology'. Interestingly, the provision does not explicitly address the need to verify the declared age and the consequent validity of the child's consent.[91] Up to now, companies usually requested a self-declaration or stated the requirement somewhere in their terms and conditions.[92] The Article 29 Working Party suggested adopting a 'proportionate approach'.[93] What is reasonable 'may depend upon the risks inherent in the processing as well as the available technology'.[94] In low-risk cases, verification via an e-mail sent to the declared parent should be sufficient, while in high-risk cases more proof could be requested, where the excessive collection of data is to be avoided.[95] As an example, a parent or guardian could be asked to make a payment of €0.01 to the controller via a bank transaction.[96] However, similar methods do not seem usefully implementable under the GDPR. Children in several European countries have the right to open a bank account or credit card account, either on their own or having been granted parental approval;[97] also in the latter scenario, once they have a bank account they are able to perform similar payments without consulting their parents. Any verification method should ensure children aged above the threshold (but still a minor) can access the service. In those countries where parental approval is required to open a bank account until

the age of majority, the requirement of a bank transaction would still make children older than 16 dependent on their parents' decision.

In theory, such a high age threshold, in combination with its broad scope of application, requires all children below the threshold to ask their parents about almost every activity they carry out in the digital environment. This situation would easily lead to a 'disturbing irritation' among parents, hindering a serious choice by them.[98] In practice, however, this rule is likely to be generally ignored, since the methods used to verify parental consent are quite weak.[99] In addition, the tendency to access the internet through individual mobile devices makes it ever-more difficult for parents to oversee their children's use of the internet.[100] Such circumstances are likely going to be used to circumvent parental consent by children who are not willing to justify their online activities to their parents[101] or who trying not to constantly bother their parents. Already, the assumption that parents should be able to better assess the situation, properly understanding how data protection works, is rather open to criticism;[102] key research gaps have been highlighted in regard to the role of parents and their skills.[103] Some scholars underlined that parents would not always be able to grasp the full potential of the digital environment for children or that there could be cases of disagreement or simply unjustified refusals to provide consent.[104]

Children who are neither able nor willing to collect the consent will likely try to gain access to online services anyway, so as not to be cut off from social networks, websites and apps. Recent surveys have shown that one child in three had a profile on a social network site even though their privacy policies prohibited that. Setting 16 as the age requirement is likely to exacerbate this situation further.[105] The negative repercussions of this situation on children's development are self-evident. On the one hand, they are told they should comply with certain rules. On the other hand, they know nothing will happen if they break them, which could result in a general lack of respect for rules in general.[106]

Several compatibility problems with the UN CRC and the EU Fundamental Rights Charter arise, where – as seen – they request that the child's views and evolving capacities be taken into consideration. A single age requirement is a 'bright-line rule', a clearly defined threshold which does not take the evolving capacities of the child into account.[107] It assumes that a child of a certain age is able to provide consent, while younger children are not. It is true that an assessment of the child's maturity on a case-by-case basis would likely turn out to be excessively burdensome.[108] However, a gradual approach, requiring parental consent at different ages according to the risk children may be exposed to in each situation, would have mitigated the adverse repercussions of age requirements. For instance, the threshold requested for a newsletter or a child-friendly gaming website could have been lower than, say, for those registering themselves in more adult gaming environments. Privacy concerns, underlining that parents could become invaders of the online activities of their teenage kids to monitor their online activities,[109] would have been partially addressed. Potentially, such a differentiated approach would have been more easily understandable for children, acknowledging their autonomy while better highlighting dangerous environments or activities. Similar risk-based requirements are provided for under US COPPA.[110] Practically,

this is also going to be the case in the EU, if the suggestions provided by the Article 29 Working Party regarding the required verification's efforts are implemented. However, while this follows a clear provision in the US, it will be the practical consequence of a large-scale disregard of legal rules in Europe. Additionally, there is no explicit room for the views of children below the threshold. Only those with parental responsibility are asked to provide consent, unless one wants to follow that opinion suggesting that the requirement of a non-clearly defined[111] 'authorisation' could veil a joint consent.[112]

E. New Opportunities Launched by the GDPR to Fulfil Children's Rights

Beyond the rule on consent, the GDPR explicitly deals with the position of children in other provisions. Despite their remarkable vagueness and the fact that they are often not provided with coercive legal effects, they could pose a decisive stimulus to develop empowering measures for children and to advocate for a better consideration of their interests into policy and legal instruments throughout Europe. This paragraph aims to briefly describe the most important of them, while the next will provide some more practical suggestions for their implementation at the national and European level.

Recital 38 recalls that children 'merit specific attention' with regard to their personal data. They 'may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data'. In addition, it calls for the aforementioned exception from Article 8: Parental consent 'should not be necessary in the context of preventive or counselling services offered directly to a child'.

Secondly, recital 58 and Article 12 tackle the need to provide children with information adapted to their level of understanding. The most common ground for a lawful processing of personal data is, both for adults and children, the 'informed' consent of the person involved. The specific information to be provided under the GDPR is more extensive in comparison with the requirements set by the 1995 Data Protection Directive.[113] However, it goes without saying that the language commonly used to collect the consent is hardly understandable by a child, who could also lack the necessary awareness and knowledge about the mechanisms behind data processing. To consider the child's consent as 'informed', the information notice needs to be delivered using appropriate language so that people understand what they are consenting to and for what purposes, avoiding overly complicated legal or technical jargon.[114] While the recital asks for 'a clear and plain language that the child can easily understand', Article 12 states that the information should be provided 'in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child'. The language used to address children of different age groups must be adapted to the corresponding level of understanding, potentially providing different versions of the privacy notice; graphics, cartoons and videos could be taken into consideration.[115] Appropriate informative tools for children with disabilities should also be available.

Thirdly, associations and other bodies could prepare codes of conduct, specifying the

application of the GDPR in various processing sectors. This also applies to the information provided to children and their protection, as well as to the manner in which to obtain the consent of the holders of parental responsibility (Article 40). Member States, supervisory authorities, the European Data Protection Board and the Commission shall encourage the drawing up of codes of conduct.

Fourthly, among national supervisory authorities' tasks the regulation lists the promotion of 'public awareness and understanding of the risks, rules, safeguards and rights in relation to [data] processing' (Article 57). In this regard, 'activities addressed specifically to children shall receive specific attention'.

Fifthly, 'profiling' (Article 22) refers to those automatic data processing techniques applying a 'profile' to a certain user, particularly to take decisions concerning them or for analysing or predicting their personal preferences, behaviours and attitudes.[116] According to recital 71, such measures 'should not concern a child'. This provision could lead to the conclusion that profiling of children is prohibited, even if any Article explicitly expresses it.[117] The Article 29 Working Party, however, has a different view, namely that there is not an absolute prohibition.[118] Irrespective of interpretation issues raised by the interrelationship of recital 71 with Article 22,[119] it is worth asking whether such a (partial) prohibition will be practically implementable, distinguishing between adults and children without excessively interfering into users' privacy.[120] What if, for instance, a child uses their parent's device? Even if a child possesses their own device, should they have to be recognisable as such by industry actors, so that they cannot access certain services provided for grown-ups or to ensure the commercial content shown to them is age-appropriate and clearly distinguishable?

Sixthly, a special treatment for children regarding the 'right to be forgotten' is provided by recital 65 and Article 17. This term refers to the possibility to have data erased and is therefore more properly defined as 'right to erasure'.[121] It grounds on the assumption that individuals should be able to evolve beyond their past, in spite of the 'persistence' which characterises the internet. According to the recital, such a right 'is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing'. The exercise of such a right should not be impeded 'by the fact that he or she is no longer a child'. Consequently, Article 17 provides for a right to have personal data erased as long as the data was collected in relation to services offered directly to the child, in the framework of Article 8. In this case, the data must be erased upon a simple request. It should be noted that, according to Article 7(3), to withdraw one's consent should be as easy as to give it. Hence, the same age requirements should apply for children to provide or withdraw consent.

Furthermore, other GDPR provisions may be relevant for children. Among those are data portability, the so-called 'data privacy by design and by default' principle and the data protection impact assessment.[122] These are 'age-blind' instruments, which do not take into account the age or capacity of the user but provide certain rights to everyone.

The right to data portability is grounded on Article 20 of the GDPR. It allows for users to receive the personal data they have provided in a structured, commonly used and machine-readable format. The purpose is to be able to transmit this data to another data controller.[123]

This would enable children, for instance, to avoid being hemmed in into social networks they chose at a younger age and easily move on to 'better' ones that were not available before. Interestingly, the applicability of this provision for children is not specifically thematised, nor has it been examined by the Article 29 Working Party in its guidelines.[124] Even though all children as data subjects hold such a right, it is debatable if the latter may be exercised by children themselves, after they have attained a certain age or only through their parents. Such a procedural question may play a decisive role in the actual implementation of the right to data portability in the case of children.

'Data protection by design and by default' (Article 25 GDPR) refers to the fact that companies and organisations shall build data protection safeguards into their services from the very beginning ('by design') and ensure that personal data 'by default' is processed with the highest privacy protection and is not made accessible to an indefinite number of people. This provision is particularly relevant for children who might lack the necessary skills to manage their privacy settings. As an example, icons may convey a more intelligible overview of certain processing than the child may be interested in; an easy access to the transparency tools or the exclusion of children from profiling are also mentioned in this connection.[125]

Lastly, the 'data protection impact assessment' (generally known as DPIA) is an appraisal of the impact of certain data processing operations, where it is likely to result in a high risk to the rights and freedoms of natural persons (Article 35 GDPR). The purpose is to identify and minimise the risks, prior to the data processing. According to the Article 29 Working Party, one of the criteria to assess if the processing may result in a high risk is the vulnerability of the subjects concerned. As explicitly stated, '[v]ulnerable data subjects may include children […]'.[126] Consequently, the DPIA could be a powerful tool to protect children's rights and force data controllers to think about children up front.[127]

IV. A Few Pathways to Empower Children Online

A. To Start with, Let's Avoid Simplistic Answers

The reconciliation of child's protection and rights in the digital world is highly complicated. Simplistic answers, focusing on specific components of the problem while missing the bigger picture, could easily prove to be inefficient. The child would not be efficiently protected and/or their access to the ICTs unreasonably restricted. A legal response would fall short as it would be unable to appropriately grapple with the situations children are facing. General and abstract rules can hardly cope with the specificity of every situation a child may experience and with the steadily changing technologies. Indeed, the way technological innovation will impact on children's lives in the future can hardly be foreseen.[128]

More than a rule for consent only, a truly protective environment needs a prior empowerment through the provision of relevant knowledge and skills. In this regard, empowering children means to equip them with 'the necessary capabilities for interpreting

and acting upon a social world that is intensively mediated by the new media'.[129] Today's society demands new and more sophisticated skills to cope with its ceaseless development.[130] However, there can be little doubt that providing children with digital literacy does not, as such, reduce risks. On the contrary, the more children are able to use devices and surf the net, the more online risks they will encounter. At the same time, higher digital competence leads to more opportunities, because children need to encounter risks to learn and gain resilience.[131] Opportunity and risk are closely intertwined. Consequently, an effective digital and media literacy is a crucial step to enable children to cope with potential harmful content and behaviour and to make the best of their online opportunities.

B. The Role of Families and Educational Actors for Digital Literacy, Encouraging Children to Critically Interrogate the Whole Picture

There can be no doubt that, nowadays, the right to education also covers digital issues. As emphasised by the UN Committee on the Rights of the Child, 'training and support should be provided as part of the basic education curriculum to ensure the development of adolescents' digital, information and media and social literacy skills'.[132] However, public institutions and especially national data protection authorities have so far shown several shortcomings, while citizens' awareness about children's rights in the digital environment is lacking.[133] Families need to be more aware of the interests at stake, to provide children with appropriate guidance.[134] Parents should be conscious of the importance of private spaces for their child's development. Research has amply shown that the full pedagogical potential of digital devices and services is largely under-explored in many households.[135] Regardless of the increasingly blurred boundaries between online and offline reality and the internet being integrated in everyone's life throughout the day, most parents still tend to focus on restricting children's 'online time' rather than on discussing content.[136] Since younger kids learn intensely through interaction with the familiar environment, parents should also personally set an example.[137] For instance, avoiding sharing excessively detailed information and pictures of their children (so called 'sharenting') or to unreasonably stick to their smartphones while children are around.[138] The whole family in the broader sense should take responsibility. Siblings, grandparents, relatives are important reference points for the child,[139] who may be happier to share thoughts with them, or ask for their help, rather than their parent's.

Furthermore, the commitment to an effective digital and media literacy should involve all the different actors with whom children are in contact. Indeed, relying just on the efforts of the family could exacerbate social inequalities, owing to the fact that parents could lack sufficient digital skills, as well as knowledge about privacy issues and time to adequately address them.[140] Schools, in particular, are best placed to reach the majority of children, regardless of age, income or background.[141] Informal educational settings are also relevant, both to connect formal literacy programmes with out-of-school media practices and to reach out to those children not attending school. As people start using the internet at very young ages, digital and media literacy should also begin in early childhood.[142] Legal thresholds

asking for parental permission below 16 should not prevent a serious commitment by schools before that age.

Educational initiatives should provide practical skills to children, for instance on how to de-tag oneself from a social media post, manage privacy settings and exercise rights such as that to data portability. Children should also be fostered in the production of creative content or in the carrying out of civic activities online. Despite the fact that both are crucial components of the 'ladder of opportunities', many children still do not reach this level of competence and engagement.[143] However, digital literacy should go beyond mere practical skills. Educational campaigns should encourage children to critically interrogate the methods of online marketing and the role privacy plays in their lives and in democratic societies.[144] They should spark awareness on what personal data is, what their rights are and what the risks are when sharing information online.[145] The positive and negative repercussions of a widespread access to ICT on equality, also concerning gender and disability, should be discussed. Digital and media literacy should provide children with a critical understanding of the whole social and economic effects of digital innovation and of the power dynamics at stake.[146] To this end, discussions among peers and with other reference groups, such as teachers or families, constitute an essential component of critical thinking about the issues at stake.[147]

C. The Role of the Business, Taking Responsibility for Children's Rights and Drawing Up Codes of Conduct

The link between business and (children's) human rights has been the object of important resolutions in recent years both by the Council of Europe[148] and at the United Nations and NGO level.[149] They underline how business should meet their responsibility to respect children's rights and commit to supporting them. At the same time, they call for states to encourage business to consider the rights of the child when carrying out human rights due diligence and to involve all relevant stakeholders in the elaboration and implementation of policies on matters which are particularly sensitive with regard to children's rights.

The sincere involvement of economical actors is decisive in the aftermath of the GDPR, since many child-empowering measures within it are self-regulatory.[150] The business sector should thus be supported in its duty to provide clear explanations for children on how data is collected and used. Examples of how terms and conditions could be drafted in a child-friendly manner already exist.[151] Moreover, practical tools to easily exercise the rights provided by the GDPR should be developed. These should differentiate according to the child's age and/or preference. A tool developed for younger children would make broader use of pictures and videos, while the same tool for teenagers – or children willing to know more – could also rely on infographics and written text. Similarly, tools for children with disabilities should be available. Information sheets for parents could also be developed, aiming to provide them with child-friendly information they can rely on to discuss the issues with their offspring.

To this end, codes of conduct are a powerful tool.[152] Article 40 of the GDPR lists among the aspects which may be specified by codes of conduct 'the information provided to and the protection of, children and the manner in which the consent of the holders of parental responsibility over children is to be obtained'. Voluntary codes have, so far, not had great success,[153] but, in the aftermath of the GDPR's launch, they constitute the possibility for children's rights scholars and practitioners, as well as civil organisations, to closely cooperate with the industry. Their input would help in making business actors more aware of the great burden of responsibility they carry, as well as positively influence the policies concretely applied, especially by middle-sized and small companies. Such companies, indeed, are likely to adopt the suggestions provided by the codes, since the GDPR provides several incentives in this regard.

Furthermore, codes of conduct may turn out to be flexible methods of setting standards addressing children's vulnerabilities in specific sectors.[154] For instance, a code could show how to ensure that any age verification measure takes into account the available technology and complies with fundamental rights.[155] In addition, a code could spark positive internal policies, like awareness trainings about children's rights.

Since draft codes prepared by associations and other bodies must be approved by the competent data protection supervisory authority, these should be spurred to have a particular closer look at the measures regarding children's rights. What's more, Article 41 provides for an independent body to monitor compliance with a code of conduct. As this must own 'an appropriate level of expertise in relation to the subject-matter of the code', educational and legal experts with profound knowledge of children's rights data protection issues should be involved. To this end, however, a corresponding 'persuasion' effort by supervisory authorities, them being in charge of the independent bodies' accreditation, seems indispensable.

D. The Role of Supervisory Authorities in Sensitizing and Supporting All the Actors

According to Article 57 of the GDPR, supervisory authorities should generally promote public awareness and understanding of the risks, rules, safeguards and rights in relation to data processing; activities addressed specifically to children 'shall receive specific attention' (lit. b). Additionally, they have to promote the awareness of controllers and processors of their obligations (lit. d); encourage the drawing up of codes of conduct (lit. m); and publish the criteria for accreditation and conduct the accreditation, of a body for monitoring codes of conduct (lit. p and q). Consequently, supervisory authorities play an important role in sensitising and fostering the different stakeholders in taking responsibility for children's digital rights. They should support the delivery of those programmes already mentioned in the framework of formal and informal educational settings and provide guidance for the drawing up of codes of conduct. In addition, authorities should encourage national decision-makers to implement a children's rights impact assessment into the policy-making and law-making process. At the European level, the EU Agenda for the Rights of the Child[156] already

recognises that the rights of the child are one of the fundamental rights to consider in the framework of the fundamental rights check that EU legislative proposals must undergo.[157] Similar impact assessments should take place at the national level, taking into account policy and legal measures likely to remarkably affect children's rights.

On a final note, the European Data Protection Board should offer an authoritative clarification of the exclusion from the rule of consent of preventive or counselling services offered directly to a child, as provided for by recital 38. Such a clarification seems unavoidable in order to ensure the consistent application of the GDPR, therefore falling into its competence as listed in Article 70 of the regulation.

E. The Role of Academia and Research Institutes for an Evidence-Based Multistakeholder Cooperation

As shown, an overarching response to the challenges children face online requires the interdisciplinary cooperation of legal and educational actors, families, business, civil society organisations, as well as an inter-institutional collaboration of various public bodies. Actors dealing exclusively with ICT-related topics will have to work closely with those responsible for children's rights and family issues and the other way around.[158] Academia, as well as public and private research institutes, could give momentum to this dialogue. Important pieces of research have already been carried out on children's interactions in the digital world, leading to a significant body of knowledge. While the continual development of technology makes constant research unavoidable, available research findings should trigger a more attentive discussion on children's digital rights. To stimulate such an exchange,[159] researchers should be encouraged to consider the practical implementation of their work more. As an example, this could happen through specific funding schemes for impact-orientated research or the enhanced consideration in rankings and the academic careers of the social impact of one's output. An important part of the scholars' work could consequently be represented by the dissemination to relevant social actors of the research findings, for instance through practical guidelines and the use of business-friendly language. Conversely, on the side of industry players and decision-makers, the independency of research should be ensured and a merely utilitarian usage of scholars' input avoided.

To allow for such an evidence-based exchange, coping with the constant development of technologies, permanent clusters are essential. They should involve all the mentioned actors – educational actors, industry, decision-makers, families, research actors, civil society –, together with representatives of children. Indeed, a bottom-up approach is pivotal to ensure the solutions provided effectively meet the challenges the youngest among us are facing. Children need to be involved in such clusters from the very beginning. In this regard, attention should be paid to diversifying their representation and to considering the different genders, geographical and social origins and children with specific needs as those with disabilities.

To avoid a jeopardisation of standards among the European Union, coordination among countries – potentially via cross-border clusters – must be ensured.

V. Conclusions

Regulating children's digital rights has proven to be particularly challenging. Due to the close link between online risks and opportunities, a rather over-protective approach is likely to unduly restrict children's rights. Indeed, nowadays, online spaces are paramount for the development of the child's personality and offer extraordinary opportunities to children to participate in social life, making their voice heard and increasing equality and the overall democratic character of society. However, risks connected to the digital environment need to be adequately addressed. This chapter has specifically focused on the data protection risks. Fundamental rights, although mainly enacted in a pre-digital era, need to be implemented dynamically, ensuring that the crucial interests of children are not sacrificed on the altar of a simplistic societal answer. Families, in their broader meaning, are asked to provide children with a safe environment in which to take advantage of the opportunities of the internet. However, the balance between overseeing children's activities and recognising private spaces, is highly demanding. Placing such a burden only on families is likely to negatively impact on equality, due to the different knowledge, skills and (time) availability parents and other family members may have.

Thus, other actors need to take responsibility. Educational actors are requested to provide children with adequate digital literacy. Besides imparting children technical skills and the competence to proactively take advantage of the online opportunities, digital literacy should also invite them to critically approach the digital environment and scrutinise its methods. Awareness and competence-enhancing campaigns towards families could be developed. The industry should become more aware of the responsibility it carries, attentively considering children's rights and needs when setting their policies. In the aftermath of the GDPR, codes of conduct and the corresponding monitoring bodies are likely to turn out to be powerful tools in this regard. Showing social responsibility towards digital rights may also be advantageous for business, fostering social trust in them. Public authorities, especially supervisory authorities, play an important role in encouraging the different stakeholders in this, fostering and monitoring their efforts. Lastly, academia as well as private and public research institutes should keep on providing evidence-based advice, paying particular attention to the social impact of their work.

Besides critical shortcomings, the GDPR has played an important role in the enhancement of children's rights in the online environment. It has sparked a long-deserved public discussion on such topics, while it provides important normative tools to foster children's digital rights. For instance, the regulation requires a child-friendly language to be applied when providing children with information. It calls on companies and organisations to think about children up front, via the data protection impact assessment or the 'data protection by design and by default' principle. Additionally, national supervisory authorities should devote specific attention to children when promoting public awareness and understanding of data protection issues. The regulation also provides children with relevant rights, for instance in connection to the right to be forgotten and the right to data portability.

However, the way these provisions will find implementation is going to be decisive with regard to their effectiveness. While the regulation's enactment has neither relied on evidence-

based advice, nor has it considered children's views, it is now time to catch up on these fronts. The implementation of the regulation should be accompanied by the setting up of permanent clusters, where the different actors – including children – may cooperate in shaping its practical application. Such multidisciplinary clusters will plausibly turn out to be efficient frameworks, where to work on normative and practical solutions for safely enhancing children's rights and participation in the digital environment.

References

30th International Conference of Data Protection and Privacy Commissioners, 'Resolution on Children's Online Privacy' (Strasbourg 17 October 2008).

38th International Conference of Data Protection and Privacy Commissioners, 'Resolution for the Adoption of an International Competency Framework on Privacy Education' (Marrakesh 18 October 2016).

Anderson M and Jingjing Jiang, 'Teens' Social Media Habits and Experiences' (2018). Available at: www.pewinternet.org/wp-content/uploads/sites/9/2018/11/PI_2018.11.28_teens-social-media_FINAL2.pdf.

Article 29 Working Party, 'Opinion 15/2011 on the definition of consent' (2011).

——, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679: WP 248 rev.01' (2017).

——, 'Guidelines on the right to data portability: WP 242 rev.01' (2017).

——, 'Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679: WP 251 rev.01' (2018).

——, 'Guidelines on consent under Regulation 2016/679: WP 259 rev.01' (2018).

Atkinson L, 'Interpreting the Child-Related Provisions of the GDPR' (2018) 23(1) *Communications Law* 31.

boyd d, 'Taken Out of Context: American Teen Sociality in Networked Publics' (Dissertation, University of California, 2018).

Buitelaar JC, 'Child's Best Interest and Informational Self-determination: What the GDPR can Learn from Children's Rights' (2018) 8(4) *International Data Privacy Law* 293.

Byrne J and Burton P, 'Children as Internet Users: How Can Evidence Better Inform Policy Debate?' (2017) 2(1) *Journal of Cyber Policy* 39.

Calvert SL, 'Children as Consumers: Advertising and Marketing' (2008) 18(1) *The Future of Children* 205.

Charlotte Alter, 'The Young and the Relentless: Adults have failed to stop school shootings. Now it's the kids' turn to try' *Time* (2 April 2018).

Chaudron S, Di Gioia R and Gemo M, 'Young Children (0–8) and Digital Technology. A Qualitative Study Across Europe' (2018).

Council of Europe, 'The protection of individuals with regard to automatic processing of personal data in the context of profiling: Recommendation CM/Rec(2010)13 and explanatory memorandum' (2010).

——, 'Recommendation CM/Rec(2016)3 of the Committee of Ministers to member States on human rights and business' (2016).

——, 'Strategy for the Rights of the Child (2016–2021)' (Strasbourg 2016).

——, *Internet Literacy Handbook* (Council of Europe, 2017).

Crone EA, *The Adolescent Brain: Changes in Learning, Decision-making and Social Relations* (Routledge, 2016).

d'Haenens L, Vandoninck S and Donoso V, 'How to Cope and Build Online Resilience?' (2013). EU Kids Online. Available at: eprints.lse.ac.uk/48115/.

Dias P et al, 'The Role of Parents in the Engagement of Young Children with Digital Technologies: Exploring Tensions between Rights of Access and Protection, from "Gatekeepers" to "Scaffolders"' (2016) 6(4) *Global Studies of Childhood* 414.

Donoso V et al, 'Faraway, So Close: Why the Digital Industry Needs Scholars and the Other Way Around' (2016) 10(2) *Journal of Children and Media* 200.

Dürager A and Livingstone S, 'How Can Parents Support Children's Internet Safety?' (2012). EU Kids Online. Available at: eprints.lse.ac.uk/42872/.

European Commission, ‘Strategy for the Effective Implementation of the Charter of Fundamental Rights by the European Union: COM(2010) 573 final’ (19 October 2010).
——, ‘An EU Agenda for the Rights of the Child: COM(2011) 60 final’ (15 February 2011).
——, ‘Impact Assessment Accompanying the General Data Protection Regulation and the Directive on the Protection of Individuals: SEC(2012) 72 final’ (25 January 2012).
——, ‘Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation): COM(2012) 11 final’ (25 January 2012).
——, ‘European Strategy for a Better Internet for Children: COM(2012) 196 final’ (2 May 2012).
European Union Agency for Fundamental Rights (FRA), ‘Mapping Minimum Age Requirements Concerning the Rights of the Child in the EU. Dataset “Age requirements and health”’ (2017). Available at: fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements-concerning-rights-child-eu.
——, ‘Mapping Minimum Age Requirements Concerning the Rights of the Child in the EU “Issuance of a credit card” and “Age at which a child can open a bank account, with parental consent”’ (2017). Available at: fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements-concerning-rights-child-eu.
European Union Agency for Fundamental Rights (FRA) et al, *Handbook on European Data Protection Law*: 2018 edition (Luxembourg, Publications Office of the European Union, 2018).
European Union Agency for Fundamental Rights (FRA) and Council of Europe, *Handbook on European Law Relating to the Rights of the Child* (Publications Office of the European Union, 2015).
Garante per la protezione dei dati personali, ‘Parere sullo schema di decreto legislativo recante disposizioni per l’adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679’ (2018). Available at: www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9163359.
Janssens A et al, ‘Parents’ and Adolescents’ Perspectives on Parenting: Evaluating Conceptual Structure, Measurement Invariance, and Criterion Validity’ (2015) 22(4) *Assessment* 473.
Jasmontaite L and De Hert P, ‘The EU, Children under 13 Years, and Parental Consent: A Human Rights Analysis of a New, Age-based Bright-line for the Protection of Children on the Internet’ (2015) 5(1) *International Data Privacy Law* 20–33.
John Carr, ‘An open letter to the European Data Protection Supervisor and the Chair of the Article 29 Working Party’ (2017). Available at: www.lse.ac.uk/media@lse/documents/MPP/eNACSO-letter-re-GDPR.pdf.
Krivokapić Đ and Adamović J, ‘Impact of General Data Protection Regulation on Children’s Rights in Digital Environment’ (2016) *Belgrade Law Review* 205.
Livingstone S et al, ‘EU Kids Online II. Final Report’ (2011). EU Kids Online. Available at: eprints.lse.ac.uk/39351/.
——, ‘Risks and Safety on the Internet. The Perspective of European Children: Full Findings and Policy Implications from the EU Kids Online Survey of 9–16-year-olds and their Parents in 25 Countries’ (2011). EU Kids Online. Available at: eprints.lse.ac.uk/33731/.
Livingstone S, Carr J and Byrne J, ‘One in Three: Internet Governance and Children’s Rights’ (2016). Unicef Office of Research-Innocenti Discussion Paper 2016-01.
Livingstone S and Ólafsson K, ‘Risky Communication Online’ (2011). EU Kids Online. Available at: eprints.lse.ac.uk/33732/.
Livingstone S and Third A, ‘Children and Young People’s Rights in the Digital Age: An Emerging Agenda’ (2017) 19(5) *New Media & Society* 657.
London School of Economics and Political Science, ‘EU Kids Online. Findings – Methods – Recommendations’ (2014). EU Kids Online. Available at: eprints.lse.ac.uk/60512/.
Longfield A, ‘How Parents and Carers can Support their Children to Manage their Rights and Privacy Online’ (2017). Available at: www.childrenscommissioner.gov.uk/2017/11/28/how-parents-and-carers-can-support-their-children-to-manage-their-rights-and-privacy-online/.
Macenaite M, ‘From Universal Towards Child-specific Protection of the Right to Privacy Online: Dilemmas in the EU General Data Protection Regulation’ (2017) 19(5) *New Media & Society* 765.
Macenaite M and Kosta E, ‘Consent for Processing Children’s Personal Data in the EU: Following in US Footsteps?’ (2017) 26(2) *Information & Communications Technology Law* 146.
Madden M et al, ‘Teens, Social Media, and Privacy’ (2013). Available at: www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/.
Mansell R, ‘From Digital Divides to Digital Entitlements in Knowledge Societies’ (2002) 50(3) *Current Sociology* 407.
Mantelero A, ‘Children Online and the Future EU Data Protection Framework: Empirical Evidences and Legal Analysis’ (2016) 2(2/3/4) *International Journal of Technology* 175.
McCullagh K, ‘The General Data Protection Regulation a Partial Success for Children on Social Network Sites’ in Tobias Bräutigam and Samuli Miettinen (eds), *Data Protection, Privacy and European Regulation in the Digital Age* (Unigrafia,

2016) 110–139.
Milkaite I and Lievens E, ‘The Changing Patchwork of the Child’s Age of Consent for Data Processing across the EU (January 2019)’. Available at: www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=3017751.
Milkaite I and Verdoodt V, ‘The General Data Protection Regulation and Children’s Rights: Questions and Answers for Legislators, DPAs, Industry, Education, Stakeholders and Civil Society: Roundtable Report, Brussels, 23 June 2017’. Available at: www.betterinternetforkids.eu/documents/167024/2013511/GDPRRoundtable_June2017_FullReport.pdf.
Morgan A, ‘The Transparency Challenge Making Children Aware of their Data Protection Rights and the Risks Online’ (2018) 23(1) *Communications Law* 44.
Ólafsson K, Livingstone S and Haddon L, ‘Children’s Use of Online Technologies in Europe. A Review of the European Evidence Base’ (2014). EU Kids Online. Available at: eprints.lse.ac.uk/50228/.
Reid AS, ‘Online Protection of the Child within Europe’ (2009) 23(3) *International Review of Law, Computers & Technology* 217.
Reyna VF and Farley F, ‘Risk and Rationality in Adolescent Decision Making’ (2006) 7(1) *Psychological Science in the Public Interest* 1.
Rosani D, ‘Child’s Participation Online and the General Data Protection Regulation – A Dialogue between Educational and Legal Sciences is Urgently Needed’ (2018) Special Issue *merzWissenschaft* 41–52.
Save the Children, United Nations Global Compact and Unicef, ‘The Children’s Rights and Business Principles’ (2012).
Savirimuthu J, ‘Article 8 General Data Protection Regulation: Has Anyone Consulted the Kids?’ LSE blog. Available at: blogs.lse.ac.uk/mediapolicyproject/2016/03/01/eu-general-data-protection-regulation-article-8-has-anyone-consulted-the-kids/.
——, ‘Networked Children, Commercial Profiling and the EU Data Protection Reform Agenda: In the Child’s Best Interests?’ in Ingi Iusmen and Helen Stalford (eds), *The EU as a Children’s Rights Actor: Law, Policy and Structural Dimensions* (Barbara Budrich Publishers, 2016) 221–257.
Staksrud E and Milosevic T, ‘Adolescents and Children in Global Media Landscape: From Risks to Rights’ (2017) 41(3–4) *Annals of the International Communication Association* 235.
Stald G et al, ‘Online on the Mobile: Internet Use on Smartphones and Associated Risks among Youth in Europe’ (2014). EU Kids Online. Available at: eprints.lse.ac.uk/59960/.
Steeves V, ‘Young Canadians in a Wired World Phase III: Talking to Youth and Parents about Life Online’ (2012).
——, ‘Young Canadians in a Wired World, Phase III: Online Privacy, Online Publicity’ (2014).
——, ‘Now You See Me: Privacy, Technology, and Autonomy in the Digital Age’ in Gordon DiGiacomo (ed), *Human Rights: Current Issues and Controversies* (University of Toronto Press, 2016).
——, ‘Swimming in the Fishbowl: Young People, Identity and Surveillance in Networked Spaces’ in Irma van der Ploeg and Jason Pridmore (eds), *Digitizing Identities: Doing Identity in a Networked World* (Routledge, 2016) 125–139.
Steeves V, Milford T and Butts A, ‘Summary of Research on Youth Online Privacy’ (2010). Available at: www.priv.gc.ca/media/1731/yp_201003_e.pdf.
Steeves V and Regan P, ‘Young People Online and the Social Value of Privacy’ (2014) 12(4) *Journal of Information, Communication and Ethics in Society* 298.
Terras MM and Ramsay J, ‘Family Digital Literacy Practices and Children’s Mobile Phone Use’ (2016) 7(1957) *Frontiers of Psychology* 1–11.
Tobin J and Parkes A, ‘Article 13: The Right to Freedom of Expression’ in John Tobin (ed), *The UN Convention on the Rights of the Child: A Commentary*, 1st edn (Oxford University Press, 2019).
UK Information Commissioner’s Office, ‘Consultation: Children and the GDPR Guidance’ (2018).
Unicef, *Children in a Digital World* (Unicef, 2017).
United Nations Committee on the Rights of the Child, ‘General measures of implementation of the Convention on the Rights of the Child (Arts 4, 42 and 44, para 6): CRC/GC/2003/5’ (27 November 2003).
——, ‘General comment No 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (Art 3, para 1): CRC/C/GC/14’ (29 May 2013).
——, ‘General comment No 20 (2016) on the implementation of the rights of the child during adolescence: CRC/C/GC/20’ (6 December 2016).
van der Hof S, ‘I Agree, or Do I?: A Rights-Based Analysis of the Law on Children’s Consent in the Digital World’ (2016) 34(2) *Wisconsin International Law Journal* 409.
van der Hof S and Lievens E, ‘The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children’s Personal Data under the GDPR’ (2018) 23(1) *Communications Law* 33.
Zaman B and Nouwen M, ‘Parental Controls: Advice for Parents, Researchers and Industry’ (2016). EU Kids Online. Available at: eprints.lse.ac.uk/65388/.

[1] Department of Italian Law, University of Innsbruck. The author would like to thank all the friends and colleagues who contributed to this chapter with important insights. Thank you also to the reviewers for their very valuable comments.

[2] According to the United Nations Convention on the Rights of the Child, 'a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier' (Art. 1).

[3] On this topic see Section III.B.

[4] On this topic see Section III.C and D.

[5] S Livingstone, J Carr and J Byrne, 'One in Three: Internet Governance and Children's Rights' (Florence 2016). Unicef Office of Research-Innocenti Discussion Paper 2016-01 15 f.

[6] European Commission, 'Impact Assessment Accompanying the General Data Protection Regulation and the Directive on the Protection of Individuals: SEC(2012) 72 final' (25 January 2012) 23; S Livingstone et al, 'Risks and Safety on the Internet. The perspective of European Children: Full Findings and Policy Implications from the EU Kids Online Survey of 9–16-year-olds and their Parents in 25 Countries' (2011). EU Kids Online. Available at: eprints.lse.ac.uk/33731/; S Livingstone et al, 'EU Kids Online II. Final Report' (2011). EU Kids Online 18. Available at: eprints.lse.ac.uk/39351/. As regards the situation in Canada, see V Steeves, 'Young Canadians in a Wired World, Phase III: Online Privacy, Online Publicity' (2014) 13.

[7] L Jasmontaite and P De Hert, 'The EU, Children under 13 Years, and Parental Consent: A Human Rights Analysis of a New, Age-based Bright-line for the Protection of Children on the Internet' (2015) 5(1) *International Data Privacy Law* 20–33, 20.

[8] EU Kids Online in 2014 has highlighted a key research gap as regards mobile technologies: G Stald et al, 'Online on the Mobile: Internet use on Smartphones and Associated Risks among Youth in Europe' (2014). EU Kids Online. Available at: eprints.lse.ac.uk/59960/; see also Stald et al (n 10), or the project 'Net Children Go Mobile', which finished in December 2014.

[9] Privacy concerns have been raised in recent years in this regard. For instance, in 2017 Germany banned a children's doll due to the unlawful transmission of data recorded by the internal camera and microphones. See also Bundesnetzagentur, Press Release: 'Bundesnetzagentur removes children's doll 'Cayla' from the market' (2017). Available at: www.bundesnetzagentur.de/SharedDocs/Downloads/EN/BNetzA/PressSection/PressReleases/2017/17022017_cayla.pdf?__blob=publicationFile&v=2.

[10] P Dias et al 'The Role of Parents in the Engagement of Young Children with Digital Technologies: Exploring Tensions between Rights of Access and Protection, from "Gatekeepers" to "Scaffolders"' (2016) 6(4) *Global Studies of Childhood* 41, 44; V Donoso et al, 'Faraway, so Close: Why the Digital Industry needs Scholars and the Other Way Around' (2016) 10(2) *Journal of Children and Media* 200, 201.

[11] S van der Hof, 'I Agree, or Do I: A Rights-Based Analysis of the Law on Children's Consent in the Digital World' (2016) 34(2) *Wisconsin International Law Journal* 409, 412.

[12] Ibid at 412 ff.

[13] Research has observed an increase of the number of children sharing their cell phone number on social media, from 2% in 2006 up to 20% in 2012; interestingly, most of them were boys rather than girls: M Madden et al, 'Teens, Social Media, and Privacy' (2013) 3. Available at: www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/.

[14] van der Hof (n 11), 416.

[15] SL Calvert, 'Children as Consumers: Advertising and Marketing' (2008) 18(1) *The Future of Children* 205, 217.

[16] J Byrne and P Burton, 'Children as Internet Users: How Can Evidence Better Inform Policy Debate?' (2017) 2(1) *Journal of Cyber Policy* 39, 46.

[17] See the network's website London School of Economics and Political Science, 'EU Kids Online: Enhancing Knowledge of European Children's Online Opportunities, Risks and Safety'. Available at: www.lse.ac.uk/media-and-communications/research/research-projects/eu-kids-online.

[18] Research in Canada has been carried out especially by Valerie Steeves (n 6).

[19] See recently, M Anderson and Jingjing Jiang, 'Teens' Social Media Habits and Experiences' (2018). Available at: www.pewinternet.org/wp-content/uploads/sites/9/2018/11/PI_2018.11.28_teens-social-media_FINAL2.pdf.

[20] Steeves (n 6) 38.

[21] EA Crone, *The Adolescent Brain: Changes in Learning, Decision-making and Social Relations* (Routledge, 2016) 46.

[22] d boyd, 'Taken Out of Context: American Teen Sociality in Networked Publics' (Dissertation, University of California, 2018) 2. According to the author, the other features of networked publics are replicability, scalability, and searchability.

[23] S van der Hof and E Lievens, 'The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data under the GDPR' (2018) 23(1) *Communications Law* 33, 39.

[24] Ibid.

[25] S Livingstone and A Third, 'Children and Young People's Rights in the Digital Age: An Emerging Agenda' (2017) 19(5) *New Media & Society* 657, 661.

[26] Livingstone et al, 'EU Kids Online II. Final Report' (n 6) 2.

[27] van der Hof (n 11), 428.

[28] In 2011, 50% of 11-to-16-year-olds said it was easier to be themselves on the internet than with people face to face: S Livingstone and K Ólafsson, 'Risky Communication Online' (2011). EU Kids Online 1. Available at: eprints.lse.ac.uk/33732/.

[29] Anderson and Jingjing Jiang (n 19) 9, 13.

[30] Ibid.

[31] See Charlotte Alter, 'The Young and the Relentless: Adults have Failed to Stop School Shootings. Now it's the Kids' Turn to Try' *Time* (2 April 2018) 26.

[32] Livingstone and Third (n 25), 667.

[33] Case C-540/03 *Parliament v Council* [2006] ECR I-5769 37; European Union Agency for Fundamental Rights (FRA) and Council of Europe, *Handbook on European Law Relating to the Rights of the Child* (Luxembourg, Publications Office of the European Union 2015) 27.

[34] United Nations Committee on the Rights of the Child, 'General Measures of Implementation of the Convention on the Rights of the Child (Arts. 4, 42 and 44, para. 6): CRC/GC/2003/5' (27 November 2003) 3 ff.

[35] van der Hof (n 11), 427.

[36] Ibid at 427, 433.

[37] J Tobin and A Parkes, 'Article 13: The Right to Freedom of Expression' in John Tobin (ed), *The UN Convention on the Rights of the Child: A Commentary*, 1st edn (Oxford University Press, 2019) 440.

[38] The UN Committee on the Rights of the Child emphasises that the concept of 'matters that affect them' concerns also the consultation of groups of children on particular issues; as an example, children who have experienced the juvenile justice system, or adopted children, on proposals for law reforms of the corresponding sectors: United Nations Committee on the Rights of the Child, 'General measures of implementation of the Convention on the Rights of the Child (Arts 4, 42 and 44, para. 6)' (n 34) 5.

[39] Tobin and Parkes (n 37) 440.

[40] United Nations Committee on the Rights of the Child, 'General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1): CRC/C/GC/14' (29 May 2013) 9.

[41] Ibid at 11.

[42] VF Reyna and F Farley, 'Risk and Rationality in Adolescent Decision Making' (2006) 7(1) *Psychological Science in the Public Interest* 1, 33.

[43] M Macenaite, 'From Universal Towards Child-Specific Protection of the Right to Privacy Online: Dilemmas in the EU General Data Protection Regulation' (2017) 19(5) *New Media & Society* 765, 774.

[44] For an overview of the rules provided by the EU Member States in this regard, see European Union Agency for Fundamental Rights (FRA), 'Mapping minimum age requirements concerning the rights of the child in the EU. Dataset "Age requirements and health"' (2017). Available at: fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements-concerning-rights-child-eu.

[45] van der Hof (n 11), 428, 433.

[46] Ibid at 440.

[47] V Steeves, 'Swimming in the Fishbowl: Young People, Identity and Surveillance in Networked Spaces' in Irma van der Ploeg and Jason Pridmore (eds), *Digitizing Identities: Doing Identity in a Networked World* (Routledge, 2016) 132. On this topic see the full report: Steeves(n 6).

[48] London School of Economics and Political Science, 'EU Kids Online: Findings – Methods – Recommendations' (2014), EU Kids Online 32. Available at eprints.lse.ac.uk/60512/.

[49] Steeves' (n 47) 132.

[50] V Steeves, T Milford and A Butts, 'Summary of Research on Youth Online Privacy' (2010) 14. Available at: www.priv.gc.ca/media/1731/yp_201003_e.pdf.

[51] See, for an overview, B Zaman and M Nouwen, 'Parental controls: advice for parents, researchers and industry' (2016). EU Kids Online. Available at: eprints.lse.ac.uk/65388/.

[52] A Dürager and S Livingstone, 'How can parents support children's internet safety?' (2012). EU *Kids Onlin*e 1. Available at: eprints.lse.ac.uk/42872/.

[53] London School of Economics and Political Science (n 48) 22.

[54] V Steeves and P Regan, 'Young People Online and the Social Value of Privacy' (2014) 12(4) *Journal of Information, Communication and Ethics in Society* 298. For instance, large numbers of US kids do revise their social media profiles, are able to block people, and sometimes poste false information, which under some circumstances may be understood as a healthy way to protect one's privacy: Madden et al (n 13).

[55] L d'Haenens, S Vandoninck and V Donoso, 'How to Cope and Build Online Resilience?' (2013). EU Kids Online. Available at: eprints.lse.ac.uk/48115/.

[56] London School of Economics and Political Science (n 48) 9.

[57] Zaman and Nouwen (n 51) 5.

[58] Steeves (n 47) 133.

[59] A Janssens et al, 'Parents' and Adolescents' Perspectives on Parenting: Evaluating Conceptual Structure, Measurement Invariance, and Criterion Validity' (2015) 22(4) *Assessment* 473, 474.

[60] Steeves (n 47) 133 f.

[61] London School of Economics and Political Science (n 48) 35.

[62] On these topics see D Rosani, 'Child's participation online and the General Data Protection Regulation – A Dialogue between Educational and Legal Sciences is Urgently Needed' (2018) Special Issue *merzWissenschaft* 41–52.

[63] Livingstone and Third (n 25), 658–660; Macenaite (n 43), 769.

[64] Livingstone and Third (n 25), 665.

[65] AS Reid, 'Online Protection of the Child within Europe' (2009) 23(3) *International Review of Law, Computers & Technology* 217, 218.

[66] Livingstone and Third (n 25), 657–661.

[67] Byrne and Burton (n 16), 41.

[68] European Commission, 'European Strategy for a Better Internet for Children: COM(2012) 196 final' (2 May 2012).

[69] European Commission, 'An EU Agenda for the Rights of the Child: COM(2011) 60 final' (15 February 2011).

[70] E Staksrud and T Milosevic, 'Adolescents and Children in Global Media Landscape: From Risks to Rights' (2017) 41(3–4) *Annals of the International Communication Association* 235, 235–238.

[71] Macenaite (n 43), 765, 775.

[72] Staksrud and Milosevic (n 70), 239; J Savirimuthu, 'Article 8 General Data Protection Regulation: Has Anyone Consulted the Kids?' *LSE blog*. Available at: www.blogs.lse.ac.uk/mediapolicyproject/2016/03/01/eu-general-data-protection-regulation-article-8-has-anyone-consulted-the-kids/.

[73] John Carr, 'An open letter to the European Data Protection Supervisor and the Chair of the Article 29 Working Party'

(2017) 12. Available at: www.lse.ac.uk/media@lse/documents/MPP/eNACSO-letter-re-GDPR.pdf.

74 Macenaite (n 43), 772; Jasmontaite and De Hert (n 7), 25.

75 UK Information Commissioner's Office, 'Consultation: Children and the GDPR Guidance' (Wimslow 2018) 27.

76 Article 29 Working Party, 'Guidelines on consent under Regulation 2016/679: WP 259 rev.01' (2018) 9 n76) 25.

77 I Milkaite and E Lievens, 'The Changing Patchwork of the Child's Age of Consent for Data Processing across the EU (January 2019)' (2019). Available at: www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=3017751.

78 As an example, this is the case for Italy: Garante per la protezione dei dati personali, 'Parere sullo schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679' (2018) 2.4. Available at: www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9163359.

79 European Commission, 'Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation): COM(2012) 11 final' (25 January 2012).

80 Already in 1998, the Children's Online Privacy Protection Rule (US COPPA) had laid down certain requirements for online services dealing with children, setting 13 years as the age of consent for data processing. In the framework of the US Online Privacy Protection Rule, children are defined as individuals under the age of 13: Code of Federal Regulations (CFR), Title 16 (Commercial Practices) Part 312 (Children's Online Privacy Protection Rule) § 2 (Definitions). See M Macenaite and E Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?' (2017) 26(2) *Information & Communications Technology Law* 146, 146.

81 European Commission, 'Impact assessment accompanying the General Data Protection Regulation and the Directive on the protection of individuals' (n 6) 107.

82 John Carr (n 73) 12; Sonia Livingstone, as cited in I Milkaite and V Verdoodt, 'The General Data Protection Regulation and children's rights: questions and answers for legislators, DPAs, industry, education, stakeholders and civil society: Roundtable report, Brussels, 23 June 2017' 14. Available at: www.betterinternetforkids.eu/documents/167024/2013511/GDPRRoundtable_June2017_FullReport.pdf.

83 A Nairn, J Carr and B Lilliu, 'When Free Isn't It: Business, Children and the Internet' (Rome 2016) 44.

84 Savirimuthu (n 72) 195.

85 van der Hof (n 11), 425.

86 K McCullagh, 'The General Data Protection Regulation A Partial Success for Children on Social Network Sites' in Tobias Bräutigam and Samuli Miettinen (eds), *Data Protection, Privacy and European Regulation in the Digital Age* (Unigrafia, 2016) 124.

87 In this regard it is worth noting that the definition of the child as 'any person below the age of 18 years', as provided for in the Commission's GDPR proposal, was deleted, together to any reference to the UN CRC. However, the ratification of the UN CRC by all the Member States, and their relevance at EU level as general principle of Union law, should unmistakably lead to the conclusion that in the framework of the GDPR all those under 18 years are considered children.

88 van der Hof (n 11), 440.

89 'An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent': Code of Federal Regulations (CFR), Title 16 (Commercial Practices) Part 312 (Children's Online Privacy Protection Rule) § 5 (Parental consent).

90 Macenaite (n 43), 775.

91 Macenaite and Kosta (n 80), 195; Nairn, Carr and Lilliu (n 83) 46; UK Information Commissioner's Office (n 75) 29.

92 McCullagh (n 86) 116.

93 Article 29 Working Party, 'Guidelines on Automated Individual Decision-making and Profiling for the purposes of Regulation 2016/679: WP 251 rev.01' (2018) 25. On the relevance of codes of conduct in this regard, see the last para of this chapter.

94 Ibid at 26.

95 Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679' (n 76) 25.

[96] Ibid at 26.

[97] European Union Agency for Fundamental Rights (FRA), 'Mapping Minimum Age Requirements Concerning the Rights of the Child in the EU. Datasets "Issuance of a Credit Card" and "Age at which a Child can Open a Bank Account, with Parental Consent"' (2017). Available at: fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements-concerning-rights-child-eu.

[98] Macenaite (n 43), 773.

[99] Jasmontaite and De Hert (n 7), 26.

[100] A Mantelero, 'Children Online and the future EU Data Protection Framework: Empirical Evidences and Legal Analysis' (2016) 2(2/3/4) *International Journal of Technology* 175.

[101] Unicef, *Children in A Digital World* (Unicef, 2017) 92.

[102] van der Hof (n 11), 436; see also Macenaite (n 43), 776.

[103] K Ólafsson, S Livingstone and L Haddon, 'Children's Use of Online Technologies in Europe. A Review of the European Evidence Base' (2014). EU Kids Online 5. Available at: eprints.lse.ac.uk/50228/.

[104] Macenaite (n 43), 773.

[105] Unicef (n 101) 93.

[106] Macenaite (n 43), 775; Nairn, Carr and Lilliu (n 83) 46.

[107] Jasmontaite and De Hert (n 7), 28.

[108] Macenaite (n 43), 768; Jasmontaite and De Hert (n 7), 25; critical towards fixed age limits and blanket approaches JC Buitelaar, 'Child's Best Interest and Informational Self-Determination: What the GDPR can Learn from Children's Rights' (2018) 8(4) *International Data Privacy Law*, 293, 306–307.

[109] Macenaite (n 43), 773; Livingstone and Third (n 25), 659.

[110] See the exceptions to prior parental consent listed in 16 Code of Federal Regulations (CFR) § 312 (5)(c).

[111] Đ Krivokapić and J Adamović, 'Impact of General Data Protection Regulation on Children's Rights in Digital Environment' (2016) (3) *Belgrade Law Review* 205, 211.

[112] Macenaite and Kosta (n 80), 195.

[113] A Morgan, 'The Transparency Challenge Making Children Aware of their Data Protection Rights and the Risks Online' (2018) 23(1) *Communications Law* 44, 45.

[114] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent' (2011) 35.

[115] UK Information Commissioner's Office (n 75) 42.

[116] Council of Europe, 'The protection of individuals with regard to automatic processing of personal data in the context of profiling: Recommendation CM/Rec(2010)13 and explanatory memorandum' (2010). Available at: https://rm.coe.int/16807096c3.

[117] Macenaite (n 43) 771.

[118] Given the recital, however, as a rule profiling should not rely on the exceptions provided by Art 22(2) of the GDPR, amongst others the data subject's explicit consent. Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (n 93) 26.

[119] UK Information Commissioner's Office (n 75) 37.

[120] Buitelaar (n 108), 304–305.

[121] European Union Agency for Fundamental Rights (FRA) *Handbook on European Data Protection law*: 2018 Edition (Publications Office of the European Union, 2018) 221.

[122] Macenaite (n 43), 770.

[123] Article 29 Working Party, 'Guidelines on the right to data portability: WP 242 rev.01' (2017) 3.

[124] Ibid.

[125] van der Hof and Lievens (n 23), 36.

[126] Article 29 Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether

processing is “likely to result in a high risk” for the purposes of Regulation 2016/679: WP 248 rev.01’ (2017) 10.

127 van der Hof and Lievens (n 23), 38–39; L Atkinson, ‘Interpreting the Child-Related Provisions of the GDPR’ (2018) 23(1) *Communications Law* 31, 32.

128 van der Hof (n 11), 412; Council of Europe, ‘Strategy for the Rights of the Child (2016–2021)’ (Strasbourg 2016) 9, 21.

129 This view had already been expressed by R Mansell, ‘From Digital Divides to Digital Entitlements in Knowledge Societies’ (2002) 50(3) *Current Sociology* 407, 409.

130 van der Hof (n 11), 441.

131 Livingstone et al (n 6) 43.

132 United Nations Committee on the Rights of the Child, ‘General comment No. 20 (2016) on the implementation of the rights of the child during adolescence: CRC/C/GC/20’ (6 December 2016).

133 Jasmontaite and De Hert (n 7), 31.

134 Livingstone and Third (n 25), 666.

135 Dias et al (n 10), 420.

136 Ibid at 421.

137 MM Terras and J Ramsay, ‘Family Digital Literacy Practices and Children’s Mobile Phone Use’ (2016) 7(1957) *Frontiers of Psychology* 1–11.

138 Some interesting ideas for ‘positive and proactive digital parenting’ are provided by the Council of Europe: Council of Europe, *Internet Literacy Handbook* (Council of Europe, 2017) 114.

139 London School of Economics and Political Science (n 48) 22.

140 McCullagh (n 86) 127.

141 See, on this topic, 38th International Conference of Data Protection and Privacy Commissioners, ‘Resolution for the Adoption of an International Competency Framework on Privacy Education’ (Marrakesh, 18 October 2016); 30th International Conference of Data Protection and Privacy Commissioners, ‘Resolution on Children’s Online Privacy’ (Strasbourg 17 October 2008).

142 See in this regard the studies of the EU Joint Research Centre, among others the following one: S Chaudron, R Di Gioia and M Gemo, ‘Young Children (0–8) and Digital Technology. A Qualitative Study across Europe’ (2018).

143 London School of Economics and Political Science (n 48) 6.

144 V Steeves, ‘Now You See Me: Privacy, Technology, and Autonomy in the Digital Age’ in Gordon DiGiacomo (ed), *Human Rights: Current Issues and Controversies* (University of Toronto Press, 2016).

145 Morgan (n 113), 46.

146 van der Hof and Lievens (n 23), 37.

147 Steeves, Milford and Butts (n 50) 7, 19.

148 Council of Europe, ‘Recommendation CM/Rec(2016)3 of the Committee of Ministers to member states on human rights and business’ (2016).

149 Save the Children, United Nations Global Compact and Unicef, ‘The Children’s Rights and Business Principles’ (2012).

150 Buitelaar (n 108), 300.

151 A Longfield, ‘How Parents and Carers can Support their Children to Manage their Rights and Privacy Online’ (2017). Available at: www.childrenscommissioner.gov.uk/2017/11/28/how-parents-and-carers-can-support-their-children-to-manage-their-rights-and-privacy-online/.

152 J Savirimuthu, ‘Networked Children, Commercial Profiling and the EU Data Protection Reform Agenda: In the Child’s Best Interests?’ in Ingi Iusmen and Helen Stalford (eds), *The EU as a Children’s Rights Actor: Law, Policy and Structural Dimensions* (Barbara Budrich Publishers, 2016) 224.

153 Macenaite (n 43), 776.

154 Macenaite and Kosta (n 80), 189.

[155] UK Information Commissioner's Office (n 75) 30.

[156] European Commission, 'An EU Agenda for the Rights of the Child' (n 69) 3 f.

[157] European Commission, 'Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union: COM(2010) 573 final' (19 October 2010).

[158] Byrne and Burton (n 16), 47; McCullagh (n 86) 132; van der Hof and Lievens (n 23), 40.

[159] On the issue of cooperation between business and academia *cf* Donoso et al (n 10), on which the following considerations to a large extent rely.

5

Risk to the ‘Rights and Freedoms’

A Legal Interpretation of the Scope of Risk under the GDPR

KATERINA DEMETZOU[1]

Abstract

The concept of *risk* in the GDPR has been attributed a broad scope by the legislature in that it refers to all rights and freedoms of natural persons. This chapter affirms this broad scope and substantiates it by examining the role that *risk* plays in the GDPR. Identifying the role of a concept and using this finding as a basis for the interpretation of the concept is a method of interpretation that has been applied to other key data protection notions (ie personal data and data controller). *Risk* is a criterion introduced to enable accountability and hence effective compliance with the GDPR. The GDPR is, in turn, a piece of legislation aiming for the protection of all rights and freedoms. The chapter concludes that *risk* should be understood as referring to all rights and freedoms exactly as the wording of the legislature suggests and that this broad scope should be made explicit.

Keywords

Data protection, risk, role, scope, interpretation, accountability, compliance, rights and freedoms.

I. Introduction

The concept of *risk* has gained a prominent position in the General Data Protection Regulation (hereafter, the GDPR),[2] the general EU legal framework on data protection which has repealed the preceding Directive 95/46.[3] *Risk* is used as a criterion for forming legal obligations[4] as well as for triggering legal obligations (eg DPIA Article 35, communication of personal data breach to the data subject Article 34) and its prevalent position in the GDPR has led legal scholars talk about a ‘riscification’[5] of the EU data protection legislation. According to the Working Party 29 (WP29),[6] ‘[a] risk is a scenario describing an event and its consequences, estimated in terms of severity and likelihood’.[7] This is the definition that

should guide data controllers in meeting their legal obligations. However, this definition raises questions as to the way the concept of *risk* and its constitutive elements (severity and likelihood) should be interpreted under the GDPR. In the present chapter I will take a first step towards the qualification of *risk* by paying keen attention to its role in the GDPR. I intend to answer the following Research Question:

'What is the role of *risk* in the GDPR? In what way is the identification of this role important for determining the scope of *risk*?'

The chapter is divided into three parts; in Section II, I will make a methodological point. I will demonstrate that the CJEU has used the role that is attributed to two key data protection concepts under the GDPR ('personal data' and 'data controller') as a tool for the determination of the scope of these concepts. That way, I intend to highlight the importance of a teleological interpretation of *risk*. Based on the conclusions of Section II, I will proceed to Section III where I will identify and analyse the role of *risk*. In Section IV, I will explain the way in which the identified role of *risk* substantiates the broad scope that has already been afforded to the concept by the legislature ('risk to the rights and freedoms of natural persons') in the relevant legal provisions.

All in all, the purpose of this chapter is not to suggest an alternative definition of *risk* other than the one endorsed by the WP29. It is rather to identify the role that this concept is intended to play in the field of personal data protection and to prove that by understanding its role, we can identify its scope. That means that one could eventually answer the questions: What does risk refer to under the GDPR? What does this concept encompass? If the scope is not made clear, data controllers could be confronted with high fines, for example, for having carried out a DPIA (Article 35)[8] in an 'incorrect way'.[9] In this chapter, I argue that *risk* has been attributed a broad scope which is substantiated by the role it has in the GDPR. *Risk* should be understood as referring to all rights and freedoms of natural persons and this broad scope should be made explicit.

II. 'Personal Data' and 'Data Controller': *Role* and *Scope* of Two Key Concepts in the GDPR

The aim of this section is to demonstrate the importance of examining the intended role of a concept in order to determine its scope. For that, 'personal data' and 'data controller' will be examined. There are two reasons why I choose to examine specifically these two concepts; first, both play a crucial role in the data protection legal framework. 'Personal data' relates to the material scope of the GDPR, while 'data controller' relates to compliance and allocation of responsibility. Secondly, they are often used as ancillary concepts for further defining other notions in the GDPR.[10]

A. ‘Personal Data’

According to Article 4(1) GDPR,

> “personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

The concept of personal data plays a crucial role in the data protection legal framework since it relates to the *material scope* of the GDPR.[11,12] That means that if processing of information of a natural person, in a given case, does not fit in the definition of ‘processing of personal data’, then this activity automatically falls outside the material scope of the GDPR and the natural person is deprived of the legal protection afforded by this legal framework. Having said that, ‘personal data’ is a concept that – along with other conditions which have to be met[13] – constitutes the ‘gateway’ for a natural person to get the legal protection afforded by the GDPR. The aim of those concepts which relate to the material scope of the GDPR is to afford the widest protection possible.

The definition of ‘personal data’ is ‘extensive’[14] and its wording is general ‘so as to include all information concerning an identifiable individual’;[15] this reflects the legislature’s intention for a wide notion of ‘personal data’. This was also confirmed by the CJEU in the *Nowak* case whereby it said that ‘[t]he use of the expression ‘any information’ in the definition of the concept of ‘personal data’ […] reflects the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it “relates” to the data subject’.[16] The WP29 has stressed the importance of taking into account the ultimate purpose of the rules in the data protection legal framework when interpreting and applying them; the ultimate purpose is ‘to protect fundamental rights and freedoms of natural persons and in particular their right to privacy, with regard to the processing of personal data’.[17] Therefore, an ‘undue restriction’[18] of the scope of ‘personal data’ would have the unwanted consequence of depriving natural persons of their rights.

The CJEU confirms that ‘the scope of Directive 95/46 is very wide and the personal data covered by that directive is varied’.[19] The Court has opted for an objective[20] and factual approach when interpreting ‘personal data’. The approach is objective in the sense that the data controller’s intention (or knowledge of whether the data that are processed qualify as personal data)[21] does not matter; as long as the data can result to the identification of a natural person, data protection law applies.[22] The approach is factual, in the sense that for the data to qualify as personal data, one needs to examine the specifics and the context of each case (‘the extent to which certain identifiers are sufficient to achieve identification is something dependent on the context of the particular situation’).[23] For example, in the case of *Nikolaou v Commission*, even if the applicant was not named, the information published in the press release was personal data given that the applicant was easily identifiable ‘under the

circumstances'.[24]

At this point, it is interesting to mention that in addition to the broad scope attributed to 'personal data', the CJEU has confirmed the intention to provide for the widest protection possible, by adopting (on the contrary) a narrow interpretation of cases that fall outside the material scope of the GDPR (the exceptions stipulated in Article 2(2)). More specifically, the Court has said that 'derogations and limitations in relation to the protection of personal data must apply in so far as is strictly necessary'.[25] In its recent *Buivids* case, the CJEU advocated once more in favour of such a strategy by explicitly linking the underlying reasoning of a strict interpretation, to the fundamental rights nature of the right to data protection.[26] This enhances, *a contrario*, the broad meaning and scope of concepts that relate to the material scope of the GDPR. By narrowing the scope of the exceptions, the material scope of the legal framework is broadened.

In a nutshell, the broad interpretation afforded to the concept of 'personal data' by both the WP29 and the CJEU is justified given that this concept relates to the material scope of the GDPR and should aim for the widest protection possible. When interpreting notions that determine whether a specific case falls under the (material) scope of the GDPR, the meaning of these notions should be broad and their interpretation should be done in light of fundamental rights.[27]

B. 'Data Controller'

According to Article 4(7) GDPR:

> "controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

The concept of 'data controller' also plays a crucial role for data protection since it 'determines who shall be responsible for compliance with the data protection rules, and how data subjects can exercise their rights in practice'.[28] In other words it helps in allocating responsibility. The objective of the concept of 'data controller' is to promote an effective and complete protection of data subjects. Thus, the interpretation of this concept must be aligned with this objective. In *Google Spain*, the CJEU pointed out that '[…] it would be contrary not only to the clear wording of that provision [art 2(d) of Directive 95/46] but also to its objective – which is to ensure, through a broad definition of the concept of 'controller', effective and complete protection of data subjects – to exclude the operator of a search engine from that definition […]'.[29] This was upheld again by the CJEU in the recent *Fashion ID* case,[30] the *Wirtdchaftsakademie* case[31] as well as the *Jehovan* case.[32]

The WP29 has opted for a wide and dynamic meaning and scope of 'data controller'.[33] The CJEU has similarly followed a strategy of adopting a very wide scope of 'data controller'. In the *Fashion ID* case, the AG recognised this maximalist approach saying that in the 'understandable desire to secure the effective protection of personal data, the recent case-law of the Court has been very inclusive when being asked to define, in one way or another, the notion of (joint) controller'.[34]

The CJEU in both cases (*Google Spain* and *Wirtdchaftsakademie*) interpreted the concept of a data controller in the light of fundamental rights[35] and followed a pragmatic, functional approach[36] in order to conclude whether the actors[37] could qualify as 'controllers'. Instead of relying solely on a formal analysis (eg based on arrangements such as a contract), the Court examined thoroughly the factual influence that these actors had over the respective data processing operations. This approach 'contributes to ensuring more complete protection of the rights of persons visiting a fanpage'.[38] It also accentuates the potential of a technologically neutral provision to respond to the advancements of technology, whereby new and more actors participate in even more complicated environments.

Another important element which guides the interpretation of 'data controller' is the need to approach it as an autonomous concept, meaning that 'it should be interpreted mainly according to Community data protection law'.[39] It has been highlighted by the WP29 that a 'uniform and therefore autonomous interpretation of such a key concept'[40] contributes to an effective application of data protection rules and to a high level of protection.[41] Autonomous concept means that it has 'its own independent meaning in Community law, not varying because of – possibly divergent – provisions of national law'[42] and that 'although external legal sources can help identifying who is a controller, it should be interpreted mainly according to data protection law'.[43]

Keeping in mind that the ultimate goal is to enhance effective and complete protection, the AG in the *Fashion ID* case called into question the aforementioned maximalist approach. The question raised by AG Bobek was whether effective protection is indeed enhanced when everyone is made responsible for ensuring it.[44] The AG went on: '[t]hat, in a nutshell, is the deeper moral and practical dilemma demonstrated by the present case and expressed in legal terms by the scope of the definition of (joint) controller'.[45] In paragraph 75, AG Bobek suggests that '[t]he problem is that the delineation of responsibility so far does not follow from the broad definition of a controller. The danger of that definition being too broad is that it results in a number of persons being co-responsible for the processing of personal data'.[46] He later on adds that 'effective protection of something tends to dramatically decrease if everyone is made responsible for it […]'.[47]

The WP29 had also raised a similar concern [a 'key challenge'] that '[i]f it is not sufficiently clear what is required from whom (eg no one is responsible or a multitude of possible controllers) there is an obvious risk that too little, if anything, will happen and that the legal provisions will remain ineffective'.[48] More specifically, the WP29 had pointed out that '[i]n such a complex environment it is even more important that roles and responsibilities can be easily allocated, so as to ensure that the complexities of joint control do not result in an unworkable distribution of responsibilities which would hamper the effectiveness of data protection law'.[49]

In a nutshell, the concept of a 'data controller' must be interpreted in line with its role in the data protection legal framework; that is, allocation of responsibility in such a way that the effective and complete protection of data subjects is guaranteed. Having this as the basis for interpretation, the CJEU has, until now, adopted a maximalist approach with regard to the

meaning and scope of ‘data controller’. This approach is, however, now being put into question. Does a broad and inclusive definition of ‘data controller’ still serve the concept’s role? Or should we adopt a different approach in view of the different and more complex environment?[50] In its judgment on the *Fashion ID* case, the CJEU unfortunately did not address – at least directly – the concerns raised by AG Bobek, with regard to the maximalist approach and the way this approach could hamper the goal of an effective and complete protection.

The methodological point that I made in this section has also been made by the WP29 in its Opinions on the concept of personal data and the concept of controllers and processors. In both documents, the WP29 first examined the role that these concepts play in the data protection legal framework and then it proceeded to defining and interpreting them in line with their identified role.[51] Bearing this in mind, the next section of the chapter is dedicated to the identification of the role of *risk* in the GDPR. This, in turn, will lay the foundations for a teleological interpretation of the concept.

III. Role of *Risk* in the GDPR

In order to identify the role of *risk*, I shall first point out the legal provisions whereby this concept appears. To begin with, Article 24(1) GDPR reads:

> ‘Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.’

Article 24(1) prescribes the general responsibility of data controllers under the GDPR. The wording of this Article and more specifically the phrase ‘[…] to ensure and to be able to demonstrate’ compliance, refers us directly to the principle of accountability as stipulated in Article 5(2):

> ‘The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (“accountability”).’

The EDPS has pointed out that Article 24 ‘refers to the implementation of all data protection principles and the compliance with the whole of the GDPR’.[52] This is a function identical to that of the principle of accountability. The principle of accountability requires that processing operations are performed in compliance with the data protection principles of Article 5(1) and for that it has been characterised as a ‘fundamental principle of compliance’.[53] We thus acknowledge that both the wording and the substance of these two provisions [Article 24(1) and Article 5(2)] advocate for the fact that Article 24(1) is the legal provision that materialises, in general terms, the accountability principle.[54] It does so by setting out the criteria that should be taken into account when deciding upon the measures (technical and organisational) that are appropriate for complying with the data protection principles (found in Article 5(1)) and the respective legal obligations stipulated in the GDPR. The fact that Article 24(1) is the expression of the accountability principle also means that the way we

read and understand the general responsibility of data controllers should be in line with and promote those elements that come along with the concept of accountability. A first important element that accountability entails is that it introduces a proactive approach given that data controllers have to be able to demonstrate compliance even if there is no incident of non-compliance.[55] That practically means that controllers need to have tools and mechanisms in place that will facilitate them to prove that they have been compliant with the GDPR. A second important element of accountability is scalability; accountability is 'implemented through scalable obligations'.[56]

Except for Article 24(1), the GDPR presents other, more specific, legal obligations which introduce tools/processes that enable the principle of accountability. Data protection by design and by default is a legal obligation found in Article 25 which has been introduced as a way to ensure that the controller 'meet[s] the requirements of this Regulation and protect[s] the rights of data subjects'. Recital 78 makes even clearer the way this legal obligation materialises the accountability principle, by saying that '[i]n order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default'. With regard to the legal obligation to maintain records of processing activities according to Article 30, again Recital 82 makes clear that this obligation is in place '[i]n order to demonstrate compliance with this Regulation'. The same goes for Article 35 and the obligation to perform data protection impact assessments, which is, according to Recital 84, a way to 'enhance compliance with this Regulation' and a way to decide upon the most appropriate measures to 'demonstrate that the processing of personal data complies with this Regulation'.[57] Apart from the wording used in these legal provisions, it is also their intended function that backs up the accountability principle. These obligations aim to facilitate and 'stimulate controllers to put into place proactive measures in order to be able to comply with all the elements of data protection law'.[58]

Having acknowledged the relationship between the above-mentioned legal obligations and the principle of accountability, the next step is to examine the way in which *risk* appears in these provisions. Article 24(1) introduces *risk* and places it among the general criteria ('nature, scope, context and purposes') that the data controller should take into consideration when deciding upon the 'appropriate' measures. Recital 76 reads: 'The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing.' *Risk* appears to be a criterion broader than the rest, given that 'nature, scope, context and purposes' are factors to be taken into account so as to conclude about the *risk* involved. In addition, the legal obligations of Articles 25, 30 and 35 also use *risk* as their major criterion.[59] This points to the link between the concept of *risk* and the principle of accountability as stipulated in Article 5(2).

Although the principle of accountability is not new in the European data protection legal framework,[60] the way it has been materialised in the GDPR testifies to the intention of the legislature to enhance the principle and bring it to the forefront of the established compliance scheme. The term 'compliance' is hereby used in its broader sense, stipulating an overarching

compliance with the aim and purposes of the GDPR. It takes the meaning of a legal strategy which appears to have been differentiated from the one under Directive 95/46. The difference lies in that the compliance scheme under the GDPR is characterised by the introduction of proactive legal means that are to ensure an effective implementation of data protection measures and sufficient means of accountability for controllers.[61] The aim of this legal strategy is to 'defend what has been formally recognised'[62] meaning the data protection principles of Article 5(1); in other words, a more effective compliance in practice. *Risk* is a core concept of this legal strategy given that it enables accountability and enhances the proactive approach; it is thus introduced as a legal means to stimulate responsibility of data controllers. This strategy is the so-called risk-based approach, a 'scalable and proportionate approach to compliance'[63] with the GDPR.

Risk is a concept that relates to the principle of accountability and therefore to 'compliance', both in the sense of compliance with concrete data protection provisions, as well as in the sense of compliance understood as a legal strategy. The GDPR introduces a modified compliance scheme which has taken a substantial turn towards a reinforced accountability principle. The legislature has differentiated the legal strategy towards compliance by introducing mechanisms that encourage a proactive approach with the aim to achieve effectiveness in complying with the data protection principles. *Risk* has emerged as a prominent criterion that has been chosen to lead this modified scheme because it enables the principle of accountability.

As explained in Section II, the concept of 'data controller' also relates to compliance, however, not in the same way. 'Data controller' answers the question of 'who shall be responsible for compliance'; it has to do with allocation of responsibility among (possibly more than one) actor(s). *Risk* answers the question of 'what should the data controller do to have the appropriate measures in place'. For both concepts however, the end goal is the achievement of effective and complete protection which is the way that 'compliance' in the GDPR is to be understood. 'Effectiveness' is the reason why *risk* has been introduced in the first place. *Risk* forms part of the chosen means to achieve the final purpose (effective and complete protection).

IV. Scope of *Risk* in the GDPR

In this section I will talk about the scope of *risk* under the GDPR. For that matter, the findings of Section III will be used in line with the method of interpretation explained in Section II. Given that there is still no developed case law as to the way *risk* should be legally approached, the wording in the GDPR will serve as the starting point.

Article 1(2) lays down the objective of the GDPR and stipulates that:

> 'This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data'.

The wording in Article 24(1) – which sets the foundations of the reasoning behind

compliance with the GDPR – as well as the wording in other legal provisions (eg Arts 25, Art 35 etc.), suggests a broad scope of the concept of *risk*. They suggest that *risk* refers to the 'rights and freedoms of natural persons'.[64] Recital 4 explains what that means in the context of the GDPR and specifies that 'rights and freedoms' refer to:

> 'all fundamental rights […] the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity'.

This broad scope can be additionally substantiated by the intended role of *risk*. *Risk* must be understood always in relation to accountability as established under the modified compliance scheme of the GDPR. This scheme has been developed to facilitate compliance; in other words, to mitigate the risk that processing operations will not be compliant with the GDPR. The previously predominant reactive approach to compliance (found in Directive 95/46) failed to deliver complete protection for data subjects.[65]

The principle of accountability and consequentially the mechanisms that back this principle up aim to enable compliance with the data protection principles found in Article 5(1). It has been argued that these principles constitute the 'essence' of the fundamental right to data protection, in the meaning of Article 52(1) of the Charter of Fundamental Rights.[66] If this is the case, then the principle of accountability along with all the mechanisms and measures that enable it, relates to the scope of the fundamental right to data protection. In that way, it actually enhances the rights-based approach and the fundamental rights character of the data protection legal framework. It goes without saying that the risk-based approach (which, as previously explained, forms part of the legal strategy for more effective compliance) is being employed to protect the essence of the fundamental right to data protection and hence enhances the rights-based character of the legal framework. If we link this to the fact that the GDPR aims to protect rights and freedoms with regard to the processing of personal data (see again, Article 1(2)), then *risk* should indeed be understood as referring to all rights and freedoms; this affords the concept of *risk* a broad scope, exactly as the wording of the GDPR suggests. Compliance with the GDPR can be achieved only if risks are identified, assessed and mitigated with regard to the rights and freedoms of natural persons.

As mentioned in Section I, the question raised when discussing the scope of *risk* is: what does the concept refer to under the GDPR? The answer given in this chapter is that *risk* refers to the rights and freedoms of natural persons. Limiting the scope of *risk* to what has been suggested as 'non-compliance risk'[67] would go against both the wording and the role of the concept in the GDPR. Understanding *risk* as 'non-compliance' means that we shall examine whether 'the processing operation will (not be) compliant with data protection requirements'.[68] The idea of *risk* as a 'non-compliance risk' has been suggested as a solution to a conundrum in the GDPR which is that '[o]n the one hand the GDPR [it] is risk-based, meaning that it will provide a level of protection directly dependent upon the level of risk at stake [while] [o]n the other hand it must respect the rights-based nature of data protection as a fundamental right of the EU, which is its exact counterpart insofar as it provides for an

even level of protection to all (irrespective of the level of risk)'.[69] I argue that such a conundrum does not exist in the GDPR. One thing is the level of protection that the legislature aims for (which is the level of protection afforded to fundamental rights – rights-based approach) and another thing is the way in which this level of protection can be effectively achieved (which is the legal strategy adopted under the GDPR, having *risk* as the prominent criterion that leads the modified compliance scheme – risk-based approach).[70]

What is probably worth clarifying at this point is that there is a difference between *risk* playing a crucial role in the compliance scheme of the GDPR [it refers to the *role of risk*] and *risk* being understood as a compliance risk [it refers to the *type of risk*]. In a scenario where *risk* is understood as a compliance risk, then the whole point of introducing the proactive scalable compliance scheme described above, seems to be annulled. That, of course, does not mean that compliance issues are not integrated within the risk analysis process.[71]

An inaccurate understanding of what falls under the scope of *risk* in the GDPR would hamper its role in the compliance scheme and would limit its potential in protecting rights and freedoms. Instead of following the reasoning that says *since compliance with the GDPR automatically means that rights and freedoms have been taken into consideration, then it still makes sense to talk about 'non-compliance' risk which also encompasses rights and freedoms*, I suggest that it is of crucial importance to make explicit that *risk* is to be understood with regard to rights and freedoms. The reason is the following; under Directive 95/46[72] the protection of fundamental rights and freedoms of natural persons was also part of being compliant with the legal framework. However, even though this was the legislature's aim and wording, in practice this was not – at least effectively – met. This is the reason why the legislature introduced the risk-based approach as the GDPR's legal strategy for effective compliance. This is also the reason why the following points have been made, mainly raised in the context of the obligation to perform DPIAs (Article 35); first of all, that the identification and the assessment of risks should be done from the perspective of data subjects.[73] This point has been raised to combat the practice so far, mainly with regard to PIAs (Privacy Impact Assessments), whereby data controllers adopted primarily a business perspective. The second point that is reaffirmed is that the process of identifying, assessing and mitigating *risks* should break free from the past formalities of compliance checklists.[74]

The identification of the scope of *risk* should be understood as a first research step towards the legal qualification of *risk* under the GDPR. Future work will deal with the two constitutive qualities of *risk*¸ meaning likelihood and severity. These two qualities cannot be understood or measured if the type of *risk* the legislature refers to is not clear. For example, if we understand risk as 'non-compliance risk' and at the same time consider compliance as being a binary situation of 'yes/no', then would there be any room to talk about 'likelihood', a concept that refers to chances and probabilities that the *risk* will occur?

V. Conclusion

In this Chapter, I have examined the role of *risk* in the GDPR with the aim of using the underlying reasoning of this role to determine the scope of the concept.

Identifying the role of a concept and using this finding as a basis for the interpretation of the concept is a method of interpretation that has been used by the regulator but also by the CJEU. In Section II, I give two examples of how this method has been applied to key data protection concepts; 'personal data' and 'data controller'. 'Personal data' is a concept that relates to the material scope of the GDPR and is given the broadest scope so that more natural persons fall under the legal protection of the Regulation. 'Data controller' is a concept that relates to compliance and the allocation of responsibility. It should therefore be interpreted in a way to guarantee the most effective and complete protection of personal data. This does not mean that the solution is, beyond any doubts, a broad meaning. While the CJEU has, until now, given an inclusive scope, there are concerns raised as to whether this wide scope actually enhances an effective protection.

After having demonstrated the way in which the role of a concept determines its scope, I proceeded in specifically examining the role that *risk* plays in the GDPR, in Section III. For that, I pointed out the legal provisions whereby the concept is introduced. These are primarily Article 24(1), which lays the foundations of data controllers' responsibility under the GDPR and materialises the principle of accountability, but also other provisions that introduce more specific obligations, such as record keeping or DPIAs. *Risk* appears as a major criterion in all those legal obligations that enable accountability. Its role is therefore inextricably linked to accountability and to compliance. It introduces the risk-based approach, a legal strategy that aims to enable accountability and facilitate compliance by promoting a proactive and scalable approach.

Having this role of *risk* in mind, I examined the scope of the concept in Section IV. The wording used in the GDPR ('risk to the rights and freedoms of natural persons') suggests a broad scope. I argue that such a broad scope is substantiated also by the role that *risk* holds in the GDPR. *Risk* is a criterion introduced to enable accountability and hence effective compliance with the GDPR which, according to Article 1(2), aims to the protection of rights and freedoms with regard to the processing of personal data. *Risk* should thus be understood as referring to all rights and freedoms and thus having a broad scope, exactly as the wording of the GDPR suggests.

It remains to be seen whether such a broad scope afforded to the concept of *risk* serves the primary intention of the legislature, that is to achieve a more effective protection of personal data in practice. This will be proved only in practice, when specific cases will be examined and effectiveness will be assessed in light of the specific circumstances of each case – exactly as is now the case for the concept of 'data controller'.

References

Alhadeff, Joseph, Brendan Van Alsenoy and Jos Dumortier, 'The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions' in Daniel Guagnin, Leon Hempel, Carla Ilten, Inga Kroener, Daniel Neyland and Hector Postigo (eds) *Managing Privacy Through Accountability* (Palgrave Macmillan, London, 2012).

Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final, 28.10.1992.
Article 29 Data Protection Working Party 'Opinion 4/2007 on the Concept of "Personal Data" in 01248/07/EN WP 136 (2007).
Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' in 00264/10/EN WP 169 (2010).
Article 29 Data Protection Working Party 'Statement of the Working Party on Current Discussions Regarding the Data Protection Reform Package' (2013).
Article 29 Data Protection Working Party 'Opinion 05/2014 on Anonymisation Techniques' in 0829/14/EN WP216 (2014).
Article 29 Data Protection Working Party, 'Statement on the Role of a Risk-based approach in Data Protection Legal Frameworks' in 14/EN WP 218 (2014).
Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' in 17/EN WP 248 rev.01 (2017).
Commission, Communication from the Commission to the European Parliament and the Council, 'Stronger Protection, New Opportunities – Commission Guidance on the Direct Application of the General Data Protection Regulation as of 25 May 2018', COM(2018) 43 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0043.
European Data Protection Supervisor (EDPS) 'Opinion 5/2018, Preliminary Opinion on Privacy by Design' (2018).
Case C-25/17 *Jehovan* [2018] ECLI:EU:C: 2018:551.
Case C-40/17, *Fashion ID* [2018] ECLI:EU:C:2018:1039 AG Opinion.
Case C-73/16 *Puškár* [2017] ECLI:EU:C:2017:725.
Case C-131/12 *Google Spain SL, Google Inc v AEPD, Mario Costeja González* [2013] ECLI:EU:C:2013:424, Opinion of AG Jääskinen.
Case C-131/12 *Google Spain SL, Google Inc v AEPD, Mario Costeja González* [2014] ECLI:EU:C:2014:317.
Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein* [2018] ECLI:EU:C: 2018:388.
Case C-212/13 *Ryneš* [2014] ECLI:EU:C: 2014:2428.
Case C-434/16 *Nowak* [2017] ECLI:EU:C: 2017:994.
Case C-473/12 *IPI* [2013] ECLI:EU:C: 2013:715.
Case C-582/14 *Breyer* [2016] ECLI:EU:C: 2016:779.
Case C-40/17, *Fashion ID* [2019] ECLI:EU:C:2019:629.
Case C-345/17 *Buivids* [2019] ECLI:EU:C: 2019:122.
Case T-259/03 *Nikolaou v Commission* [2007] ECLI:EU: T: 2007:254.
Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others* [2014] ECLI:EU:C: 2014:238.
Katerina Demetzou 'GDPR and the Concept of *Risk*' in Eleni Kosta, Jo Pierson, Daniel Slamanig, Simone Fischer-Hübner and Stephan Krenn (eds) *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data. Privacy and Identity 2018. IFIP Advances in Information and Communication Technology*, vol 547, (Springer, 2019) pp 137–154.
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281, 23.11.1995, pp 31–50.
European Data Protection Supervisor (EDPS) 'Opinion of the EDPS on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions – "A comprehensive approach on personal data protection in the European Union"' (2011). Available at: https://edps.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_en.pdf.
Gellert, Raphaël, 'Why the GDPR Risk-Based Approach is about Compliance Risk, and Why It's Not a Bad Thing' in Erich Schweighofer, Franz Kummer and Christoph Sorge (eds) *Trends und Communities der Rechtsinformatik – Trends and Communities of Legal Informatics: Tagungsband des 20. Internationalen Rechtsinformatik Symposions – IRIS 2017 – Proceedings of the 20th International Legal Informatics Symposium* (Austrian Computer Society, 2017) pp 527–532.
Gellert, Raphaël, 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) 34(2) *Computer Law & Security Review* 279–288.
Rodotà, Stefano, 'Data Protection as a Fundamental Right' in Serge Gutwirth et al (eds), *Reinventing Data Protection?* (Springer, 2009).
Lynskey, Orla, *The Foundations of EU Data Protection Law* (Oxford University Press 2015).
OECD Guidelines on the protection of privacy and transborder flows of personal data, 1980. Available at: www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

Macenaite, Milda, ‘The “Riskification” of European Data Protection Law through a Two-fold Shift’ (2017) 8(3) *European Journal of Risk Regulation* 506–540.

Purtova, Nadezhda, ‘The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law’ (2018) 10(1) *Law, Innovation and Technology* 40–81.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119, 4.5.2016, pp 1–88.

Spina, Alessandro, ‘A Regulatory Mariage de Figaro: Risk Regulation, Data Protection, and Data Ethics’ (2017) 8(1) *European Journal of Risk Regulation* 88–94.

---

[1] OO&R Radboud University.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119, 4.5.2016, pp 1–88.

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281, 23.11.1995, pp 31–50.

[4] For example, Art 24(1) GDPR on the general responsibility of data controllers, places *risk* among the criteria to be taken into account when deciding upon the most appropriate technical and organisational measures.

[5] A Spina, ‘A Regulatory Mariage de Figaro: Risk Regulation, Data Protection, and Data Ethics’ (2017) 8(1) *European Journal of Risk Regulation* 88–94. M Macenaite, ‘The “Riskification” of European Data Protection Law through a Two-fold Shift’ (2017) 8(3) *European Journal of Risk Regulation* 506–540.

[6] The WP29 (Article 29 Working Party) was an advisory body which has now been replaced by the EDPB (European Data Protection Board).

[7] Article 29 Working Party, ‘Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is “Likely to Result in a High Risk” for the Purposes of Regulation 2016/679’ in 17/EN WP 248 rev.01 (2017), 6.

[8] In the example of the legal obligation to perform Data Protection Impact Assessment (DPIA) under Art 35 GDPR, a crucial step is the identification of risks. In that sense, the scope of the concept of risk becomes relevant.

[9] Article 29 Working Party (n 7) 4.

[10] For example, the definition of who could qualify as a ‘data subject’ is dependent on the notion of ‘personal data’ (ie Art 4(1): ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’)). The same goes for the concept of ‘data processor’ (Art 4(8): ‘“processor” means a natural or legal person, public authority, agency or other body which processes personal data *on behalf of the controller*’).

[11] Article 29 Data Protection Working Party ‘Opinion 4/2007 on the Concept of Personal Data’ in 01248/07/EN WP 136 (2007), 3 ‘Working on a common definition of the notion of personal data is tantamount to defining what falls inside or outside the scope of data protection rules’.

[12] According to Art 2(1) GDPR: ‘This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.’

[13] ‘Personal data’ is a necessary but not a sufficient condition for a case to fall under the material scope of the GDPR. There needs to be ‘processing’ that is performed ‘wholly or partly by *automated means*’ or otherwise needs to be performed on ‘personal data which form *part of a filing system* or are intended to form part of a filing system’. Additionally, Art 2(2) enumerates cases that are excluded from the GDPR’s material scope.

[14] Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final, 28.10.1992, 10 (commentary on Art 2).

[15] Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final, 28.10.1992, 9.

[16] Case C-434/16 *Nowak* [2017] ECLI:EU:C: 2017:994, para 34.

[17] Article 29 Data Protection Working Party (n 11) 4.

[18] Ibid at 5.

[19] Case C-434/16 *Nowak* [2017] ECLI:EU:C: 2017:994, para 33.

[20] As explained in N Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10(1) *Law, Innovation and Technology* 40–81, was also followed in the recent *Breyer* case.

[21] Check, Case C-131/12 *Google Spain SL, Google Inc v AEPD, Mario Costeja González* [2013] ECLI:EU:C:2013:424, Opinion of AG JÄÄSKINEN, para 72 ('The fact that their character as personal data would remain "unknown" to internet search engine provider, whose search engine works without any human interaction with the data gathered, indexed and displayed for search purposes, does not change this finding.')

[22] Article 29 Data Protection Working Party 'Opinion 05/2014 on Anonymisation Techniques' in 0829/14/EN WP216 (2014), 10.

[23] Article 29 Data Protection Working Party (n 11) 13.

[24] Case T-259/03 *Nikolaou v Commission* [2007] ECLI:EU: T: 2007:254, para 222.

[25] Case C-212/13 *Ryneš* [2014] ECLI:EU:C: 2014:2428 para 28. (See also, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others* [2014] ECLI:EU:C: 2014:238 para 52, Case C-473/12 *IPI* [2013] ECLI:EU:C:2013:715, para 39.) Also, see Case C-73/16 *Puškár* [2017] ECLI:EU:C:2017:725, paras 36–38 and the case law cited thereby.

[26] Case C-345/17 *Buivids* [2019] ECLI:EU:C: 2019:122, para 41.

[27] Case C-131/12 *Google Spain SL, Google Inc v AEPD, Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 68.

[28] Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' in 00264/10/EN WP 169 (2010), 2.

[29] Case C-131/12 *Google Spain SL, Google Inc v AEPD, Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 34.

[30] Case C-40/17 *Fashion ID* [2019] ECLI: EU:C:2019:629, para 66.

[31] Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein* [2018] ECLI:EU:C: 2018:388, paras 28, 42.

[32] Case C-25/17 *Jehovan* [2018] ECLI:EU:C: 2018:551, para 66.

[33] Article 29 Data Protection Working Party (n 28) 3.

[34] Case C-40/17 *Fashion ID* [2018] ECLI:EU:C:2018:1039 AG Opinion, para 72.

[35] Case C-131/12 *Google Spain SL, Google Inc v AEPD, Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 68 and Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein* [2018] ECLI:EU:C: 2018:388.

[36] This was also highlighted by the Article 29 Data Protection Working Party (n 28) '[…] functional, in the sense that it is intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis'.

[37] The operator of a search engine in the Case C-131/12 *Google Spain SL, Google Inc v AEPD, Mario Costeja González* [2014] ECLI:EU:C:2014:317, and the Facebook fanpage administrator in the Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein* [2018] ECLI:EU:C: 2018:388.

[38] Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein* [2018] ECLI:EU:C: 2018:388, para 42.

[39] Article 29 Data Protection Working Party (n 28) 1.

[40] Ibid at 8.

[41] Ibid.

[42] Ibid.

[43] Ibid at 9.

[44] Case C-40/17, *Fashion ID* [2018] ECLI:EU:C:2018:1039 AG Opinion para 71.

[45] Ibid at para 72.

[46] Ibid at para 75.

[47] Ibid at para 92.

[48] Article 29 Data Protection Working Party (n 28) 7.

[49] Ibid at 18.

[50] At the time of writing, the EDPB has announced that the concept of 'data controller' is in its working programme.

[51] Article 29 Data Protection Working Party (n 11) 4 (Section II General Considerations and Policy Issues), Article 29 Data Protection Working Party (n 28) 4 (Section IIA Role of concepts).

[52] European Data Protection Supervisor (EDPS) 'Opinion 5/2018, Preliminary Opinion on Privacy by Design' (2018), para 25.

[53] J Alhadeff, B Van Alsenoy, J Dumortier, 'The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions' in D Guagnin, L Hempel, C Ilten, I Kroener, D Neyland, H Postigo (eds) *Managing Privacy through Accountability* (Palgrave Macmillan, 2012) 4.

[54] This is the case with all data protection principles. They are all specified through specific legal obligations of the GDPR.

[55] Alhadeff, Van Alsenoy and Dumortier (n 53) p. 27.

[56] Commission, Communication from the Commission to the European Parliament and the Council, 'Stronger Protection, New Opportunities – Commission Guidance on the Direct Application of the General Data Protection Regulation as of 25 May 2018', COM(2018) 43 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0043, 3.

[57] For the relationship between the DPIA and the principle of accountability see also: (n 7): 'it is characterised as a process for building and demonstrating accountability'.

[58] European Data Protection Supervisor (EDPS) 'Opinion of the EDPS on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions – "A comprehensive approach on personal data protection in the European Union"' (2011). Available at: https://edps.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_en.pdf, 22.

[59] Article 25(1) 'Taking into account […] as well as the *risks* of varying likelihood and severity for rights and freedoms of natural persons posed by the processing […]' *(emphasis added)*, Article 30(5) '[…] unless the processing it carries out is likely to result in a *risk* to the rights and freedoms of data subjects'*(emphasis added)*, Article 35 'Where a type of processing […] is likely to result in a high *risk* to the rights and freedoms of natural persons …' *(emphasis added).*

[60] OECD Guidelines on the Protection of privacy and transborder flows of personal data, 1980. Available at: www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[61] Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' in 00264/10/EN WP 169 (2010), 5.

[62] S Rodotà 'Data Protection as a Fundamental Right' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Netherlands, 2009).

[63] Article 29 Data Protection Working Party, 'Statement on the Role of a Risk Based approach in Data Protection Legal Frameworks' in 14/EN WP 218 (2014).

[64] For further analysis of this wording see also, K Demetzou 'GDPR and the Concept of *Risk*' in E Kosta, J Pierson, D Slamanig, S Fischer-Hübner, S Krenn (eds) *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data. Privacy and Identity 2018. IFIP Advances in Information and Communication Technology*, vol 547, 143–146 (Springer, 2019).

[65] European Data Protection Supervisor (EDPS) 'Opinion of the EDPS on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions – "A comprehensive approach on personal data protection in the European Union"' (2011). Available at: https://edps.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_en.pdf, para 99.

[66] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others* [2014] ECLI:EU:C:2014:238, para 40. See also O Lynskey, *The Foundations of EU Data Protection Law* (Oxford: Oxford University Press, 2015), para 30.

[67] R Gellert, 'Why the GDPR Risk-Based Approach Is about Compliance Risk, and Why It's Not a Bad Thing' in E Schweighofer, F Kummer and C Sorge (eds) *Trends und Communities der Rechtsinformatik – Trends and Communities of legal informatics: Tagungsband des 20. Internationalen Rechtsinformatik Symposions – IRIS 2017 –Proceedings of the 20th International Legal Informatics Symposium* (Austrian Computer Society, 2017) pp 527–532, R Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) 34(2) *Computer Law & Security Review* 279–288 at 282 '[…] "compliance risk" at the heart of the GDPR, namely the chances that a given processing operation will not comply with the GDPR […]'.

[68] Gellert, 'Why the GDPR Risk-Based Approach Is about Compliance Risk, and Why It's Not a Bad Thing' (n 67) 527–532.

[69] Ibid at 529.

[70] See Section III 'Role of *Risk* in the GDPR'.

[71] Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' (n 67).

[72] Directive 95/46: Art 1(1): 'In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.'

[73] Article 29 Data Protection Working Party (n 7) 17.

[74] Article 29 Data Protection Working Party, 'Statement of the Working Party on current discussions regarding the data protection reform package' (2013), 2.

6

Modelling and Verification in GDPR's Data Protection Impact Assessment

A Case Study on the AccuWeather/Reveal Mobile Case

WOLFGANG SCHULZ,[1] FLORIAN WITTNER,[2] KAI BAVENDIEK[3] AND SIBYLLE SCHUPP[4]

Abstract

The GDPR's obligation to the performance of a data protection impact assessment (DPIA) is one of the Regulation's new provisions. Meeting that obligation requires data controllers to have a clear picture of their processing acts and a structured approach to assessing the risks connected to them. This contribution uses a privacy-critical case, *AccuWeather/Reveal Mobile*, involving applications and implemented third parties on Apple's iOS platform, to demonstrate two important things against the background of the ECJ's *Wirtschaftsakademie* decision on joint controllership: firstly, how difficult such a risk assessment can be when multiple actors are involved in the processing to various degrees and at various steps. Secondly, how important an efficient assessment, especially in these cases, is to prevent adverse effects for data subjects. The contribution then examines *CAPVerDE*, a technical tool using formal methods, as an example of how such tools might help controllers to gain a clearer understanding of their processing environments and ultimately improve their risk assessments.

Keywords

GDPR, data protection impact assessment, privacy verification, formal methods, state of the art, joint controllership.

I. Introduction

Of the numerous challenges that have arisen with the GDPR[5] and its application within the EU since 25 May 2018, the data controller's obligation to perform a data protection impact assessment (DPIA) pursuant to Article 35 GDPR[6] is certainly one important example. While

under the now obsolete DPD[7] a similar instrument in the form of prior checks and notices existed, DPIAs promise to demand more of controllers when it comes to identifying and assessing risks connected to their processing activities.

Using the widely discussed[8] case of the iOS app AccuWeather, where a company called Reveal Mobile used implemented code in the app to gain access to data allowing the approximation of users' location even when they had specifically denied consent and the permissions granted by iOS, we want to demonstrate how technical tools can help controllers find and assess risks as well as potential measures they plan on taking against these risks. We chose this case because of its complex constellation of actors and the issues resulting from it: latent risks of forbidden data access and the fact that neither actor is capable of eliminating those risks completely on their own. Where this is the case and one actor cannot eliminate, but only mitigate, risks an efficient and dependable approach to assessing the effectiveness of mitigating actions and their sufficiency regarding GDPR compliance becomes paramount.

Because the inclusion of other ad-monetisation companies and their code in smartphone apps is the rule, rather than the exception, this case also brings with it a certain amount of practical importance. Analysing the case and the actors involved, we focus on Apple as the company behind iOS and on AccuWeather as the company behind the eponymous app, whose inclusion of Reveal Mobile's code opened the door for their collection of users' data. Taking into account the important role Apple – or rather iOS – plays as a gatekeeper for iPhone apps and expanding on the criteria hypothesised by the ECJ in the decision of *ULD Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein*,[9] we classify Apple and AccuWeather as joint controllers who both need to meet their obligations under Article 35.

After a short legal analysis covering the roles and obligations of these controllers and giving an assessment of the potential legal bases of the processing acts that occurred in the case, we try to demonstrate how the performance of a DPIA, supported by a technical tool, could have anticipated, or at least made transparent, the possibilities of an unwanted collection of data by Reveal Mobile.

CAPVerDE is a tool for designing architectures with privacy properties and generating proofs by using formal methods to verify or falsify given statements. By using *CAPVerDE*, we model the architecture of the actors involved in the case with regard to data flows and the general possibility of acquiring users' location data or data that can be used to approximate their location. We then try to quantify the risks detected and match the result with envisaged mitigation actions to calculate the probability of a risk realising itself. This might help controllers working with complex processing environments or sensitive data better assess the suitability of their measures as well as prove said suitability to the Data Protection Authorities (DPAs) receiving their DPIAs.

To conclude, we evaluate the benefit of this tool-assisted assessment using three different categories: real-world use, scientific gain, and its potential contribution to the advancement and concretisation of the GDPR's technology-sensitive provisions.

II. Case Description and Legal Classification

The case of AccuWeather became publicly known in 2017 when a security researcher reported that iPhone users' location data was being sent to a third party called Reveal Mobile when using the AccuWeather app, even when access to that data was declined by the users at the operating system level.[10] A similar case concerning InMobi, a competitor of Reveal Mobile, had occured as early as 2015 and had even been handled by the US Federal Trade Commission (FTC).[11] AccuWeather, an app offering weather forecasts specific to the users' location, had implemented an SDK[12] developed by Reveal Mobile, a company that helps app developers monetise their apps by displaying third-party advertisements. Through this implementation, the Reveal Mobile code was executed with the same access rights granted to AccuWeather by the operating system. The location data gathered through this access[13] were then enriched with real-world context, for example, the companies and stores located at the respective addresses, which allowed Reveal Mobile to find patterns in users' location histories. These patterns could then be used by advertisers to target specific consumers by matching their desired characteristics.[14]

A. Technical Description

On a technical level, different kinds of data were used to determine or approximate users' locations. Where users gave the app permission to track their location, it could utilise iOS's Core Location API[15] that – depending on the app's needs and other factors like reception – falls back on 'GPS, Bluetooth, WiFi hotspot and cell tower locations'[16] to determine or approximate the location. Where users denied permission, no access through the Core Location API was possible. However, AccuWeather (or rather Reveal Mobile through AccuWeather) could still gain access to data such as connected WiFi router names, BSSIDs[17] and the users' current Bluetooth status.[18] These data were not transmitted through iOS's Core Location channel, but went around this channel, instead using the Captive Network API, an interface that could be accessed by apps independent of the user's permission choices. By matching these data with public databases listing the locations of wireless access points, Reveal Mobile was able to infer respective locations.[19]

B. Legal Analysis

Data collected from a user's smartphone are information relating to the owner of the smartphone, an identified or at least identifiable natural person, and are therefore personal data pursuant to Article 4(1).[20] Data relate to an identified person when his or her identity is directly recognisable from them and relate to an identifiable person when his or her identity can be inferred directly or indirectly through an identifier or in combination with other data available to the person processing. Article 4(1) explicitly names location data as one type of identifier. Ultimately, the distinction between data relating to identified or identifiable persons is moot; the GDPR treats both merely as personal data and therefore the same.[21]

This means that all acts of processing regarding these data must rely on one of the legal

grounds established in Article 6 and adhere to both the general principles listed in Articles 5 and several specific obligations throughout the GDPR.

i. Controllership

The responsibility for acting compliant in the face of these obligations belongs to the controller(s), one or more actors who are, according to Article 4(7), determining the purposes and means of the processing. This means that the classification of involved actors must follow a functional analysis of the respective scenario with regard to who has the authority over the essential decisions.[22]

Reveal Mobile is arguably the most central actor in this case: it collected location data for the purpose described above and, therefore, clearly acted as a controller. For the purposes of this chapter, though, we focus on analysing the roles of Apple and AccuWeather.

AccuWeather never had any direct contact with their users' location data, at least in those relevant cases where consent in this regard was denied. As described above, those data passed directly from the users' smartphone to Reveal Mobile while the AccuWeather app was merely the vessel through which Reveal Mobile was able to gain access to the phone. However, AccuWeather intentionally implemented Reveal Mobile's SDK as part of their decision to monetize their app through advertisements. It remains unclear whether AccuWeather knew about Reveal Mobile's intention of using every technical loophole available to gain mediated location data,[23] but ultimately that does not need to be answered conclusively. Ill will or not, by implementing Reveal Mobile's SDK they directly determined the means through which it was able to collect the data. Furthermore, the scope of affected users was contingent on the app's user base. Only those users attracted by the AccuWeather app could be affected. Following the ECJ decision mentioned before,[24] this 'definition of parameters'[25] of data subjects also constitutes a certain determination of processing purpose. AccuWeather, therefore, acted as a controller when Reveal Mobile collected location data from app users. A lack of direct influence in the moment of data collection is irrelevant in that regard, as controllership does not necessarily require access to the data in question.[26]

Apple, similarly, did not have any direct access to the data in question. However, their involvement does, in our opinion, appear in two prominent ways. Firstly, Apple is a company with a harsh and rigid review process regarding the admission of apps on the iOS AppStore. Possible candidates are thoroughly checked and vetted for different characteristics, including their level of privacy and data security.[27] Secondly, Apple – just like their biggest competitor Google does with Android – chooses to handle user permissions globally at the level of the operating system. Correspondingly, they offer app-dedicated APIs for accessing user data in accordance with given or refused admissions. This means that while, at first glance, Apple is relatively far away from any interaction happening between app users and apps (including third parties embedded into those apps), they factually make the decision to act as an intermediary governing the way those transactions took place.[28] This idea can again be combined with the notion of Apple as an especially fierce gatekeeper regarding admissions to their AppStore. Both to app developers and users, Apple brands their AppStore as a place

that takes data protection and security very seriously[29] and thereby differentiates itself from its less-secure and less-regulated competitors such as Google with Android. It can, therefore, in our opinion, convincingly be argued that through these measures Apple contributed to and shaped the determination of both the processing purposes and means: by regulating which apps with which purposes are admitted to the AppStore, by handling user permissions on the level of their operating system and providing the data access APIs. Apple therefore somewhat appropriates the purposes and designs of AppStore-admitted apps, leading to a kind of symbiotic relationship creating benefits for both actors: the app profits from the large number of iPhone users, while Apple profits from the appeal of the apps on their platform. It thus seems reasonable to classify Apple and AccuWeather as joint controllers regarding the processing of location data by Reveal Mobile.[30] This also best reflects the different impact levels exerted by the actors in the different stages of processing.[31]

ii. Legal Basis According to Article 6

Next, we provide a short assessment of the lawfulness of the processing acts in question with regard to the applicability of one of the legal bases listed in Article 6.[32]

(a) Consent

Firstly, the affected users could have expressed their free, specific, informed and unambiguous consent regarding the processing of their data for the approximation of their location (Article 4(11)(6)(1)(a)).

Such an act of expressing consent could be seen in the mere usage of the app and the acceptance of AccuWeather's privacy policy. In this policy, AccuWeather made transparent (and still does, in their newest version[33]) that (location) data are shared with third parties for several purposes, including so-called Online Behavioural Advertising (OBA). It also, in accordance with Article 13(1)(c), describes consent as the legal basis that it wants to use for its processing acts.[34] While it is already questionable if this meets the requirements for an informed and specific consent, the fact that this sharing with third parties is designed as an opt-out instead of an opt-in regime is even more doubtful, not least because Article 4(11) clearly demands consent in the form of an 'unambiguous indication' of the subject's wishes.[35] Article 25(2) formulates the principle of data protection by default as an important and binding provision of the GDPR, obligating controllers to design their systems in a way where by default only the least amount of data necessary is being processed. In addition, recital 32[36] substantiates that 'silence, pre-ticked boxes or inactivity should not therefore constitute consent'. In light of these facts, it would be highly questionable to accept the mere usage of the AccuWeather app as an effective expression of consent legitimising the processing of location data.

Furthermore, in the cases relevant to our argument, users even explicitly denied the sharing of location data when asked through the iOS prompt. Even if one were to assume an implicit expression of consent through the usage of the app and acceptance of its privacy

policy, this denial of admission would, as an explicit act of denial, certainly serve as a withdrawal of consent pursuant to Article 7(3).

Therefore, the processing of location data cannot be based on the users' consent.

(b) Legitimate Interests

Secondly, the controller's (or a third party's) legitimate interests can, according to Article 6 (1)(f), serve as a legal basis for processing acts unless the data subject's interests or fundamental rights in the specific case outweigh them. Here, recital 47 further elaborates on the criteria for such an assessment. While it states that 'relevant and appropriate relationships' between data subject and controller can provide the basis for such legitimate interests, it also states that the question whether a data subject 'can reasonably expect […] that processing for that purpose may take place' should be an elemental part of the assessment.

As was described above, users in this case had explicitly expressed their denial of submitting location data to the AccuWeather app. While AccuWeather's privacy policy did inform their users about their intention of sharing data with third parties, it also said that: 'When You use AccuWeather Sites, You consent to the terms and conditions and the practices described in this Privacy Policy.'[37] This creates the impression that consent was the only legal basis on which AccuWeather based their processing. The users could therefore not reasonably expect the sharing of location data to continue even after they denied permission. Finally, even if one were to come to the conclusion that AccuWeather's interests in sharing those data with Reveal Mobile outweigh the users' interests, the omission of stating Article 6(1)(f) as the legal basis of choice in the privacy policy would be a violation of the obligation in Article 13(1)(c).[38]

The processing of user data could therefore not be based on legitimate interests.

C. Interim Result

In conclusion, Apple and AccuWeather acted as joint controllers whenever Reveal Mobile was able to collect users' location data through the AccuWeather App. They did not have any legal grounds upon which to base this processing.

III. Logic and *CAPVerDE*

This section introduces the formal basis for a formal verification of privacy properties in software systems. It is a somewhat technical description of what can be (formally) described by the language and how this description is used to make claims regarding privacy. Described in a simple manner, this is achieved by modelling the architecture of a certain system including its relevant actors as well as abilities and expectations regarding data and information flow. By comparing expectations with what is possible within the system,

privacy claims can be verified. For the purposes of this chapter, we assume that the formal description of the system comes from the controller and is considered as input for the verification tool.

We make use of the Computer-Aided Privacy Verification tool (*CAPVerDE*).[39] It is a free, open-source automatic privacy verifier that can be used to model software systems on the architectural level and automatically verify privacy properties for the modelled architectures.[40] The logic and tool are based on the work of Le Métayer.[41] To support the modelling of necessary elements such as consent and impact, we extended the formal language of *CAPVerDE*. In the following, we briefly describe the extensions to the formal framework and then model the AccuWeather system in the formal description language of *CAPVerDE* and perform the first step necessary for the impact assessment. Later, in section IVB, we continue with the second step of our formal impact assessment by modelling two possible measures for the two actors Reveal Mobile and Apple, mentioned earlier, and analyse their respective impact.

Table 6.1 Syntax of relations describing the data flow of a software system

$R ::= Has_i(\tilde{X})$	$Compute_i(\tilde{X} = T)$
$Receive_{i,j}(\{\tilde{X}\})$	$CReceive_{i,j}(\mathcal{DT}, \{\tilde{X}\})$
$Permission_{i,j}(\mathcal{DT})$	$Revoke_{i,j}(\mathcal{DT})$

CAPVerDE's framework consists of a description language for software architectures and privacy properties where the former describes the status quo of the system and the latter what we expect of it. The tool uses inference rules for the verification process to decide whether a property ϕ holds for an architecture A. We extended the syntax of the architecture language with three new relations. Relations model the information and data flow in an architecture. An architecture consisting of components C_i is described by its relations. The full set of relations necessary for the scope of this paper is shown in Table 6.1. The relations include $Has_i(\tilde{X})$ which expresses that component C_i has the ability to obtain variable $\tilde{X}$ from outside the system, for example, via a sensor. This is how data enters the system. $Compute_i(\tilde{X}=T)$ denotes the fact that component C_i can compute the variable $\tilde{X}$ from the right-hand-side term T. This is how data is computed or processed, for example, how they are encrypted or aggregated. $Receive_{i,j}(\{\tilde{X}\})$ expresses that component C_i can receive a set of variables $\{\tilde{X}\}$ from component C_j. This models the inter-component data flow when data is shared between components (possibly two different actors). While this transfer of variables represents data flow, the following relations model the flow of consent. These new relations are $Permission_{i,j}(\mathcal{DT})$ and $Revoke_{i,j}(\mathcal{DT})$. While the former expresses that component C_i gives component C_j permission (e.g., user consent) regarding variables belonging to the data type $\mathcal{DT}$, $Revoke_{i,j}(\mathcal{DT})$ is the opposite denoting the revocation of a given permission. The introduction of consent into the system also calls for the need of a new form of data flow.

$CReceive_{i,j}(\mathcal{DT}, \{\mathcal{X}\})$ is the relation that only shares data if a valid consent is held. $\mathcal{DT}$ represents a data type, that is, a predefined set of variables that belong to one category. The relation $CReceive_{i,j}(\mathcal{DT}, \{\mathcal{X}\})$ models the option of a conditional receive where component C_j gives component C_i a set of variables $\{\mathcal{X}\}$ belonging to a certain data type $\mathcal{DT}$ if there is a valid permission given to component C_i regarding this data type.

We also extended the syntax of the properties to express the violation of user consent. We introduce a property called $consentViolated_i(\mathcal{DT})$ that is true if the component C_i passes on variables from the data type $\mathcal{DT}$ without the corresponding consent. We use this property to detect the leaking of sensitive data without user consent for the impact assessment.

While the syntax is used to formalise the description of a software system, the semantics are necessary to define how the relationships affect the architecture's state. The semantics of the architecture language are defined via states, events and traces. Informally, we can say that each component keeps track of its knowledge about the system, including the variables it knows or the data flow involving it. The relationships are considered events that can be triggered in arbitrary order (as long as the consistency is not violated, for example, a variable cannot be used for computation before it is obtained). A trace is the observation of such an arbitrary order of events. A trace alters the (initial) state of the architecture with each event. The impact of an event (relation) on the state of the architecture, which is just the collection of states of the components, is described by the semantics. In this chapter, we only present the semantics' definitions of the new relations ($CReceive_{i,j}(\mathcal{DT}, \{\mathcal{X}\})$, $Permission_{i,j}(\mathcal{DT})$, and $Revoke_{i,j}(\mathcal{DT})$). S_E is the semantics function that takes an event and a state and returns a state σ, which denotes a state of an architecture, consisting of the states of all components σ_i. These states consist of different sub-states which store information and data for their respective components. For the context of this chapter, we only consider the origin state σ_i^o keeping track of where data came from and the consent state σ_i^c keeping track of given and revoked user consent. $S_E(Permission_{i,j}(\mathcal{DT}),\sigma) = \sigma[\sigma_j/(\sigma_j^o, \sigma_j^c \cup \mathcal{DT})]$ is the definition of the semantics of the consent relation. The notation of $\sigma[\sigma_j]$ is the replacement of an architecture's state by a state that only differs in the component's state σ_j. Similarly, the notation $\sigma_j/(\sigma_j^o,..)$ describes the replacement of a component's state by the listed sub-states. The property that only the state of component C_j changes (hence only σ_j) in only the consent state (σ_j^c), which is extended by adding the data type $\mathcal{DT}$. This simply expresses that component C_j now knows that it received a consent for the data $\mathcal{DT}$. $S_E(Revoke_{i,j}(\mathcal{DT}), \sigma) = \sigma[\sigma_j/(\sigma_j^o, \sigma_j^c \backslash \mathcal{DT})]$ is the semantic definition of the revoke relation. Similar to the consent relation, we only change the

consent state of component C_j by removing the data type $\mathcal{DT}$. This has the opposite impact as the component now knows that it no longer has consent. The conditional receive relation has a different impact on the state of the architecture:

$$S_E(CReceive_{i,j}(\mathcal{DT},\{\tilde{X}:V\}),\sigma) = \sigma[\sigma_i/(\sigma_i^o[\{\tilde{X}:j\}],\sigma_i^c \cup \mathcal{DT})] \quad \text{if } \forall_{\tilde{X}},\ \tilde{X} \in \mathcal{DT} \wedge \mathcal{DT} \in \sigma_j^c$$
$$= \sigma[\sigma_j/Error] \text{ otherwise}$$

This event also alters the origin state σ_i^o. The notation $\tilde{X}$*:V* expresses that the variable $\tilde{X}$ is assigned a value *V*. For *{*$\tilde{X}$*:j}* this expresses that component C_i (the receiving component) keeps track of the fact that it received variable $\tilde{X}$ from component C_j. This event also adds the data type $\mathcal{DT}$ to the known consents.

Error denotes the error state.

The other introduced relations like $Has_i(\tilde{X})$ also affect the sub-states of involved components. The details about the semantics of these relations is outside the scope of this chapter but can be found in related work.[42] This concludes the semantics of relations and therefore the architectures. Next, the semantics of properties are introduced.

For the verification of properties, semantically, the logic makes use of the states introduced in the architectures' semantics. The semantics of properties are defined via architectures satisfying the properties. The semantics of the introduced consent-violation property is defined as:

$$A \in S\left(consentViolated_i(\mathcal{DT})\right) \Leftrightarrow \exists_{\sigma \in \mathcal{S}(A)},\ \exists_{\tilde{X} \in \mathcal{DT}},\ \sigma_j^o\ (\tilde{X}) = i \wedge \mathcal{DT} \notin \sigma_i^c$$

where $\mathcal{S}(A)$ denotes the set of all possible states σ of the architecture *A* (ie the resulting states of all possible traces and sub-traces). The property holds for an architecture if a state exists in which the component C_i has passed on a variable for which it does not have the corresponding consent. For this the origin state and the consent state are checked for all possible sequences of events.

CAPVerDE verifies properties based on inference rules. The notation $\frac{premise_1,\ \ldots\ , premise_n}{conclusion}$ expresses that the conclusion holds true if all premises hold true. $A \vdash \phi$ denotes the fact that the architecture *A* satisfies the property ϕ. The inference rule ***C*** regarding the *consentViolated* property is:

$$C\frac{Receive_{j,i}(E) \in A \quad \exists_{\mathcal{DT}}, E \cap \mathcal{DT} \neq \emptyset \wedge \left(Revoke_{i,k}(\mathcal{DT}) \in A \vee Permission_{i,k}(\mathcal{DT}) \notin A\right)}{A \vdash consentViolated_i\ (\mathcal{DT})}$$

Here E is a set of variables that is passed on. The rule can informally be read as follows. The architecture A satisfied the property $consentViolated_i(\mathcal{DT})$ if component C_i shares a set of variables E with another component and E contains at least one variable that is covered by the data type $\mathcal{DT}$ and either does not have a matching consent for said data type or the consent was revoked. In this case 'A satisfies the property' means a violation of missing or revoked consent.

Using this rule the tool can detect whether the consent for a certain data type was violated. The only part missing for the impact assessment is the impact level and the probability of occurrence. We define the weighting function $\omega: Var^n \rightarrow Int$, with $\omega(location) := 4$ to assign impact levels from 1 (negligible) to 4 (maximum) to data types. This is based on the sensitivity of these data (eg, the leaking of location data has a maximum impact level due to its close proximity to – and probability of drawing inferences regarding – the sensitive data listed in Article 10).[43] Similarly, the probability of occurrence of a potential breach is also defined from 1 (negligible) to 4 (maximum). The levels negligible, limited, comprehensive, and maximum are not formally defined but derived from examples. For instance, the probability level could be set by answering the question 'How easy is it for a potential malicious party to breach the privacy?' For the probability level, one must evaluate the complete system and it often heavily depends on the implementation. Therefore, this level is derived user input that is supported by guidelines to classify it on the described scale.[44]

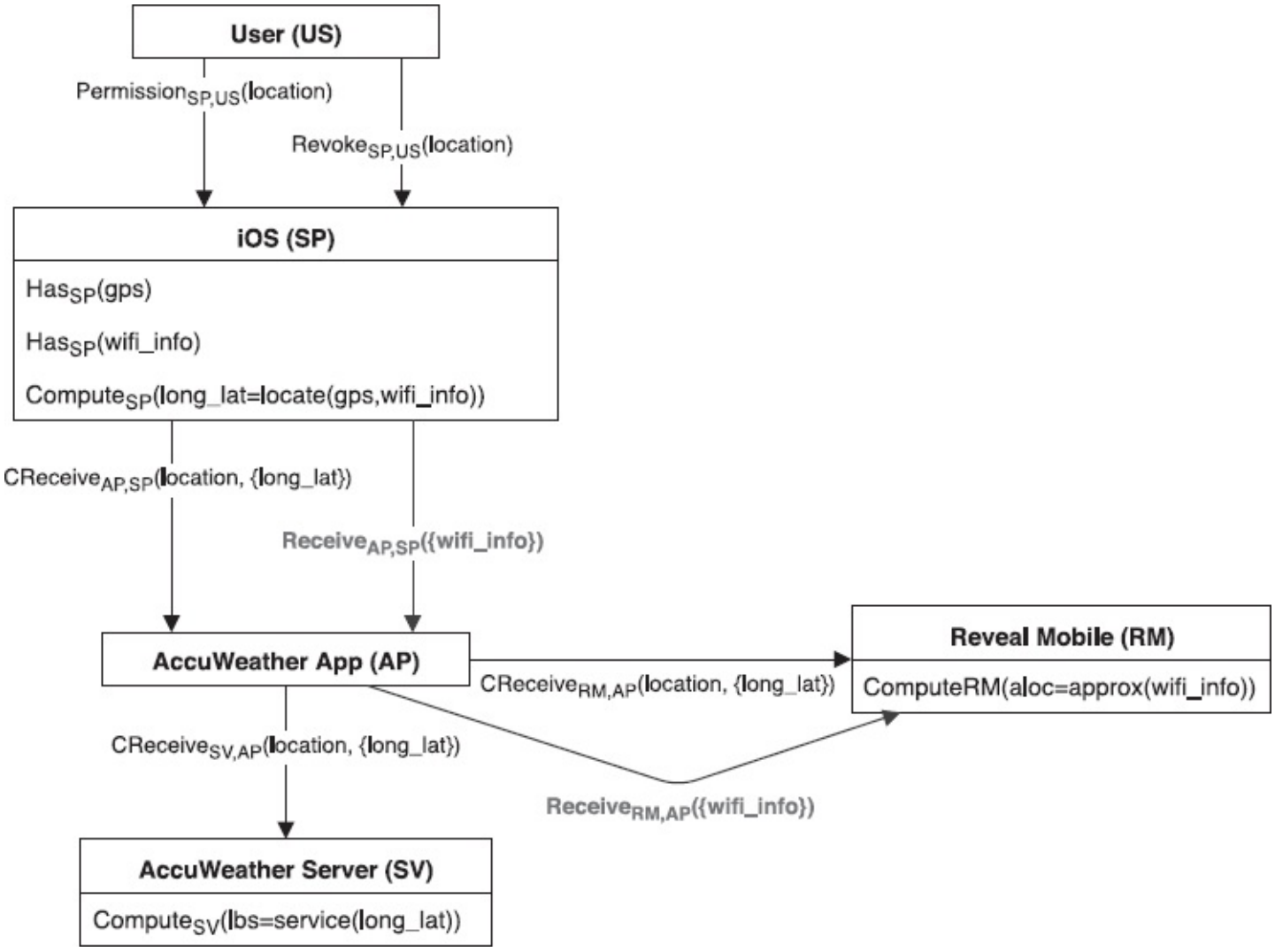
The overall level of a potential risk is the product of the impact level and the probability level and thus scales from 1 to 16, where 1 and 2 are considered a low risk, 3 to 9 a medium risk, and 12 and 16 a high risk. This level corresponds to the 'high risk' mentioned in Article 35 (1). This is visualised in the heat map in Figure 6.1.

Figure 6.1 Risk assessment heat map

		Risk Assessment				
	Impact Level[45]					
maximum	4	4	8	12	16	
comprehensive	3	3	6	9	12	
limited	2	2	4	6	8	
negligible	1	1	2	3	4	
		1	2	3	4	Probability
		negligible	limited	comprehensive	maximum	
Low Risk	Medium Risk				High Risk	

Figure 6.2 shows the graphical representation of the AccuWeather case including the principal actors: the user (US), the iOS platform (SP), the AccuWeather iOS app (AP), the remote AccuWeather service (SV) and the Reveal Mobile SDK (RM). As described in IIA, we see how iOS provides two different ways for the app to access or compute the approximate location of the user. In more detail, the user can give consent for the sharing of location data (*location*) with apps on the iOS device. The user can also revoke this consent. For simplification, in our model iOS can only use the GPS information (*gps*) and WiFi information (*wifi_info*) to estimate the location of the user (*long_lat*). An app such as AccuWeather can access *long_lat* if there is a valid consent for *location* via the Core Location API. An app can also access *wifi_info* (including the BSSID) via the Captive Network API without having to rely on user consent. In fact, at server side, AccuWeather only uses the consent-based location *long_lat* for its service to provide the location-based service (*lbs*). The Reveal Mobile part of the app utilises both channels to access the location of the user, the consent-based *long_lat* and the *wifi_info*. The latter is used to derive an approximate location (*aloc*).

Figure 6.2 Architecture of the original AccuWeather system with critical data flow highlighted in red



Furthermore, we must define all data types in terms of variables. *location = {gps, wifi_info, long_lat, aloc}* is the only data type in the architecture.

This description is already the first step of a two-fold formal verification. Describing the actual system in a formal language can also help make the system more readable and understandable for non-experts. Making use of a graphical representation that displays the explicit data flow can be beneficial for this task.

IV. Data Protection Impact Assessment According to Article 35 GDPR

In the following paragraphs, we want to both introduce the general rationale and typical process of a DPIA and model an exemplary DPIA performance including possible measures to counter the risks using the two actors examined above. We then show how *CAPVerDE* can help controllers check the efficiency of their chosen measures with regard to the risks they identified and assessed.

A. General Rationale

Article 35 obliges controllers planning processing acts connected to especially high risks for data subjects to run through these acts and assess the specific risks, the likelihood of them realizing, and possible mitigation actions as well as their potential effectiveness. The ideal conception behind this is the fostering of better data protection compliance in high-risk areas by increasing responsibility of controllers, making them more aware of privacy implications connected to their processing acts in the early stages of their development and planning.[46] In the end, only those acts whose risks, according to the controller's assessment and – in a second step – the DPA's opinion,[47] have been correctly identified and sufficiently mitigated,[48] should be further employed by their respective controllers.

On a broader scope these assessments, when performed efficiently, can help develop efficient measures across Europe. Increased exchanges between DPAs and controllers lead to more DPA knowledge about typical high-risk processing acts and about new and innovative measures that controllers may come up with. This, combined with the certification schemes described in Article 40 et seq., can lead to a better guidance for other controllers or even to standard setting and thus increased compliance throughout society. Conversely, new acts of processing whose risks are impossible to mitigate sufficiently at a certain time might be prevented from being used until state-of-the-art mitigation actions have progressed accordingly.

B. Application on Case

Considering these general thoughts, how would the performance of a DPIA by Apple and AccuWeather have affected the case at hand as well as similar cases? While not every measure towards compliance merits the performance of a DPIA, we argue that the specific constellation of actors in this case makes the DPIA the ideal instrument to emphasise the following: the possibilities of exerting influence for joint controllers that do not process data themselves are typically situated upfront of the processing act itself. Conversely, the obligations for such controllers, stemming for example from Article 24, are therefore typically directed at influence on the level of the framework or architecture structuring the cooperation between the relevant actors.

Taking into account the mitigating actions taken by these actors in the aftermath of the public debate over the case and new measures that have not been applied but have partially been recommended by other (affected) actors, we demonstrate how such an assessment – when supported by *CAPVerDE* – could have foreseen and mitigated the probability of an unlawful collection of location data by Reveal Mobile.

i. Obligation to Carry out a DPIA

According to Article 35 (1), carrying out a DPIA is obligatory for controllers where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons.

While the assessment of this risk is usually done on a case-by-case basis by the controller, DPAs can provide certainty by putting typical high- or low-risk processing acts on so-called black- or whitelists.

In our case, the processing of location data was the processing act in question. At least for those app users consenting to the usage of these data, AccuWeather planned on both processing them for the purpose of the app (offering weather forecasts for the user's current location) and for monetisation through the sharing of these data with Reveal Mobile. In the blacklists drafted by DPAs so far, the processing of individuals' location data on a large scale is listed as an activity that triggers the obligation of Article 35 (1).[49] Similarly, the Article 29 Data Protection Working Party[50] included the processing of location data in their guidelines on DPIAs.[51] It can, therefore, be concluded that the general usage of the app demanded controllers to carry out a DPIA.

ii. The Actual DPIA

A DPIA can be structured along three basic steps: the systematic description of the planned processing acts and assessment of general risks connected to it, the development of mitigation actions and an assessment of their effectiveness and, lastly, the decision as to whether the resulting risk has been sufficiently mitigated to go through with the processing.

Because Apple and AccuWeather are classified as joint controllers in our case, we model their DPIA as one combined effort covering the combined risks stemming from their respective contributions, but ultimately relating to one set of processing: the retrieval of the users' location or network data by the AccuWeather app or third parties implemented in the app's code. Consequently, the origin of the measures is irrelevant as long as they mitigate all risks. This is in line with recital 92, which states that it can be 'reasonable and economical for the subject of a data protection impact assessment to be broader than a single project […]', especially where several controllers '[…] a common application or processing environment across an industry sector or segment for a widely used horizontal activity'.

Lastly, because we are most interested in the technological risks attributed to the case, we limit the 'DPIA' we run here to those risks most interesting from a technical perspective. We are aware and do acknowledge that the following is not a complete DPIA in the way a controller such as Apple or AccuWeather would have carried it out.

(a) First Level: Assessment of Risks

The first level of the DPIA includes the controllers' systematic description of the system's internal and external architecture as well as the planned processing acts and their purposes. It also includes the normative assessment of how this description fares in relation to the GDPR's obligations and principles and a description and assessment of the risks resulting from this comparison. This first level corresponds to the preparation phase and the assessment phase of the four-part DPIA process introduced by the ULD, Schleswig-Holstein's DPA,[52] or the context and fundamental principles as well as part of the risks phase

developed by the CNIL, the French DPA.[53]

As described above, the processing act in question for our case is the collection of location data.[54] The legal analysis above shows us that the lawfulness of this act is dependent on the users' consent. Where this consent is missing, the collection of location data is unlawful. Depending on the way we look at the case, the main privacy risk can therefore be defined either as the risk of a processing happening without the required legal basis, or as a data security risk regarding unwanted access from a risk source in the form of Reveal Mobile. The model in Figure 6.2 further shows us that two actors had the possibility of collecting those data through the AccuWeather app: AccuWeather themselves (here described as the AccuWeather server) and Reveal Mobile. Thus, the primary risk was the transmission of location data to either of these actors in cases where no user consent was given or such a consent had been revoked.

The model also shows that two possible channels for collecting location data existed. Exact location data could be collected through Apple's Core Location API, while network routers' BSSID data could be collected through the Captive Network API. The first channel, through the Core Location API, has always been dependent on the users' permission. Where no such permission was given, the API could not be used. The Captive Network API, however, had been active and permission-independent at the time of the case. Leaving this channel open constituted a high risk of an unlawful collection or transmission of data. Regarding AccuWeather, this risk was somewhat mitigated as their privacy policy clearly stated that the sole purpose of processing location data was the improvement of their app's functionality and user experience by offering weather forecasts directly for users' current locations. Where users did not care for this functionality and thus did not give permission, this purpose ceased to be relevant. For Reveal Mobile, however, the purpose of gaining knowledge about the users through their past and current locations in order to display relevant advertisements to relevant users stands even where a corresponding user consent is absent. An open and permission-independent API allowing access to data that – while somewhat less sensitive than direct location data – allowed for the approximation of users' locations through rather simple means combined sensitive data with a high probability of their collection by an illegitimate actor.[55]

Loosely following the traditional risk level estimation as a sum of the severity and likelihood of the occurrence of a specific risk, a first assessment would have thus shown a very high risk for the users of the AccuWeather app.

(b) Second Level: Possible Solutions

At this stage, we look at several measures that Apple and AccuWeather could have envisaged to mitigate this risk. For the selection, we draw on different kinds of sources: measures that Apple applied after being confronted with the AccuWeather case, measures that were suggested by knowledgeable third parties and measures that were inspired by approaches from other areas of law. They can be loosely divided into technical, legal and procedural measures.

This level corresponds to the first half of the measure phase as introduced by the ULD[56]

and another part of the risks phase as described by the CNIL.[57]

Technical

No Access to BSSID Data

A possible technical solution Apple could– and did actually choose to apply in iOS version 11 – is to completely deny the access to the Captive Network API and thus prohibit apps from obtaining WiFi information including the BSSID. This prevents the leakage of location-revealing data via the described channel. This is a somewhat conservative approach as this solution affects all apps on the Apple App Store, including network analysis apps that have a legitimate reason to use the Captive Network API to obtain MAC addresses of access points or routers and display them to the app user. As mentioned above, this measure was implemented in iOS 11;[58] however, Apple were criticised by developers who could no longer support their network analysis tools on the latest version of the operating system and even started a petition against this measure.[59]

Figure 6.3 shows the architectural representation of the described measure. The Captive Network API is no longer accessible and the app can therefore no longer obtain the *wifi_info* directly. Thus, Reveal Mobile can only access *long_lat* via the consent-based Core Location API channel.

Controlled Access to BSSID Data

Another technical measure that Apple could have taken is altering the access rights management related to the Captive Network API and restricting access to the API for apps. Only apps that have a legitimate reason to use the API would then get access. This was proposed by an iOS app developer[60] as a possible solution that would prevent a similar situation but would still allow some apps (that need it for legitimate purposes) to use the Captive Network API. Apple already has a strict reviewing process that analyses apps and their requested access rights.[61] App developers already have to submit additional meta-info in addition to their app including fields that defend their requests for access rights. Therefore, this measure does not require new software or reviewing processes but fits into the existing process.

Figure 6.3 Architecture after the implementation of the first measure

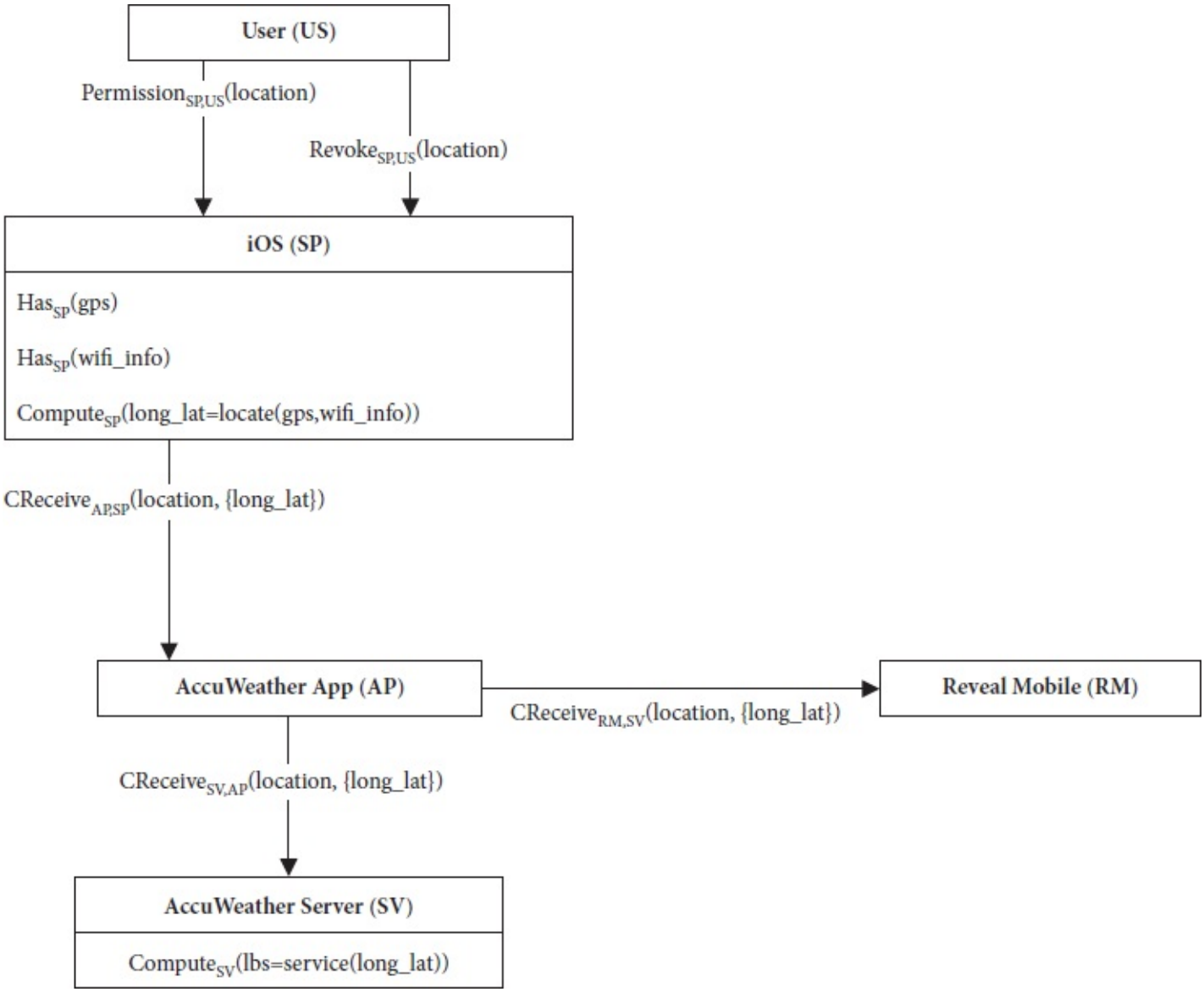


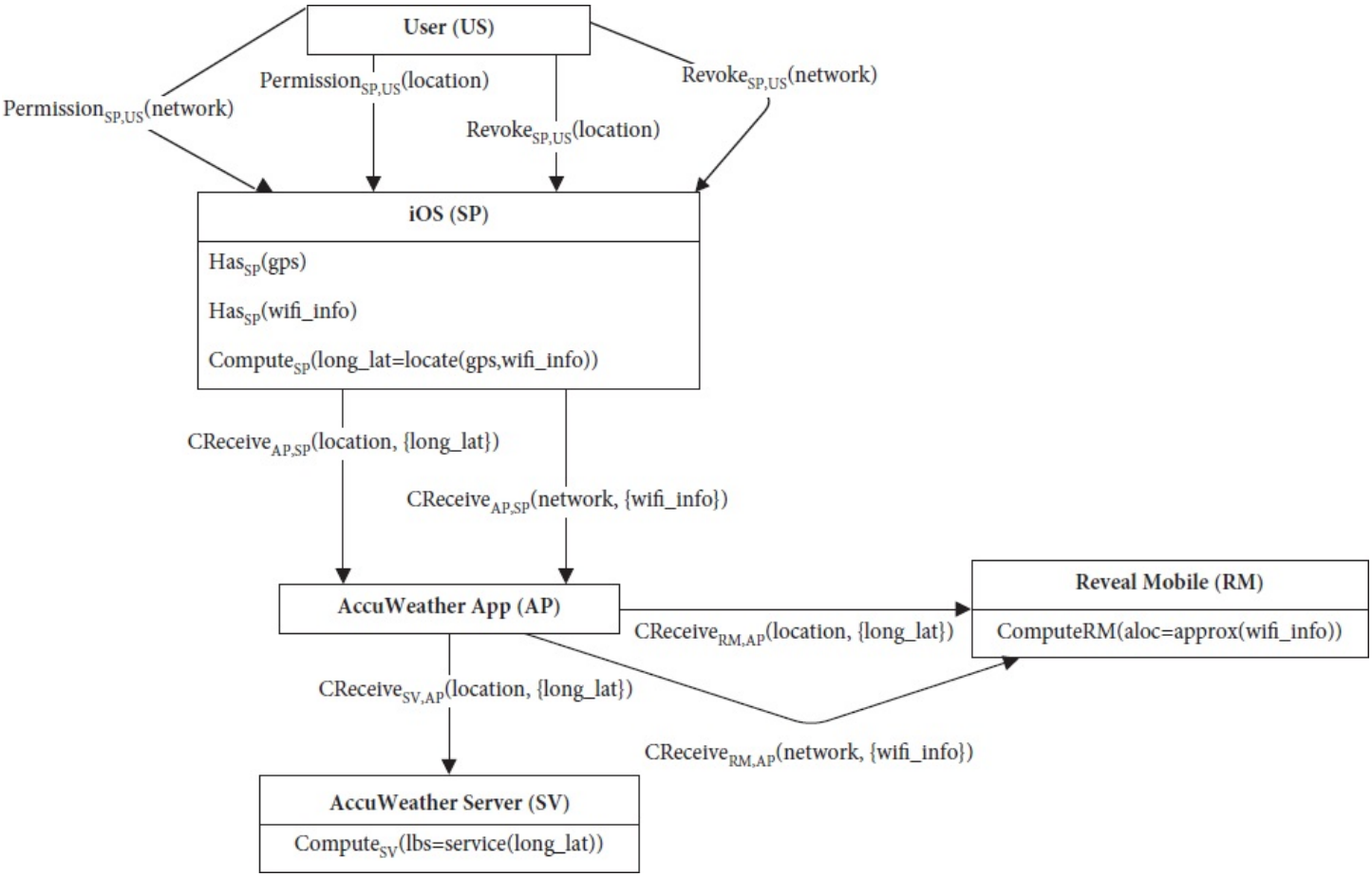
Figure 6.4 shows the architectural representation of the measure described above. Now the iOS platform introduced the *network* data type that all apps need permission for to access *wifi_info* via the Captive Network API. The decision is based on the type of app. A weather app like AccuWeather would most likely not have sufficiently convincing arguments for why it needed to access MAC addresses of WiFi access points. This change in access rights leads to different relationships. The transmission of *wifi_info* is now a conditional receive related to the *network* permission. The new data type is defined as *network = {wifi_info}* and the location data type changes correspondingly: *location = {gps, long_lat, aloc}*.

Change or No Usage of Third-Party SDK's

A possible measure for AccuWeather could have been the abandonment of any or at least the selection of other companies' SDK(s). The first of these options would have arguably mitigated the risk of an illegitimate collection of location data significantly by eliminating third parties altogether. Considering the importance of 'selling' user data for monetisation purposes in free-to-use apps, however, such a measure would have been highly unlikely. Similarly, as a plethora of companies like Reveal Mobile offer their SDK's to collect data for

the same purpose(s), choosing a different one might not have made a difference. As the *InMobi* case has demonstrated, the case of Reveal Mobile has not been an isolated one. It is fair to assume that other competitors have acted and/or act in the same way but have not (yet) been caught.

Figure 6.4 Architecture after implementation of the second measure



Legal

A possible legal measure for AccuWeather could have been to insert a contract clause explicitly prohibiting, under threat of a contractual penalty, Reveal Mobile from collecting any location-related data where no user permission is granted. This measure, while not outright making it impossible for Reveal Mobile to illegitimately collect data, would still have a deterrent effect to some degree.

Procedural

Another measure that Apple could have taken can be compared to the so-called ‘notice-and-take-down’ and ‘notice-and-scan’ approaches applied mainly to host providers with regard to illegitimate third-party content violating copyrights or personality rights.[62] It states that host providers should react within a reasonable timeframe to notices by rights holders or other third parties about such illegitimate practices. This obliges hosts to check if such allegations are true and to take down the respective content where they conclude that it is. It also obliges them to offer necessary communication channels – both for those giving notice and for those being accused – to allow for responses and explanations. A second obligation then arises for

the future: hosts must regularly check and make sure – within the limits of reasonability – the same violation doesn't occur again. This can be done by suspending the respective user's account or checking for the re-uploading or re-posting of files with the same name or comments with the exact same wording.[63]

For Apple with regard to potentially privacy-endangering apps on their AppStore, this can mean expanding their review process to check for SDKs by companies that already have a reputation for neglecting GDPR provisions. Similarly, entire sectors could be examined more closely and repeatedly even after admission to the AppStore once certain cases have become public.

For our purposes, the case of *InMobi* could have been such a precedent that could have led Apple to increased cautionary measures regarding the technical possibilities of data access that the iOS architecture affords AccuWeather and therefore Reveal Mobile.

(c) Third level: Assessment of solutions

In the following section, we perform a formal verification based on *CAPVerDE*. To demonstrate how the tool works, we retrace what the software does step by step. This level corresponds to the second half of the measures phase and the report phase as introduced by the ULD[64] as well as the second half of the risks phase and the validation phase as described by the CNIL.[65]

We limit this verification to the two technical measures described above because they are the ones that lend themselves most naturally to an implementation at this stage in the tool's development.[66]

To evaluate how the measures described change the impact of the system, we first assess the impact value of the described original architecture. This can be done automatically by CAPVerDE if we provide the architecture described in Section III and the necessary additional input. We use the default definition of ω with $\omega(location) = 4$. We define the components iOS (*SP*) representing the actor Apple and the component AccuWeather (*AP*) as the set of relevant components for this assessment.

First CAPVerDE evaluates whether there is a privacy breach in the architecture by verifying the property $consentViolated_i(location)$ for the set of relevant components. $consentViolated_{SP}(location)$ and $consentViolated_{AP}(location)$ are the two properties to verify. CAPVerDE uses pattern matching and backtracking for the verification based on inference rules. This means that the set of all relations is matched against the rules, for example, as only component C_i is fixed in the beginning, components C_j and C_k are matched against all potential components of the system. If there is a match in components, CAPVerDE also tries to match the remaining variables of the rule and potentially must backtrack when there is no possible match with the current configuration. For this type of property only rule ***C***, described above, is applicable. For the actor Apple, *CAPVerDE* matches the component C_i with *SP* and therefore looks for receive relations in the form $Receive_{j,SP}(E)$ in the architecture *A*. Only $Receive_{AP,SP}(\{wifi\_info\})$ matches this pattern. As *location* is the only existing data type in the architecture and the *CAPVerDE* pattern matches $E = \{wifi\_info\}$ the intersection

location∩*{wifi_info}* = *{wifi_info}* can be computed and is not an empty set. The first part of the conjunction thus holds. For the second part, *CAPVerDE* looks for a revoke relation of the form $Revoke_{SP,k}(location)$ in the architecture and matches the existing relation $Revoke_{SP,US}(location)$. As the first part of the disjunction holds, the second part does not have to be evaluated. *CAPVerDE* concludes that architecture *A* satisfies property $consentViolated_{SP}(location)$. Again, this is a negative property and indicates a violation.

Now *CAPVerDE* needs a likelihood estimate for the scenario where the iOS platform shares location data with an app against the user's explicit consent. As described above, this likelihood ranges from negligible (1) over limited (2) and comprehensive (3) to maximum (4). Based on an approach that connects the probability of a risk with the strength of mitigation actions,[67] we would rate the likelihood of an app using this (public and official) channel to access location-related data as maximum. *CAPVerDE* then simply multiplies the 4 from the likelihood input with the 4 of the impact category to get a risk level of 16, which is a high risk.

Denying access to BSSID data

The evaluation of the risk of the first measure in *CAPVerDE*, again starts with a check on whether a consent was violated: $consentViolated_{SP}(location)$ and $consentViolated_{AP}(location)$ are still the two properties to verify. However, because of the changed architecture, the result may differ. In fact, *CAPVerDE* cannot pattern match a receive event of the form $Receive_{j,i}(S,E)$. In this architecture location-related data is only transmitted via conditional receive relations. Therefore, the properties do not hold; as a consequence, *CAPVerDE* does not detect a data leak. Due to the possibility of side channel attacks or other unforeseen events, the minimal likelihood level is still 1, therefore yielding a risk level of 4, which is a medium risk and an improvement over the original system with a risk level of 16.

Controlled access to BSSID Data

The risk assessment of the second measure in *CAPVerDE* follows the same procedure as before. We now have two different data types to consider. Because the *network* type can be used to derive data of type *location*, it shares the maximum impact level of 4. Now CAPVerDE needs to check four properties, one for each data type and each relevant component: $consentViolated_{SP}(location)$, $consentViolated_{AP}(location)$, $consentViolated_{SP}(network)$, and $consentViolated_{AP}(network)$. As all relationships for transmitting data in the architecture are conditional receives, *CAPVerDE* does not detect a data leak in this system. However, since the permissions regarding data of the type *network* not granted by the users but by Apple at the time admission to the AppStore, we can only assume that a weather app would not receive the permission because it doesn't need it to fulfil its primary purpose. Therefore, we evaluate the likelihood of Reveal Mobile accessing *wifi_info* without the consent of the user as limited and *CAPVerDE* computes an overall risk level of 8, which is medium – albeit higher compared to the first measure.

C. Interim Conclusion

In conclusion, several possible measures could have been tangible, with some being more realistic than others. A model assessment supported by *CAPVerDE* shows that of the two technical solutions regarding direct access to BSSID data, both would have mitigated the risk significantly. While the complete denial of access would have promised the greatest level of mitigation, it would have also led (as history proved) to unwanted collateral damages.

V. Discussion

As we have shown above, *CAPVerDE* as a tool is already capable of modelling and verifying some, predominantly technical, types of privacy-preserving measures. The inclusion of other measures is in the focus of its further development. By building on existing risk and impact scales the tool can demonstrate to both controllers and DPAs the architecture behind a specific kind of high-risk processing act and visualise the 'before-and-after risk' level in relation to the controller's envisioned mitigation actions.

A crucial part of the formal verification is the input. The act of modelling the architecture is already a big step, both in terms of work and benefit. In the case presented we considered Apple as an actor that already has the capability (and even the self-imposed obligation) to perform the necessary analysis to construct such a data-flow model. Static code analysis can partially build a similar software architecture automatically. However, there are, of course, limitations. Constructing proof of the absence of something is very hard and virtually impossible for general cases. Verifying that no violations exist is, thus, considerably more complex than verifying that a certain type of violation does exist. Another problem is side channels. These are, by definition, unintended for use and difficult to detect in a data-flow model. Proving the general absence of side channels is, again, virtually impossible. One way to address the issue of side channels is the restriction of the software languages in privacy-critical systems. Similar approaches exist in safety-critical areas including the aircraft industry. The reason for this measure is the close relation of side channels and software (as well as hardware) implementation, as side channels are usually a problem that does not exist in the specification but is introduced in the implementation of specifications stage. However, some programing languages are known to be less susceptible to side-channel attacks (eg this can be due to built-in code analysis). Another limitation of the approach lies in the model checking itself. As the verification is built on the model, the quality (and honesty) of the model is an obvious limiting factor. However, we would argue that honesty and trust are an essential part of a DPIA.

Apart from these general considerations, the chapter's focus on the AccuWeather case and the connected risks and measures helps illustrate *CAPVerDE*'s potential benefits for the understanding and concretisation of the GDPR's provisions. By applying the ECJ's ruling on joint controllership from the case of *Wirtschaftsakademie* to the constellation of actors present here, we show that even in cases where the exact distribution and scope of risk-

mitigating obligations is not clear to the affected parties, an assessment of realistic measures and their efficacy is possible. The modelling and graphical depiction of both architecture and risk mitigation can help DPAs better stake out and understand what the current 'state of the art' allows with regard to certain technologies and acts of processing. Generally speaking, this has the potential to enhance one of the DPIA's general functions on a broader societal level: allowing DPAs an overview over high-risk processing acts at an early stage to decide whether what is considered state of the art is good enough. Deeming the results of companies' DPIAs insufficient and asking them to come up with better measures (as Article 36(2) empowers them to) can have an innovation-enhancing effect by impelling companies to improve their measures. Making it easier for DPAs to assess current measures' efficacy might therefore strengthen this ability to indirectly raise the state of the art of risk-mitigating measures.

To the best of our knowledge, only a few automated DPIA assist tools exist.[68] Even fewer are freely accessible. Most follow the approach of templates that provide step-by-step guidance through the process. These can be very useful tools but lack the automation. We view the DPIA support of *CAPVerDE* as an approach that can be used as a technical verifier on top of a template guide.

The French *pia*[69] tool promises to 'demonstrate compliance to the GDPR'.[70] It is a free open-source application that provides guidance through the process of a DPIA and also offers a somewhat automated risk calculation. Compared to *pia*, *CAPVerDE* obviously lacks non-technical support. If, on the other hand, we focus on the automatic risk assessment part, *CAPVerDE* offers a more automated, formal risk evaluation. The graphical representation of data flow can provide a quick overview of a software system, whereas the textual approach of *pia* can be more detailed.

VI. Conclusion

In this chapter, we have provided a description of the AccuWeather case and its privacy implications and have carried out a short legal analysis including a classification of two so far unappreciated actors as controllers. We have then used *CAPVerDE*, a tool that is able to formally model and verify privacy properties, to contribute to two different causes: firstly, how a DPIA performed by the two controllers could have been useful in identifying the risks that ultimately occurred when location data were collected by a third party despite a lack of users' consent and in finding and assessing potential mitigation actions. Secondly, how a DPIA supported by a tool like *CAPVerDE* could make DPIAs more understandable and manageable for both controllers and the DPAs assessing the validity of their outcomes.

The real-world gain of a tool-supported risk assessment lies in the comparability of systems and proposed measures as well as the metrics. A controller like Apple who already has the infrastructure to perform the necessary analysis could even implement such a tool into their toolchain.

From a scientific point of view, this chapter describes a formal method and an

implemented software application for verifying privacy properties including the detection of consent-violating leakage of personal data.

The benefit in the legal realm can be seen on multiple levels and as a reflection of the real-world gains. Controllers able to assess for themselves and demonstrate their risk management in a clearer and more understandable way to DPAs increase the chances of being compliant. DPAs are able to gain a better overview of typical risks and the measures palpable at a given time by gaining an overview from all the results that different controllers provide in the context of consultation (Article 36). A more standardised and uniform format of such DPIAs could contribute to an easier comparability and therefore to a clearer bigger picture for DPAs which could, in turn, use the overview they gained to sharpen the definitions of abstract provisions like Article 24.

While there is an intense debate on requirements for valid consent and other instruments to protect the autonomy of the data subject, the elements of system data protection under the GDPR framework – such as impact assessments – tend to be neglected. Since those elements are the more forward-looking, we believe that they need to be elaborated upon. This chapter demonstrates one way to model a system and prove whether or not it has specific properties, pushing the state of the art of DPIAs in the process.

References

Antignac, Thibaud and Le Métayer, Daniel ‘Privacy Architectures: Reasoning About Data Minimisation and Integrity’ in *10th International Workshop on Security and Trust Management 8743* (2014).

Bäcker, Matthias ‘Article 13 – Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person’ in *DS-GVO BDSG Kommentar*, eds Jürgen Kühling and Benedikt Buchner, 2nd edn, CH Beck, 2018.

Bavendiek, Kai, Adams, Robin and Schupp, Sibylle. ‘Privacy-Preserving Architectures with Probabilistic Guaranties’in *16th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2018.

Buchner, Benedikt, Kühling, Jürgen. ‘Article 7 – Bedingungen für die Einwilligung’ in *DS-GVO BDSG Kommentar*, eds Jürgen Kühling and Benedikt Buchner, 2nd edn, CH Beck, 2018.

Ernst, Stefan. ‘Article 4 – Begriffsbestimmungen’ in *Beck’sche Kompakt-Kommentare Datenschutz-Grundverordnung – Bundesdatenschutzgesetz*, eds Boris Paal and Daniel Pauly, 2nd edn, CH Beck, 2018.

Hansen, Marit. ‘Datenschutz-Folgenabschätzung – gerüstet für Datenschutzfürsorge?’ (2016) 9 *Datenschutz und Datensicherheit* 587–591.

Karg, Moritz. ‘DSGVO Art 4 Nr 1 – Begriffsbestimmung, Personenbezogenes Datum’ in *Datenschutzrecht DSGVO mit BDSG*, eds Spiros Simitis, Gerrit Hornung, and Indra Spiecker gen. Döhmann. Baden-Baden: Nomos Verlagsgesellschaft, 2018.

Kramer, Rudi. ‘Artikel 35 – Datenschutz-Folgenabschätzung’ in *Kommentar Datenschutz-Grundverordnung*, eds Gierschmann, Sibylle, Katharina Schlender, Rainer Stentzel, and Winfried Veil. Bundesanzeiger Verlag, 2018.

Kurtz, Christian, et al ‘The Unlikely Siblings in the GDPR Family: A Techno-Legal Analysis of Major Platforms in the Diffusion of Personal Data in Service Ecosystems’ in *Proceedings of the 52nd Hawaii International Conference on System Sciences 2019*.

Martini, Mario. ‘Article 35 – Datenschutz-Folgenabschätzung’ in *Beck’sche Kompakt-Kommentare Datenschutz-Grundverordnung – Bundesdatenschutzgesetz* eds Boris Paal and Daniel Pauly, 2nd edn, CH Beck, 2018.

Paal, Boris. ‘Article 36 – Vorherige Konsultation’ in *Beck’sche Kompakt-Kommentare Datenschutz-Grundverordnung – Bundesdatenschutzgesetz*, eds Boris Paal and Daniel Pauly, 2nd edn, CH Beck, 2018.

Schwendemann, Sabine. ‘Article 35 – Datenschutz-Folgenabschätzung’ in *Europäische Datenschutzgrundverordnung – Handkommentar*, ed Gernot Sydow, 2nd edn, CH Beck, 2018.

Shakila-Bu-Pasha, Alén-Savikko, Annette, Mäkinen, Jenna Guinness, Robert and Korpisaari, Päivi ‘EU Law Perspectives

on Location Data Privacy in Smartphones and Informed Consent for Transparency' (2016) 3 *European Data Protection Law Review* 312–323.

Spindler, Gerald. '§7 – Allgemeine Grundsätze' in *Telemediengesetz mit Netzwerkdurchsetzungsgesetz. Kommentar*, eds Gerald Spindler, Peter Schmitz and Marc Liesching, 2nd edn, CH Beck, 2018.

---

[1] Hans-Bredow-Institut for Media Research.

[2] Hans-Bredow-Institut for Media Research.

[3] Hamburg University of Technology, Institute for Software Systems.

[4] Hamburg University of Technology, Institute for Software Systems.

[5] Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

[6] From here on, every Article not further designated is one of the GDPR.

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive).

[8] See eg 'AccuWeather App Shared Users' Location Data' (*BBC*, 24 August 2017). Available at: www.bbc.com/news/technology-41037081.

[9] ECJ Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU:C:2018:388.

[10] Angela Fritz, 'A Security Researcher Discovered AccuWeather App Tracked, Shared your Location – Even if You "Opt Out"' (*The Washington Post*, 24 August 2017). Available at:www.washingtonpost.com/news/capital-weather-gang/wp/2017/08/23/security-researcher-discovered-accuweather-app-tracks-and-shares-your-location-even-if-you-opt-out.

[11] 'A Deep Dive into Mobile App Location Privacy Following the InMobi Settlement' (*Federal Trade Commission*, 9 August 2016). Available at: www.ftc.gov/news-events/blogs/techftc/2016/08/deep-dive-mobile-app-location-privacy-following-inmobi-settlement.

[12] A software development kit (SDK) is generally a collection of software development tools for software developers. In this context we are talking about a third-party iOS app SDK, which can be included like a library and provides certain functionality (eg advertisement management).

[13] Or rather the approximated locations determined through initial non-location data, see below.

[14] Federal Trade Commission, 'InMobi' (2016).

[15] An application programming interface (API) is a set of classes and functions that can be used to access other software. In this context the API is a level of indirection to restrict the apps' access to the underlying system.

[16] See 'About Privacy and Location Services in iOS8 and Later' (*Apple*). Available at: www.support.apple.com/en-us/HT203033.

[17] A basic service set identifier (BSSID) is a unique identifier of a WiFi network on the hardware level.

[18] Fritz (n 10).

[19] See Brian Handly, 'How to Profit from Data on the Location of Mobile Shoppers' (*DigitalCommerce360*, 1 May 2017). Available at: www.digitalcommerce360.com/2017/05/01/profit-data-location-mobile-shoppers. See also 'The Location of Black Friday – Using Mobile Location Data and Beacons to Measure Retail Shopping Behavior' (*Reveal Mobile*). Available at: www.mmaglobal.com/files/casestudies/the_location_of_black_friday_-_revealmobile.pdf which shows how Reveal Mobile themselves describe the inferring of real-world implications based on the example of Black Friday retail shopping behaviour.

[20] The tendency towards a generally wider interpretation of the GDPR's scope concerning the term 'personal data' can be seen, for example, in recital 15 and its notion of an effective protection of data subjects throughout technological change. See also Moritz Karg, 'DSGVO Art. 4 Nr. 1 – Begriffsbestimmung "Personenbezogenes Datum, para 65.

[21] Stefan Ernst, 'Art. 4 – Begriffsbestimmungen' in *Beck'sche Kompakt-Kommentare Datenschutz-Grundverordnung* –

Bundesdatenschutzgesetz, eds Boris Paal and Daniel Pauly 2nd edn, (CH Beck, 2018) para 9.

[22] Cf. 'Opinion 1/2010 on the concepts of "controller" and "processor" (Opinion No 169)' (*Article 29 Working Party*, 16 February 2010). Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf, 11 f, 39.

[23] Publicly, both AccuWeather and Reveal Mobile stated that they never had the intention of using the data in question to reverse engineer users' locations. See 'AccuWeather and Reveal Mobile Joint Statement About iOS App' (*AccuWeather*, 22 August 2017). Available at: www.accuweather.com/en/press/69041756.

[24] ECJ Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU:C:2018:388.

[25] Ibid at para 36.

[26] ECJ Judgment of 10 July 2018, *Tietosuojavaltuutettu v Jehovan todistajat – uskonnollinen yhdyskunta*, C-25/17, EU:C:2018:551, para 69.

[27] 'AppStore Review Guidelines' (*Apple)* Available at: www.developer.apple.com/app-store/review/guidelines/; See also Marco Tabini, 'How Apple is Improving Mobile App Security' (*Macworld*, 2 September 2013). Available at: www.macworld.com/article/2047567/how-apple-is-improving-mobile-app-security.html.

[28] See Carlos Ribas, 'The AccuWeather/Reveal Situation is Really an iOS Privacy Problem' (*Medium*, 25 August 2017). Available at: www.medium.com/@carlosribas/the-accuweather-reveal-situation-is-really-an-ios-privacy-problem-78e85a6f8539, stressing Apple's importance in a similar way.

[29] See 'This is How We Protect Your Privacy' (*Apple*). Available at: www.apple.com/privacy/approach-to-privacy/ for how Apple itself highlights its special dedication to protect users' data better than its competitors. See also Chris Baranuik, 'Tim Cook Blasts "Weaponisation" of Personal Data and Praises GDPR' (*BBC*, 24 October 2018). Available at: www.bbc.com/news/technology-45963935; see '"We Never Move Off Our Values" Apple CEO Tim Cook Says' (*NPR*, 05 June 2018). Available at: www.npr.org/2018/06/05/617029569/we-never-move-off-of-our-values-apple-ceo-cook-says for how Apple CEO Tim Cook highlights the importance of users' privacy rights.

[30] For further elaboration on and a more in-depth justification of this classification, see Christian Kurtz et al 'The Unlikely Siblings in the GDPR Family: A Techno-Legal Analysis of Major Platforms in the Diffusion of Personal Data in Service Ecosystems' in *Proceedings of the 52nd Hawaii International Conference on System Sciences 2019*.

[31] In cases of joint controllership, no single controller needs to be involved at all stages of processing. See 'Opinion No. 169' (2010), 18.

[32] A comprehensive analysis of the lawfulness of processing would be outside of the focus and is not relevant for the aim of this chapter.

[33] 'Privacy Policy' (*AccuWeather*, Last modified 7 May 2019). Available at: www.accuweather.com/en/privacy.

[34] Ibid: 'When You use AccuWeather Sites, You Consent to the Terms and Conditions and the Practices Described in this Privacy Policy'.

[35] See Benedikt Buchner and Jürgen Kühling, 'Article 7 – Bedingungen für die Einwilligung' in *DS-GVO BDSG Kommentar*, eds Jürgen Kühling and Benedikt Buchner 2nd edn, (CH Beck, 2018), para 57.

[36] Recitals are non-binding provisions, designed as an aid for interpreting the material provisions of the GDPR.

[37] See n 33.

[38] The question of whether such a violation automatically leads to the unlawfulness of the processing act is disputed. See Matthias Bäcker, 'Article 13 – Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person' in *DS-GVO BDSG Kommentar*, eds Jürgen Kühling and Benedikt Buchner, 2nd edn, (CH Beck, 2018), para 63f.

[39] As described by Kai Bavendiek, Robin Adams and Sibylle Schupp, 'Privacy-Preserving Architectures with Probabilistic Guaranties' *16th Annual Conference on Privacy, Security and Trust* (PST). IEEE, 2018.

[40] The software and the source code is available at: www.tuhh.de/sts/research/data-protection-machine-learning/capverde.html.

[41] The original idea was proposed in Thibaud Antignac and Daniel Le Métayer, 'Privacy Architectures: Reasoning About Data Minimisation and Integrity' in *10th International Workshop on Security and Trust Management 8743* (2014).

[42] Ibid; Bavendiek, Adams and Schupp (n 39).

[43] Shakila-Bu-Pasha et al 'EU Law Perspectives on Location Data Privacy in Smartphones and Informed Consent for

Transparency' (2016) 3 *European Data Protection Law Review* 312, 315.

[44] This general impact scale is based on several existing models. See eg 'Das Standard-Datenschutzmodell' (*Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder*, V.1.1. – Erprobsfassung 25/26 April 2018). Available at: www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V1.1.pdf, 31 f; 'Consultation: GDPR DPIA guidance' (Information Commissioner's Office, 13 April 2018). Available at: www.ico.org.uk/media/about-the-ico/consultations/2258459/dpia-guidance-v08-post-comms-review-20180208.pdf, 34; 'Risk Assessment & Datenschutz-Folgenabschätzung' (*Bitkom*, 2017). Available at: www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/FirstSpirit-1496129138918170529-LF-Risk-Assessment-online.pdf; 'Hinweise zur DS-GVO, Nr. 18' (*Bayerisches Landesamt für Datenschutzaufsicht*, 21 March 2017). Available at: www.lda.bayern.de/media/baylda_ds-gvo_18_privacy_impact_assessment.pdf.

[45] For more details on the levels and an example, see 'Hinweise zur DS-GVO, Nr. 18' (Bayerisches Landesamt für Datenschutzaufsicht).

[46] Sabine Schwendemann, 'Article 35 – Datenschutz-Folgenabschätzung' in *Europäische Datenschutzgrundverordnung – Handkommentar*, ed Gernot Sydow, 2nd edn, (CH Beck, 2018), para 6.

[47] Boris Paal, 'Article 36 – Vorherige Konsultation' in *Beck'sche Kompakt-Kommentare Datenschutz-Grundverordnung – Bundesdatenschutzgesetz*, eds Boris Paal and Daniel Pauly 2nd edn, (CH Beck, 2018) para 5.

[48] Rudi Kramer, 'Artikel 35 – Datenschutz-Folgenabschätzung' in *Kommentar Datenschutz-Grundverordnung*, eds Sibylle Gierschmann, Katharina Schlender, Rainer Stentzel and Winfried Veil (Bundesanzeiger Verlag, 2018), para 7.

[49] See, eg 'Liste von Verarbeitungsvorgängen nach Art 35 Abs. 4 DS-GVO für die gemäß Art 35 Abs. 1 DS-GVO eine Datenschutz-Folgenabschätzung von Verantwortlichen durchzuführen ist' (*Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*, 25 May 2018). Available at: www.datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20180525_LfD-SH_DSFA_Muss-Liste_V1.0.pdf as one amongst many. For a full list of blacklists by German DPAs, see Bernd Schütze, 'Aufsichtsbehörden veröffentlichten Positivlisten zur Datenschutz-Folgenabschätzung' (*Berufsverband der Datenschutzbeauftragten Deutschlands*, 30 May 2018). Available at: www.bvdnet.de/aufsichtsbehoerden-veroeffentlichten-positivlisten-zur-datenschutz-folgenabschaetzung.

[50] Now replaced by the European Data Protection Board (EDPB), which nonetheless endorsed all existing guidelines and opinions; see 'Endorsement of GDPR WP29 guidelines by the EDPB' (European Data Protection Board, 28 May 2018). Available at: www.edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_de.

[51] 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679' (Article 29 Working Party, 13 October 2017). Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236, 8.

[52] See Marit Hansen 'Datenschutz-Folgenabschätzung – gerüstet für Datenschutzfürsorge?' (2016) 9 *Datenschutz und Datensicherheit* 587, 563f.

[53] See 'Privacy Impact Assessment (PIA) – Methodology' (*Commission Nationale Informatique & Libertés*, February 2018 edition). Available at: www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf, 3.

[54] Location data in the broadest sense, including data that could be used to approximate user location, see technical description in II A.

[55] See 'Privacy Impact Assessment (n 53) 34.

[56] Hansen (n 52) 590.

[57] See 'Privacy Impact Assessment' (n 53) 3.

[58] See Jeff Butts, 'Thanks to Misuse, Apps can't View MAC Addresses on iOS 11' (*MacObserver*, 22 September 2017). Available at: www.macobserver.com/news/product-news/apps-cant-view-mac-addresses-on-ios-11/.

[59] See Marcia Savage, 'Apple iOS 11 Cripples WLAN Troubleshooting Apps' (*NETWORKComputing*, 24 October 2017). Available at: www.networkcomputing.com/networking/apple-ios11-cripples-wlan-troubleshooting-apps/715753461; 'MAC Addresses aren't available in the LAN scanner under iOS 11' (*Network Analyzer*). Available at: www.support.netanalyzer.techet.net/article/119-mac-addresses-arent-available-under-ios-11.

[60] See 'MAC Addresses' (*Network Analyzer*).

[61] For how Apple reviews apps, see Tabini (n 27).

[62] See Gerald Spindler, '§7 – Allgemeine Grundsätze' in *Telemediengesetz mit Netzwerkdurchsetzungsgesetz.*

Kommentar, edited by Gerald Spindler, Peter Schmitz, and Marc Liesching. 2nd edn, (CH Beck, 2018) para 37f. for a general overview on the German implementation of the relevant provisions from the EU E-Commerce Directive.

63 Ibid at para 33f.

64 Hansen (n 52) 590.

65 'Privacy Impact Assessment' (n 53) 3.

66 The verification of a broader variety of measures will be the focus of the tool's further development.

67 'Risk Assessment and Datenschutz-Folgenabschätzung' (n 44) 31.

68 See 'TrustArc Assessment Manager' (*Trustarc*). Available at: www.trustarc.com/products/assessment-manager; 'PIA & DPIA Automation – Operationalize Your Privacy Program' (*Onetrust*). Available at: www.onetrust.com/products/assessment-automation; 'DPIA Tool' (*Vigilant*). Available at: www.vigilantsoftware.co.uk/topic/dpia.

69 See 'The Open Source PIA Software Helps to Carry Out Data Protection Impact Assessments' (*Commission Nationale Informatique & Libertés*, 12 December 2018). Available at: www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment with further links to portable and web versions of the tool.

70 Ibid.

7

In Search of Data Protection's Holy Grail

Applying Privacy by Design to Lifelogging Technologies[1]

LIANE COLONNA[2]

Abstract

Lifelogging technologies promise to deliver an array of applications that can revolutionise the way that healthcare is currently administered. While lifelogging technologies provide great opportunity to improve efficiency and care in the healthcare settings, the ubiquity and invisibility of lifelogging devices raise critical privacy concerns. One way to cope with the privacy challenges that arise from the use of lifelogging devices is to find technological means to guarantee the protection of personal data. However, because of the nascent nature of the industry, there is a lack of guidance as to how to build lifelogging devices in a way that anticipates data protection concerns.

This chapter seeks to explore the concept of Privacy by Design within the context of lifelogging. It uses the core data protection principles set forth in the GDPR to evaluate which aspects of lifelogging have potential for privacy breaches. It then makes suggestions about how the concept of Privacy by Design can be implemented in a way to alleviate those concerns, pointing to various transparency and embedded legal measures available in order to strengthen the data protection rights of individuals within the context of lifelogging.

Keywords

Privacy, data protection, lifelogging, internet of health, privacy by design.

I. Introduction

Lifelogging technologies promise to deliver an array of applications that can significantly improve the life quality and the support of older or impaired people, revolutionising the way that healthcare is currently administered.[3] Acquisition and processing of physiological signals, motion and location data, performed activities, images seen and sounds heard, are

already the basis for a number of cutting-edge tools.[4] These tools can be used to better manage conditions like stress, encourage exercise and healthy eating, diagnose medical conditions, support compliance with treatment regimes and assist formal and informal caregivers.[5] Furthermore, predictive lifelogging systems are being developed which can detect and anticipate falls,[6] mild cognitive impairment[7] and aggressive behaviour in older adults.[8]

While lifelogging technologies provide great opportunity to improve efficiency and care in the healthcare settings, the ubiquity and invisibility of lifelogging devices raise critical privacy concerns. When these devices are used, patterns of deeply personal behaviour can be detected and inferences can be made about an individual's lifestyle and health.[9] In turn, these data can be used and shared with others in unanticipated ways, possibly giving rise to privacy harms, depending on the context.[10]

One way to cope with the privacy challenges that arise from the use of lifelogging devices is to find technological means to guarantee the protection of personal data. However, because of the nascent nature of the industry, there is a lack of guidance about how to build lifelogging devices in a way that sufficiently spotlights and anticipates data protection concerns.[11] Tools are needed to help software developers design and implement privacy friendly lifelogging systems as well as clear guidelines on how to build legal requirements into the system.[12]

This chapter seeks to explore the concept of Privacy by Design within the context of lifelogging. Taking as a starting point that the conditions for data processing are fundamentally set by the soft-and hardware created by developers and producers of lifelogging technologies, the paper seeks to offer some legal guidance as to how these technologies can be created in a privacy aware manner. This chapter uses the core data protection principles set forth in the General Data Protection Regulation (GDPR) to evaluate which aspects of lifelogging have potential for privacy breaches. It then makes suggestions as to how the concept of Privacy by Design can be implemented in a way to alleviate those concerns, pointing to various transparency and embedded legal measures available to strengthen the data protection rights of individuals within the context of lifelogging.

II. The Concept of Privacy by Design

Privacy by Design represents a new generation of legal strategies in the Digital Age where traditional forms of law have become outmoded. Taking a proactive approach to law, Privacy by Design has a conscious orientation to the future insofar as it seeks to avoid privacy problems before they can occur.[13] Fundamentally, it involves the transformation of legal rules, namely those that appertain to privacy and data protection, into information systems.[14] Multiple parties are involved in its implementation such as engineers, managers, lawyers, end-users, policymakers, and executives within an organisation and each group is expected to share responsibility for achieving privacy goals.[15]

In 2010, in an oft-cited article, Cavoukian, announced that Privacy by Design is based on seven foundational principles: proactive not reactive; privacy as the default configuration; privacy embedded into the design; privacy as additional (not reduced) functionality; end-to-end data security; visibility/transparency; and respect for the privacy of the individual user.[16] Over the years, however, these principles have been subject to substantial criticism. For example, Schartum refers to them as 'slogans' rather than 'analytic lines of actions' and states, 'their values are quite limited as process description and recipe of how to attain privacy by design successes'.[17] Likewise, engineering scholars comment that there exists little to no guidance on what precisely Privacy by Design entails, claiming the concept lacks any detail about how to actually implement it in practice, especially while meeting the functional requirements of the system under development.[18]

Despite its analytical failings, Privacy by Design is being hailed as a critical new governance strategy for achieving privacy. For example, the GDPR makes Privacy by Design a core requirement and recognises that it is a vital tool for the protection of privacy.[19] That said, the law offers engineers little advice as how to implement the concept in practice other than to use techniques like data minimisation and pseudonymisation.[20]

III. Guidelines

While engineering perspectives have certainly been considered in this work, the complete translation of privacy principles into operational engineering requirements is outside the scope of this chapter. Instead, the goal here is to consider relevant privacy techniques, strategies and patterns that serve as potential responses to legal requirements.[21] In other words, the ambition is to try to close the gap, at least a little, between legal compliance and the dynamic innovation process driven by business managers and engineers who are ultimately responsible for the design of lifelogging technologies.[22]

Set out below is a review of some major data protection concerns raised by lifelogging technologies and some attendant guidelines as to how these concerns can be addressed at the outset of a system's development. These guidelines can be used as heuristics and provide a guiding framework for developers of lifelogging technologies when seeking to embed privacy into these tools. This chapter focuses on the technical aspects of the Privacy by Design concept, rather than the organisational.

A. Lawfulness, Fairness and Transparency: Consent

In the lifelogging context, there are a number of reasons why it can be difficult, if not impossible to obtain a data subject's unambiguous consent in advance of data processing. First, since lifelogging tools collect data about an individual in a 24/7, ambient manner, it is hard to convey the full implications of the data processing in advance as a necessary precondition to obtaining lawful consent: the potential uses of these huge data sets are

practically limitless and are difficult to predict and explain *ex ante*. This issue is exacerbated by the fact that small sensors, seamlessly integrated into the user's environment, are capturing the data: relaying the surveillance capabilities of these tiny, versatile objects in a way that individuals can fully understand their power presents substantial challenges.[23]

Second, even if users could fully understand the implications of the data collection and processing, the fact remains that there are major practical obstacles to obtaining fully informed consent.[24] In order to obtain informed consent, most models today take advantage of screens to display privacy policies and terms and condition contracts containing large blocks of text.[25] However, lifelogging tools are seamlessly entwined into the user's living space so the opportunity to have a privacy notice 'pop up' is greatly diminished.[26] The former Chairwoman at the FTC, Ramirez has asked, 'as the boundaries between the virtual and physical worlds disappear' how can lifelogging tools 'provide just-in-time notice and choice if there is no user interface at all?'[27] The unrelenting nature of the data collection is also an issue insofar as people cannot reasonably be constantly asked whether they consent to data gathering or whether they understand how their data will be used.[28]

The non-consensual logging of third parties or bystanders is another critical issue when it comes to using lifelogging technologies.[29] A sick or frail person utilising a lifelogging technology may encounter many different third parties throughout her day. These people can include family members, cohabitants, friends, colleagues, acquaintances, and individuals unknown to the lifelogger.[30] The privacy of these bystanders may be affected when a sensing device is used in their surroundings and, under the law, they should be provided with notice about the processing and a choice about whether they accept it. In many instances, however, lifelogging tools are capable of capturing the data of third parties without those individuals having any awareness that their data is being captured and without having provided valid consent.[31] The privacy concerns raised by non-consensual logging of third parties are manifold such as unwanted image, speech or location capture.[32]

It must be emphasised that, unlike in traditional methods where a third party might have some understanding that they are being photographed, the embedded and ubiquitous nature of lifelogging technologies create the possibility that a third party can be sensed without any idea that their data is being processed.[33] Corbet makes the point: 'The fact that many (lifelogging) devices are not immediately visible to the eye creates difficulties in terms of meeting the legal standards typically imposed in the context of other forms of data capture.'[34] In other words, the concern is that lifelogging can lead to the surreptitious capture of personal data of bystanders in violation of basic data protection rules that require data collection to be fair, lawful and transparent.

Finally, the challenges of obtaining the fully informed consent of an individual with diminished cognitive ability must be noted. While the GDPR only contains specific provisions on capacity to consent with respect to minors, the issues of capacity are intertwined in the concept of 'informed' consent. Informed consent means that the data subject must be made aware of how their information is being used and what risks are involved: if a data controller has reason to believe that an individual lacks the mental

capacity to understand the consequences of consenting then that individual cannot provide informed consent. Under this circumstance, a third party with the legal right to make decisions on their behalf, for example under a Power of Attorney, can give consent.

Batchelor et al have addressed the challenges of obtaining consent within the particular context of dementia. They emphasise that consent is not always a black-and-white issue, especially if an individual's cognitive ability is in slow decline: mental capacity to consent appears on a spectrum and it is often difficult to clearly pinpoint when a person can no longer lawfully consent to having their data processed.[35]

B. Recommendations

As an initial consideration, the functionality of a lifelog should be adjusted to the competence of the user to increase the transparency of data processing and to strengthen data privacy.[36] Jacquemard et al explain that: 'The information obtained from a lifelog can be fed back to the lifeloggers in various forms. It is important to deliver this information appropriately which is largely dependent on the motivation for creating this information and the target audience.'[37] Within the healthcare context where lifelogging technologies target vulnerable populations, the lifelogging system should be constructed with an age-appropriate information architecture. Here, privacy-friendly default configurations and settings, intelligible to this population should be considered.[38]

Embedded legal solutions can also be used to make consent more meaningful and granular. That is, rather than relying on a binary, one-time consent model, a flexible, graduated and progressive system of control could be developed to reflect the fact that lifelogging occurs in a dynamic environment.[39] This type of system could make consent more meaningful, appropriate to changing circumstances and preferences and minimise decision overload in the wearable computing environment.[40] Here, it is important to note that granularity should concern both the category of collected data as well as the time and frequency at which data are captured.[41] Crabtree et al further advise that lifelogging devices should notify users when they are active, possibly by broadcasting a signal on a wireless channel and offer a 'do not collect' option to quickly disable data collection.[42]

Because many lifelogging tools do not have screens or just have tiny screens, a new kind of consent model needs to be developed as current methods simply do not work without a user interface.[43] While the lack of a user interface creates a formidable challenge to increasing transparency within the context of lifelogging, there are nevertheless opportunities to make notice and consent more visceral.[44] This is because hearing or other senses may be more tightly integrated with the user, so it may be easier in some ways to get the user's immediate attention.[45] Here, rather than relying on traditional consent tools like the signing of a written agreement, other types of actions should be explored as possible affirmations of consent such as a gesture or motion.[46] That said, both the FTC and the Article 29 Working Party recommend affixing QR codes or similar barcodes on devices that, when scanned display the required disclosures, as at least a short-term solution to dealing with the consent

issue.[47]

Traceability techniques, which are able to capture an issuance of consent and trace it back to the date and time when the data subject agreed should further be considered.[48] Having full traceability of all personal data in a lifelogging system is critical, if, for example, a data subject requests to withdraw her consent. Likewise, non-repudiation services through, for example, the use of a digital signature or biometrics, can be applied to ensure that an individual who has lawfully provided her consent cannot deny it.[49] These types of techniques are especially important where the data involved are sensitive and therefore explicit consent must be provable under non-repudiation.[50]

When it comes to protecting the privacy of third parties, there are a number of different computer vision techniques that can be applied to hide a bystander's identity to protect her identification where consent has not been provided.[51] These methods can broadly be divided into two groups: those that prevent the capture of images in the first place and those that remove sensitive or private information ex ante.[52] With respect to the first group, for example, intervention methods can 'prevent the acquisition of an image by means of a specialised device that interferes with the camera optical lens'.[53]

After data has been captured, image and video modification or redaction methods can be used to modify the sensitive regions of an image to conceal private information about the data subject.[54] Here, image filters can obscure parts of the human body, encryption methods can be used to distort a video, facial features can be de-identified, and objects/people can be altogether removed. It is also possible to transform a human that appears in an image into a solid silhouette, a skeleton, a 3D avatar and even a cartoon.[55] An image can further be blurred, pixelated or embossed.[56] While these techniques are not infallible, and reidentification is possible, for example, through gait analysis, there are solutions for managing these issues being developed which should be further considered.[57]

When a bystander has been heard or sensed in a non-visual way, other privacy-enhancing techniques are available. In order to prevent the collection of speech or location data, for example, location-dependent methods can be applied.[58] According to Perez et al, these methods involve the denial of data collection in certain shared spaces and usually involve banning a device's use through its temporary disablement in a shared space.[59] They explain that there are three general approaches to disabling lifelogging devices in shared spaces: sensor saturation, broadcasting commands and context-based approaches.[60]

Finally, it is important to think about ways to afford bystanders with an opportunity to protect their own personal data rather than trusting the lifelogging device or its user to ensure the respect of their private life. Here, notification methods that alert bystanders to protect their privacy should be considered.[61] For example, LEDs[62] can be used on some lifelogging devices to notify bystanders that their image or speech is being recorded.[63] Short-range radio broadcasts and Wifi-based communication protocols that notify bystanders about activity being performed in their proximity are additional solutions.[64]

Ensuring that lifelogging technologies support individual consent management is another bystander-focused solution. For example, MyData is a digital service that focuses on

managing and visualising data use authorisations.[65] Lifelogging technologies could facilitate the use of consent management tools by, for example, building Application Programming Interfaces (APIs) which enable their services to be to be connected to such consent management tools.[66]

C. Purpose Limitation

It is critical that a data subject understands the purpose of the processing of her data, including any planned sharing, selling, disclosing, or its further processing. At the same time, however, lifelogging technologies involve complex data flows that often escape the common tools used to identify and manage more traditional data flows. Not only do these devices collect highly sensitive information about an individual's body and health but they also collect incidental and behavioural data such as location, patterns and related metadata that can be combined and re-combined to discover 'new' data.[67] Here, it must be emphasised that sensors are able to collect data that is high in quantity and sensitivity, permitting even larger and more sensitive inferences to be drawn than with previous technologies.[68]

A central data protection concern that arises is inferences about the individual will be extrapolated from the data processing which they may have no idea about whatsoever. For example, inferences could include data points such as a user is pregnant or is suffering from a life-threatening disease. The individual may be completely unaware of this data and thus not be in a position to contest its accuracy, control its flow or challenge its use by others.[69] In other words, even if a data subject consents to the processing of the seemingly innocuous data collected by her lifelogging device, she may not consent to the use and sharing of the inferences that can be derived from these data, especially with people outside of her circle of care.

It is further important to mention that the inferences and conclusions that can be made by utilising a particular lifelogging technology can have both beneficial and harmful uses, depending on the particular purpose for which they are used.[70] For example, data collected from a lifelogging device may give rise to a conclusion that a woman is suffering from a chronic disease. Of course, the woman would like to be aware of this information so that she can get appropriate care but, at the same time, she would likely object to sharing this information with her employer or her insurance company. In short, controlling the use of derived lifelogging data, possibly for good, possibly for ill, is highly situational and context dependent.

D. Recommendations

In order to ensure that specified purpose(s) of data processing set forth in a privacy policy and communicated to a data subject are in fact being abided by, a Purpose-based Access Control System can be utilised. These types of systems 'evaluate access requests based on the purpose of the access, and they allow conditional or unconditional access only for

specific proposes predefined in privacy policies'.[71] Bertino explains that privacy-related metadata represents the core of access control mechanisms and without comprehensive and accurate privacy-related metadata, such as data usage purposes, these systems cannot be developed.[72]

A related approach is based on the concept of machine-readable privacy policies or sticky policies, which are mechanisms to facilitate a data subject's understanding of complex legal issues and to enable a more scalable management of an individual's privacy preferences.[73] Sticky policies are defined as machine-readable policies that 'can stick to data to define allowed usage and obligations as it travels across multiple parties, enabling users to improve control over their personal information'.[74] In 2016, exiting FTC Commissioner Julie Brill stated: 'Forty percent of information flowing with respect to the Internet of Things is machine-to-machine communication, not machine-to-human. We need to engage that communication by having privacy policies that are machine-readable.'[75] Likewise, Schwartz states, 'Machine-readable policies … hold considerable promise and deserve attention.'[76]

Metoui and Bezzi emphasise that sticky policies can be used to improve control over the usage of personal data and to define usage constraints and obligations when data moves from one party to another.[77] A sticky policy can, for example, indicate the acceptable purposes on the processing of an individual's personal data, the allowed recipients, deletion periods, and so on.[78] In short, sticky policies allow privacy preferences to flow with an individual's personal data to make sure that they are always enforced.[79]

While the idea to harness the power of information technology to create a means for transparency and user choice 'is a good one', it must be noted that there is already a Web standard to do precisely the same thing and it has not been very successful.[80] In 2002, the Platform for Privacy Preferences (P3P) standard was issued by the World Wide Web Consortium (W3C), the main standard setting body for the Web.[81] P3P was designed to permit users and websites to match privacy policies through machine-readable code.[82] There are a number of different reasons why P3P failed, but probably its biggest problem was that it was both too complex and too limited.[83] Hintze explains: 'One need only browse the P3P 1.0 specification to see the enormous number of elements and variations within those elements and get a sense of the complexity.'[84] Hintze suggest that the machine-readable privacy policies of the future and other metadata tools should be narrowly targeted to specific aspects of privacy practices and context specific.[85] Schwartz suggests building on and learning from the work completed by P3P.[86]

Privacy proxies, sometimes referred to as privacy brokers,[87] are another technical mechanism that can be used to give effect to a data subject's privacy preferences and to prevent the unwanted use of her personal data. Privacy proxies are in charge of handling 'privacy relevant interactions' such as policy access and data collection between the data subject and the data collector(s).[88] These services are continuously running and, as such, a data subject can contact them at any time and obtain instant access to her data.[89] Lioudakis explains that the central idea behind privacy proxies 'is the integration of all privacy-critical functionality into a privacy-proof middleware proxy entity … assigned with the mission of

enforcing the privacy legislation principles, on the basis of which it is conceived'.[90] To put it differently, privacy proxies represent some sort of middleware to negotiate the privacy wishes of the data subject and to protect her personal data.

Protecting data in the databases from unauthorised disclosure and use can also be achieved through the use of specially designed databases called Hippocratic Databases (HDB). HDB is a sophisticated concept of databases introduced in by Agrawal et al in 2002 designed to protect the privacy of the individual whose personal data are contained in them.[91] In their work, Agrawal et al proposed that current systems should be redesigned to enable the data system to automatically manage sensitive and personal information without hampering information flow.[92] Bhatia and Singh explain: 'HDBs can be extended as privacy preserving access control systems for minimum disclosures of privacy-related information.'[93] Essentially, the idea behind these databases is to provide granular and selective access to data based on their privacy and sensitivity.[94]

Pseudonymisation is another relevant technique, particularly when seeking to repurpose data. It can be defined as 'a security measure that is used to reduce the linkability of data to its data subjects by separating the data from direct identifiers, but does not prevent re-identification'.[95] In other words, pseudonymised data, has personally identifying information removed but can still be linked to auxiliary information to re-identify data subjects.[96] Pseudonymisation explicitly satisfies the 'data protection by design and by default' requirement introduced in the GDPR.[97] Another benefit is that if the technique is used, then a data controller may be able to repurpose the data, as long as the repurposing is for another compatible use.[98]

Finally, privacy-preserving data mining is emerging as an important tool to maximise the benefits of large collections of data while, at the same time, minimising the privacy impacts. PPDM is an umbrella term that refers to a number of different methods that seek to retrieve valid data mining results without learning the underlying data values.[99] PPDM seeks to protect sensitive raw data such as a name or id number as well as protect the sensitive knowledge through the dynamic processing of the dataset.[100] Oliveira and Za explain: 'PPDM encompasses the dual goal of meeting privacy requirements and providing valid data mining results.'[101] For example, differential privacy techniques allow users to ask questions of very large collections of sensitive, personal data while preserving individual privacy through the introduction of 'noise' into the response.[102] That is, the response is 'blurred' so that virtually nothing about any individual's data is revealed.[103]

E. Data Minimisation

Reconciling the data minimisation principle with technologies like lifelogging is challenging because, within the context of lifelogging, there is a temptation to process more personal data than is absolutely required and to store these data indefinitely. This is in order to obtain the best possible benefit from the development of the technology, which is often unpredictable and likely to grow exponentially with time. As noted by Corbet: 'Innovators will point to the

fact that in the connected health space, for example, medical knowledge and predictors of ill-health are at a very early stage, and so minimising (sic) data capture (eg running shoes that record exercise patterns for fitness purposes) may serve to prevent IoT users from availing of breakthrough technologies (eg early predictors of Parkinson's disease).'[104] In other words, while excessive collection and storage of personal data can certainly lead to privacy and security breaches, it may also have potential benefits for both the user and society alike.[105]

It is important to mention that, unlike earlier technologies, it is much more complicated to build a 'stop recording' functionality into a lifelogging device which, by its nature, is ambient and supposed to be turned on 24/7. Part of the problem, as noted above, is that many lifelogging technologies lack a user interface. The challenge is likely to become even bigger once these technologies become more embedded into the fabric of everyday life as well as into the human body itself.[106]

The fact that lifelogging tools collect data in an ambient and indefinite manner gives rise to privacy concerns about memory augmentation.[107] Clinch et al explain: 'Preserving a moment may offer benefits for recall of positive moments or useful information, but also allows the embarrassing and confidential to persist …'[108] Likewise, Allen describes lifelogs as a kind of 'memory machine'.[109] She explains: 'Ancillaries to memory, lifelogs will enable unprecedented accurate retention and recall of personal life. By design, lifelogs could be substantially less selective and less fallible than human memories stored only in the brain.'[110] Essentially, the concern is that while preserving a moment, a week or even a year of an individual's life might offer benefits, especially for someone with dementia, these records also allow the embarrassing and confidential moments of that person's life to live on in perpetuity.[111] Here, the tension between the need to store data to maximise the benefits of lifelogging tools, particularly in the health care context, and the need to delete those data in the interest of limiting memory capture must be balanced through the use of technical solutions.

F. Recommendations

There are a number of technological solutions to help lifeloggers comply with the data minimisation principle. First, as noted above, there are many different ways to protect and preserve the privacy of individuals appearing in videos by reducing the collection of data to the least amount necessary. For example, computer vision techniques can be used to recognise certain areas, mark them as private and prevent the capture of data connected to them.[112]

Second, data distribution should be limited where possible. Here, lifelogging devices should 'limit the amount of data leaving devices by transforming raw data into aggregated data and deleting raw data as soon as the data required for processing has been extracted'.[113] Crabtree further explains that 'as a principle, deletion should take place at the nearest point of data collection of raw data and where possible directly on the device'.[114]

Data anonymisation is another important technique that can be applied to comply with

the data minimisation principle within the context of lifelogging. Broadly, anonymisation 'is a process by which information in a database is manipulated to make it difficult to identify data subjects'.[115] Recital 26 of the GDPR defines anonymised data as 'data rendered anonymous in such a way that the data subject is not or no longer identifiable'.[116] If data is rendered anonymous then it falls outside the scope of the GDPR.

Lifelogging systems should automatically anonymise personal information before storing these data so that the people whom the data describe remain anonymous. These techniques can be used on all different types of personal data collected by a lifelogging technology such as data about an individual's appearance (video), health status (physiological signals), communications (audio) and behaviour.[117] There are a number of different anonymisation techniques such as randomisation and generalisation, noise addition, permutation, differential privacy, aggregation, k-anonymity, l-diversity, and t-closeness.[118] Each of these techniques has its own strengths and weaknesses.[119] None can guarantee anonymity and, in numerous studies, researchers have demonstrated how these privacy measures can be breached in practice, particularly in applications involving large data sets.[120] That said, the GDPR explicitly recognises the privacy-enhancing effects of both anonymisation and pseudonymisation.

Even if a data controller utilises encryption techniques, metadata still remains an issue. This is because metadata of encrypted content can reveal a significant amount of personal and sensitive information that may not necessarily originate from the content itself but from its properties.[121] As such, stripping unused metadata should be considered as a Privacy by Design solution towards meeting the data minimisation principle within the context of lifelogging. This process can either involve manual intervention from data controllers or it can be automated.[122]

Finally, it must be noted that, in some ways, requiring anonymisation is completely at odds with the purposes of lifelogging: the value of lifelogging lies in the analysis of personal data and anonymisation may limit the benefits of the data or even completely ruin the total value of the data set. For example, if a lifelogging technology stores images to permit an individual with mild dementia to recall events or persons, de-identifying those persons will have a negative effect on the service provided.[123] Here, it is important that a privacy-by-context approach is taken with respect to the specific device and application.

G. Storage Limitation

The very idea of storage limitation is anathema to lifelogging. In many ways, lifelogging is a technology that seeks to create a perpetual record of an individual's life, drawing insights from seemingly unrelated pieces of data collected and stored about the individual indefinitely. Unlimited storage presents huge opportunities to recall and draw insight about an individual's life. In short, the long-term storage of lifelogging data can provide a clear and perhaps even indelible picture of an individual's life and health, and how to improve it.

Another issue concerns the current distributed and redundant model of data storage today.

Because of the nature of this model, it is not clear that even small data sets can be destroyed with any high degree of assurance, let alone the kinds of big datasets involved in lifelogging technologies.[124] Even leaving aside the issues of 'zombie' cloud data,[125] the fact remains that personal data from a lifelog can be shared with a third party who can make a 'rogue' copy of the data that can be stored indefinitely.

H. Recommendations

Data management tools that facilitate the traceability of the flow of personal data from its original source to various destinations are crucial to managing the legal requirements surrounding data storage.[126] Data traceability has two components: tracking and tracing.[127] Gjermundrød et al explain that tracking is the capability to record the path of data as it gets shared and '(t)racing is the capability to identify the origin of data'.[128] When it comes to complying with data protection laws, it is critical to understand all of the locations where personal data exist such as in backups or other distributed copies, where the data are often overlooked.[129]

Developers of lifelogging technologies should consider using 'edge' or 'fog' design patterns in their infrastructure architectures to help compliance with the data storage principle as well as to enforce other privacy rules through technical means and in this way, increase their overall accountability as data controllers.[130] Quite simply, the fog is a place where data gathered from sensors can be processed and stored.[131] It embeds computing power throughout a network instead of in a cloud or at a remote data centre.[132] Instead of relying on powerful servers, it relies on weaker but more dispersed computers.[133] This decentralised architecture, with local data storage and processing, helps to prevent some of the security concerns associated with cloud storage.[134] It also helps to restrict access and enables greater control over personal data.[135] Makker explains: 'Fog computing enables system developers to enforce privacy controls at the point of collection (at the device itself) and thus opens up the opportunity to implement IoT privacy management systems guided by the principle of data minimization.'[136]

Finally, it is important to mention that the European Network of Information Security Agency (ENISA) provides guidance on data storage in its report on 'Risks and Benefits of Emerging Life-Logging Applications'. Here, it recommends that the lifelogging industry and service providers should adhere to a model of data storage that allows users to store and process their data on their own equipment, with strict access controls.[137] Recognising the limited storage and processing capabilities of many lifelogging devices, ENISA further suggests that such a model provide for interoperable services by separate companies rather than integrated large-scale data processors.[138]

I. Integrity and Confidentiality

Lifelogging tools without proper security and authentication systems are vulnerable to

attack.[139] Attacks can put an individual's personal information and reputation at risk as well as threaten her health and well-being.[140] Deep intrusions into a person's private life could occur if, for example, plain text stating, 'Sally Smith just reminded herself to take her HIV medication' was intercepted.[141] Likewise, if a lifelogging device charged with regulating insulin was hacked, then that could have dire consequences for the device owner, who may suffer dangerously low or high glucose levels as the result of incorrect insulin administration.[142]

While different lifelogging technologies have different security needs, in general, there are three main risk areas for the data collected by a lifelogging technology: on the device (storage), in transit (transmission) and in the fog/cloud (storage).[143] Data stored on the device is at risk from such things as malware.[144] During transmission, data is at risk from an array of possible threats such as traffic sniffing.[145] Once data arrives at the cloud destination, it is exposed to numerous risks such as SQL injection attacks and backdoor attacks, depending on the configuration of the system.[146] In short, lifelogging technologies must ensure the software is secure, transmissions of data are secure and servers are secure.

Regarding security, it is important to note that many lifelogging technologies have limited processing power, memory and local storage facilities: these attributes make it harder to ensure the security of the device.[147] Shrestha and Saxena explain: 'Wearable devices generally store data locally without encryption, PIN protection, or user authentication.'[148] Furthermore, since a user interface is often lacking, authentication becomes a challenge: a user of a lifelogging system might not be able to type a password on a keyboard.[149] If a lifelogging technology is used outside a controlled wireless network, then more security problems can arise.[150] Unfortunately, the lack of processing power of some lifelogging technologies, particularly small wearables, limits their ability to rely on encryption techniques to reduce these concerns.[151]

It has been proven that even popular and widely marketed wearable devices contain inadequate security protections.[152] Rahman et al examined the security protocols of the Fitbit and demonstrated that it is vulnerable to a diverse set of attacks. For example, they showed that the tracker transmitted user credentials in plain text and demonstrated that fabricated data could be generated and injected into the tracker by attaching it to moving objects like a fan.[153]

J. Recommendations

Proper access control and permissions on the data is critical to ensuring the integrity and confidentiality of data stored on a lifelogging device. Broadly, access controls involve 'the defining or restricting of the rights of individuals or application programs to obtain data from, or place data into, a storage unit'.[154] Rao and Nayak explain: 'The goal of an access control is to protect information from being lost, stolen, deleted, or modified either intentionally or accidently by those who are not authorized to access it.'[155] Depending on the

environment, there are a number of different ways that access controls can be implemented such as through the use of login and passwords or digital signatures.[156]

Access control has two main components, which include authentication and authorisation.[157] Authentication concerns the verification of 'the identity of a user or a host that is accessing the system or network resource'.[158] The creation of biometric authentication solutions for lifelogging technologies is a novel way to facilitate compliance with the integrity and confidentiality principle. Biometric authentication methodologies rely on intrinsic physical and behavioural traits rather than things like username/passwords or access card/PINs.[159] Currently, researchers are examining ways to authenticate users based on their thought.[160] Here, users set a pattern of brain waves, such as a combination of eye blink, attention and various brain rhythms like Alpha, Beta, Theta and Delta to get access to the device.[161] Likewise, researchers are examining how to authenticate a user based on their unique pattern of blood flow rhythm.[162]

Gesture-based authentication schemes are another way to sidestep the lack of a user interface.[163] Researchers have also developed an authentication scheme based on the use of a bioelectrical impedance signal.[164] Authenticating lifelogging technologies using body and gait recognition is a further possibility.[165] Because there are a multitude of different lifelogging devices and applications, there is no 'one-size-fits all' solution to the problem of continuous authentication of users on devices without conventional interfaces.[166]

Authorisation concerns permitting or restricting access to information based on the type of users and their roles.[167] Authorisations can be stored into lifelogging systems and then used to verify whether an access request can be authorised.[168] Here, access rights management systems should be implemented in the lifelogging context to mitigate the risk of data disclosure to unauthorised persons.

Within the lifelogging context, it is important that authorisation techniques 'express policies in terms of attributes of principals, resources, and contexts instead of specific identifiers or roles'.[169] This is because the point of authorisation is to provide the basis for making a decision, usually about whether to share information or device access.[170] Shahzad and Singh provide an example to support the idea that authorisation techniques should be context-aware.[171] They explain that in a situation where an individual is using various health-monitoring lifelogging devices and these devices reveal that that person is having a serious medical problem, such as a heart attack, then it might be appropriate to reveal data from her lifelogging device to anyone who is present nearby and might be willing and able to help.[172] On the other hand, they state, '… if the user is already in a hospital, then perhaps the application doesn't need to be quite so forthcoming in revealing its user's information to strangers'.[173]

Lifelogging technologies should have multiple layers of security.[174] A 'defense-in-depth' strategy helps to defend against security risks and ensures that information is accessible only by its intended recipients.[175] Having multiple layers of security means that 'even if security at one level gets compromised due to some reason, security at other levels should be able to

safeguard the underlying (lifelogging) infrastructure'.[176] The FTC recommends that developers imagine how a lifelogging device will be used and then identify potential risks and possible security soft spots.[177]

Furthermore, lifelogging technologies should use default settings that favour security.[178] Sometimes this is referred to as 'security by default' which essentially means that the settings of a device the most secure as possible, even if they are not the most user friendly.[179] One commentator explains, 'any security left to the self-determination of the end-user is likely to be a security gap, and nothing more'.[180]

Finally, end-to-end encryption should be implemented on lifelogging systems, particularly where sensitive data is being handled. By ensuring that all data from lifelogging sensors are encrypted so that it can only be read by authorised senders and receivers means that security breaches are minimised. As noted above, there are several complex algorithms available that can render sensitive information incomprehensible while in transit.

K. Accuracy

The accuracy issue in the context of lifelogging can be seen from three perspectives: (1) the accuracy of the underlying data collected; (2) the accuracy of algorithms and techniques applied in the data processing; and (3) the accuracy of the derived personal information that emerges from the processing.[181] With respect to the accuracy of the underlying data collected, a number of issues emerge. First of all, lifelogging technologies 'collect their data from the real world using imperfect sensing devices' which gives rise to accuracy issues.[182] Sensors may have faults or errors can occur because of things like faulty sensor installation, calibration or electrical problems.[183] Power instability, temperature changes, internal and external noises can also endanger the quality of the data collected by a lifelogging device.[184] A lifelogging device may involve multiple sensors, which means the chance of error accumulates.[185]

With respect to the accuracy of algorithms and techniques applied in the data processing, the reality is that it is not always possible or straightforward to ensure high-quality algorithmic design.[186] This is because '(e)very piece of software has some repertory of basic assumptions, values, limitations embedded within it'[187] which may be faulty and difficult for a human to uncover, especially where black-box algorithms are beings used. Diakopoulos and Friedler explain succinctly: 'Algorithms make mistakes, whether because of data errors in their inputs (garbage in, garbage out) or statistical uncertainty in their outputs.'[188]

It is further important to mention that even if the raw data applied in the processing is free of errors and the algorithms used in the processing are somehow free from all errors, accuracy remains an issue.[189] This is because often, the processing gives rise to new, implicit information about an individual (or a group of individuals) and this derivative information may contain mistakes or errors.[190] Additionally, even if the derived data is accurate, its accuracy and completeness must be maintained.

L. Recommendations

Data validation techniques should be applied to preserve the integrity of the data used by lifelogging devices and they should be built into the system at the outset of its development. Validation reduces inconsistencies and inaccuracies in the data and is an essential step to improve data reliability.[191] Although data validation processes have been developed by manual data analysis, performed by humans, automatic data validation tools have arisen in response to technologies like lifelogging that collect and process huge amounts of data, often in real-time.[192] There are new methods being developed to validate data collected by sensors and these techniques should be applied not only in data acquisition but also in data processing in order to increase the degree of confidence of the systems.[193]

Data cleaning is also very important to increase the accuracy of the data. As noted above, because of the low quality of sensors and random effects of their environments, sensor data are noisy. It is critical to analyse sensor data for its correctness, completeness and consistency before feeding it to the higher-level algorithms in order to, for example, conduct data analysis.[194]

M. Accountability

Lifelogging technologies give rise to many concerns about accountability, many of which have already been noted above. First, the lack of a user interface makes it difficult to convey what personal data is being collected and how these data are being used. This makes consent mechanisms more difficult to effectuate since consent should be informed.

Second, lifelogging devices and the digital ecosystems they feed into can be very opaque in how they handle data.[195] Opacity in the internal workings of lifelogging technologies hides the way data is being handled and as a result, a data subject might not fully be aware of how her data is being processed, why, by whom, where it is being stored, for how long and so on. For example, in the healthcare context, a lifelogging technology might co-exist within a platform where various applications ‘enable collaboration and workflow between doctors and patients across the entire spectrum of care, from self-care and prevention to diagnosis and treatment through recovery and wellness’.[196] The way that data is shared across the platform might give rise to a predication that an individual will respond better to one medication than another.[197] However, the factors giving rise to this conclusion might not be explicitly identifiable and explainable to the doctors, data scientists, or the patient.[198]

Finally, the size, velocity and sheer volume of data involved in lifelogging ecosystems gives rise to accountability challenges. It is not only hard to describe all data sources and uses in a privacy policy but also very challenging to keep track of all that information. When there are large volumes of data, often streaming at high speeds in real time, the possibility that consents or restrictions on information may get lost multiply due to the unrelenting pace and volume of the data.[199]

N. Recommendations

A number of different measures can contribute to the creation of an accountable lifelogging system. Here, the development of automated accountability is emerging as an important and interesting field, especially as it concerns the creation of an accountable lifelogging system.[200] The field is based on a number of different technologies such as such as formal accountability models, computer systems design and cryptographic techniques.[201] Wolf and Polonetsky explain, '(a)utomated accountability mechanisms can be designed to determine how personally identifiable information is used and whether the uses conform to established policies'.[202] Likewise, ENISA contends that lifelogging technologies should have automated mechanisms built into them that provide evidence that privacy rules are being followed.[203] It explains that accountable systems 'have automated and scalable control and auditing processes that can evaluate the level of privacy policy enforcement against the predefined machine- readable rules, as well as to provide evidence for any misconduct'.[204] That said, assuring accountability to rules depends on considerable manual effort and faces scaling challenges as the volume and complexity of data usage increases.[205]

Kagal outlines the six essential aspects of an accountable system and the first requirement is that there should be automated policy compliance through, for example, machine understandable policy language.[206] Kagal further explains that there should also be provenance management of information such as its source, creator etc.[207] Violation detection and identification is a third requirement.[208] This means that when data is misused, it is possible to identify the actual violation as well as the perpetrator.[209] Auditing is another core criterion, which for example, involves the creation of extensive audit logs of data requests, transfers and all uses.[210] Policy awareness must be included which requires that users are able to manipulate information by way of policy aware interferences that signal compliant/non-compliant uses.[211] Finally, redress mechanisms must be included so it is possible to identify the violation and perpetrator and take action.[212]

Recently, several different Data Protection Management Systems (DPMS) have emerged to support the manageability and traceability of the flow of personal data as well as to ensure and demonstrate privacy compliance with applicable legal rules. A DPMS is an internal compliance system that monitors the fulfilment of data-protection-related requirements within an entity.[213] According to Bauer et al, a DPMS can 'be understood as the entirety of all documented and implementation regulations, processes and measures that serve to systematically control the handling of personal data in the company in compliance with data protection laws'.[214] In short, a DPMS involves the utilisation of software to help data controllers demonstrate that they have established processes to implement data protection law.

IV. Conclusion

Lifelogging technologies have the capacity to transform the health and social care landscape in a way that few could have imagined. Indeed, the emergence of lifelogging technologies within these contexts presents incredible opportunities to diagnosis illnesses, engage in preventative medicine, manage healthcare costs and allow the elderly to live on their own for longer periods. These technologies, however, pose serious risks to the privacy of the individual through harmful surveillance, ubiquitous profiling and continuous tracking.

In response to some of the privacy concerns raised by lifelogging technologies, this chapter has proposed a number of technological measures that can be used to foster confidence and trust in the technology as being privacy protective. These recommendations aim at balancing data gathering and analysis while at the same time respecting the privacy of the data subject. They are general strategies that can be used to build privacy into a lifelogging technology at the outset of its development and hope to foster trust and confidence in the technology as being privacy aware from the outset of its development.

Bibliography

Agrawal, Rakesh, Jerry Kiernan, Ramakrishnan Srikant and Yirong Xu 'Hippocratic Databases' in Proceeding VLDB '02 *Proceedings of the 28th International Conference on Very Large Data Bases* (Hong Kong, 2002), 143–154.

Akl, A, B Taati, and A Mihailidis 'Autonomous Unobtrusive Detection of Mild Cognitive Impairment in Older Adults' (2015) 62 *IEEE Transactions on Biomedical Engineering* 1383.

Allen, Anita 'Dredging Up the Past: Lifelogging, Memory, and Surveillance' (2008) 75 *University of Chicago Law Review* 47.

Alshammari, M and A Simpson 'Towards a Principled Approach for Engineering Privacy by Design' in *Privacy Technologies and Policy*, eds E Schweighofer, H Leitold, A Mitrakas and K Rannenberg (Springer, 2017).

Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques, 0829/14/ENWP216 (2014).

Article 29 Working Party Opinion 8/2014 on the on Recent Developments on the Internet of Things (2014).

Ashby, Corey, Amit Bhatia, Francesco Tenore and Jacob Vogelstein 'Low-cost Electroencephalogram (EEG) Based Authentication'. Paper presented at *5th International IEEE/EMBS Conference on Neural Engineering* (Cancun, Mexico, 2011), 442–445.

Ausloos, Jef and P Dewitte 'Shattering One-Way Mirrors – Data Subject Access Rights in Practice' (2018) 8 *International Data Privacy Law* 4.

Bauer, Christoph, Frank Eickmeier and Anna Täschner White Paper: What Are the Changes Regarding Data Protection in the Future General Data Protection Regulation? ePrivacy GmbH (Hamburg, 2017). Available at: www.eprivacy.eu/fileadmin/Redakteur/News/Whitepaper_GDPR.pdf.

Bhatia, Rekha and Manpreet Singh 'Preserving Privacy in Healthcare Web Services Paradigm Through Hippocratic Databases' in *Intelligent Computing, Communication and Devices*, eds C. Lakhmi Jain, Srikanta Patnaik and Nikhil Ichalkaranje (Springer, 2015), 177–188.

Bailey, Ian Kerr 'Seizing Control? The Experience Capture Experiments of Ringley & Mann' (2007) 9 *Ethics and Information Technology* 129.

Barcena, MB, How Safe is Your Quantified Self? Symantec. Available at: www.symantec.com/content/dam/…/how-safe-is-your-quantified-self-en.pdf.

Batchelor, Rachel, Ania Bobrowicz, Robin Mackenzie and Alisoun Milne 'Challenges of Ethical and Legal Responsibilities When Technologies' Uses and Users Change: Social Networking Sites, Decision Making Capacity and Dementia' (2012) 14 *Ethics and Information Technology* 99.

Bertino, Elisa 'Purpose Based Access Control for Privacy Protection in Database Systems' in *Database Systems for Advanced Applications* eds Lizhu Zhou, Beng Chin and Ooi Xiaofeng Meng (Berlin; Heidelberg: Springer, 2005), 2–2.

Branch, Joel W, Chris Giannella, Boleslaw Szymanski, Ran Wolff and Hillol Kargupta 'In-network Outlier Detection in Wireless Sensor Networks' (2013) 34 *Knowledge and Information Systems* 23.

Brasher, Elizabeth A 'Addressing the Failure of Anonymization: Guidance from the European Union's General Data Protection Regulation' (2018) 2018 *Columbia Business Law Review* 209.

Brill, Julie, Commissioner US Federal Trade Commission 'Weaving a Tapestry to Protect Privacy and Competition in the Age of Big Data'. Address Before the European Data Protection Supervisor's Workshop on Privacy, Consumer Protection and Competition in the Digital Age (2 June 2014). Available at: www.ftc.gov/system/files/documents/public_statements/313311/140602edpsbrill2.pdf.

Brown, Ian 'GSR Discussion Paper Regulation and the Internet of Things, International Telecommunications Union' (Geneva, 2015). Available at: www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2015/Discussion_papers_and_Presentations/GSR_DiscussionPaper_IoT.pdf.

Cavoukian, Ann 'Privacy by Design: The Seven Foundational Principles', Information and Privacy Commissioner of Ontario, Canada (2010). Available at: www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

Chikhaoui, B, B Ye and A Mihailidis 'Feature-Level Combination of Skeleton Joints and Body Parts for Accurate Aggressive and Agitated Behavior Recognition' (2017) 8 *Journal of Ambient Intelligence and Humanized Computing* 957.

Chuang, John, Hamilton Nguyen, Charles Wang and Benjamin Johnson 'I think, Therefore I Am: Usability and Security of Authentication Using Brainwaves' in *Financial Cryptography and Data Security*, eds Andrew A Adams, Michael Brenner and Matthew Smith (Springer, 2013), 1–16.

Cippitelli, E, S Gasparrini, S Spinsante and E Gambi 'Kinect as a Tool for Gait Analysis: Validation of a Real-Time Joint Extraction Algorithm Working in Side View' (2015) 15 *Sensors* 1417.

Clinch, Sarah, Paul Metzger and Nigel Davies 'Lifelogging for "Observer" View Memories: An Infrastructure Approach'. Paper presented at UbiComp '14 Adjunct Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication (Seattle, Washington, 2014), 1397–1404.

Colesky, Michael, Jaap-Henk Hoepman and Christiaan Hillen 'A Critical Analysis of Privacy Design Strategies' 2016 *IEEE Security and Privacy Workshops*.

Colonna, Liane *Legal Implications of Data Mining: Assessing the European Union's Data Protection Principles in Light of the United States Government's National Intelligence Data Mining Practices* (Ragulka, 2016).

Colonna, Liane 'Mo' Data, Mo' Problems? Personal Data Mining and the Challenge to the Data Minimization Principle'. Workshop Proceedings of 'Big Data and Privacy' hosted by the Future of Privacy Forum (FPF) and the Stanford Law School's Center for Internet and Society (CIS) (September 2013). Available at: https://fpf.org/wp-content/uploads/Colonna-Mo-Data-Mo-Problems.pdf.

Corbet, Rob 'Internet of Things – Where Are We Now?' (2015) 15 *Privacy and Data Protection* 13.

Cornelius, Cory, Ronald Peterson, Joseph Skinner, Ryan Halter and David Kotz 'A Wearable System that Knows Who Wears It' in *Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys'14)*(Bretton Woods, New Hampshire, 2014) 55–67.

Crabtree, Andy, Tom Lodge, James Colley, et al 'Building Accountability into the Internet of Things: the IoT Databox Model' (2018) 4 *Journal of Reliable Intelligent Environments* 39.

Cranor Lorie, et al 'The Platform for Privacy Preferences 1.0 (P3P1.0)' Specification, W3C Recommendation, World Wide Web Consortium (16 April 2002). Available at: www.w3.org/TR/P3P.

D'Acquisto, Giuseppe, Josep Domingo-Ferrer, Panayiotis Kikiras, Vicenç Torra, Yves-Alexandre de Montjoye and Athena Bourka 'Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics, European Union Agency for Network and Information Security' (ENISA)(2015). Available at: www.enisa.europa.eu/publications/big-data-protection.

Daugherty, Paul 'The Rise of Digital Ecosystems in the "We Economy"' (2015) *Forbes* (9 March). Available at: www.forbes.com/sites/ciocentral/2015/03/09/the-rise-of-digital-ecosystems-in-the-we-economy/#401b2c655514.

Diakopoulos, Nicholas and Sorelle Friedler 'How to Hold Algorithms Accountable' (2016) *MIT Technology Review* 17 November.

Dipshan, Rhys 'The IoT Ambiguity: Secure Architecture, Vulnerable Data, Legal Tech News' (2 February 2018). Available at: www.law.com/legaltechnews/sites/legaltechnews/2018/02/02/the-iot-ambiguity-secure-architecture-vulnerable-data/.

Dwork, Cynthia 'Differential Privacy' in *33rd International Colloquium on Automata, Languages and Programming, Part II* (ICALP 2006), eds M Bugliesi, B Preneel et al (Springer-Verlag 2006), 1–12.

El Shekeil, Salah Addin and Saran Laoyookhong 'GDPR Privacy by Design: From Legal Requirements to Technical Solutions', Thesis, Stockholm University Department of Computer and Systems Sciences Master's degree. Available at: www.isaca.org/chapters4/Sweden/OmOss/Documents/Stipendie2017_ElShekeil-Laoyookhong.pdf.

European Agency for Network and Information Security (ENISA) 'To Log or Not to Log? Risks and Benefits of Emerging Life-logging Applications' (2011). Available at: www.enisa.europa.eu/publications/to-log-or-not-to-log-risks-and-

benefits-of-emerging-life-logging-applications.
European Data Protection Supervisor Opinion 5/2018, Preliminary Opinion on Privacy by Design (31 May 2018). Available at: https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf.
Ferrari, Elena 'Access Control' in *Encyclopedia of Database Systems*, eds Ling Liu and M Tamer Özsu (New York, New York: Springer, 2014).
Flórez-Revuelta, Francisco, Alex Mihailidis, Martina Ziefle, Liane Colonna and Susanna Spinsante 'Privacy-Aware and Acceptable Lifelogging Services for Older and Frail People: the PAAL Project'. Paper presented at *2018 IEEE 8th International Conference on Consumer Electronics – Berlin* (ICCE-Berlin 2018).
FTC Staff Report Internet of Things: Privacy and Security in a Connected World (2015). Available at: www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
Gjermundrød, Harald, Ioanna Dionysiou and Kyriakos Costa 'Privacy Tracker: A Privacy-by-Design GDPR-Compliant Framework with Verifiable Data Traceability Controls' in *Current Trends in Web Engineering*, eds Sven Casteleyn, Peter Dolog and Cesare Pautasso (Springer, 2016), 3–15.
Goodman, Ellen P 'The Atomic Age of Data: Policies for the Internet of Things' (2015) 1 *Aspen Institute* 38. Available at: http://csreports.aspeninstitute.org/documents/Atomic_Age_of_Data.pdf.
Gunasekara, Gehan 'The "Final" Privacy Frontier? Regulating Trans-border Data Flows,' (20070 17 *International Journal of Law and Information Technology* 147.
Gurrin, Cathal, Rami Albatal, Hideo Joho and Kaori Ishii 'A Privacy by Design Approach to Lifelogging' in *Digital Enlightenment Yearbook 2014*, eds K O'Hara, C Nguyen and P Haynes (IOS Press, 2014), 49–73.
Grandison, Tyrone and Kristen LeFevre 'Hippocratic Database' in *Encyclopedia of Cryptography and Security*, eds C Henk, A van Tilborg and Sushil Jajodia (Springer, 2011).
Hartzog, Woodrow and Frederic Stutzman 'Obscurity by Design' (2013) 88 *Washington Law Review* 392.
Hintze, Mike 'In Defense of the Long Privacy Statement' (2017) 76 *Maryland Law Review* 1044.
IMB White Paper, Integrating and Governing Big Data. Available at: www-950.ibm.com/events/wwe/grp/grp037.nsf/vLookupPDFs/Integrating_Governing_BigData/$file/Integrating_Governing_B
Ienca, Marcello, Fabrice Jotter, Constantin Vica and Bernice Elger 'Social and Assistive Robotics in Dementia Care: Ethical Recommendations for Research and Practice' (2016) 8 *International Journal of Social Robotics* 565.
Jacquemard, Tim, Peter Novitzky, Fiachra O'Brolcháin, Alan F Smeaton and Bert Gordijn 'Challenges and Opportunities of Lifelog Technologies: A Literature Review and Critical Analysis' (2014) 20 *Science and Engineering Ethics* 379.
Joe, Ryan, Exiting FTC Commissioner Julie Brill: 'Advertisers and Ad Networks Need to Provide More Usable Tools for Consumers', *Ad Exchanger* (23 March 2016). Available at: https://adexchanger.com/privacy/exiting-ftc-commissioner-julie-brill-advertisers-and-ad-networks-need-to-provide-more-usable-tools-for-consumers/.
Kagal, Lalana 'Designing for Accountability: A Checklist for Accountable Information Systems'. Paper at 2nd International Workshop on Accountability: Science, Technology and Policy, MIT Computer Science and Artificial Intelligence Laboratory (29–30 January 2014). Available at: http://dig.csail.mit.edu/2014/AccountableSystems2014.
Kamrani, Farzad, Mikael Wedlin and Ioana Rodhe 'Internet of Things: Security and Privacy Issues', Swedish Defence Research Agency (FOI), Report number, FOI-R–4362–SE (December 2016).
Kanagavel, Madhan 'Security by Default – Five Principles for Building More Secure Apps' *Enterprise Innovation* (23 August 2018). Available at: www.enterpriseinnovation.net/article/security-default-5-principles-building-more-secure-apps-2017033942/page/0/1.
Karegar, Farzaneh, Christoph Striecks, Stephan Krenn, Felix Hörandner, Thomas Lorünser and Simone Fischer-Hübner 'Opportunities and Challenges of CREDENTIAL: Towards a Metadata-Privacy Respecting Identity Provider, in Privacy and Identity Management' in *Facing up to Next Steps*, eds Anja Lehmann, Diane Whitehouse, Simone Fischer-Hübner, Lothar Fritsch and Charles Raab (Springer, 2016), 76–91.
Karjoth, Günter, Matthias Schunter and Michael Waidner 'Platform for Enterprise Privacy Practices: Privacy-Enabled Management of Customer Data' in *Proceedings of 2nd Workshop Privacy Enhancing Technologies*, eds Roger Dingledine and Paul Syverson (Springer, 2002), 69–84.
Kelly, Paul, Simon J Marshall, Hannah Badland, Jacqueline Kerr, Melody Oliver, Aiden R Doherty and Charlie Foster, 'An Ethical Framework for Automated, Wearable Cameras in Health Behavior Research' (2013) 44 *American Journal of Preventative Medicine* 314.
Klarreich, Erica and Simons Science News 'Privacy by the Numbers: A New Approach to Safeguarding Data, The Scientific American' (31 December 2012). Available at: www.scientificamerican.com/article/privacy-by-the-numbers-a-new-approach-to-safeguarding-data/.
Langheinrich, Marc 'A Privacy Awareness System for Ubiquitous Computing Environments' in *UbiComp 2002: Ubiquitous*

Computing, eds Gaetano Borriello, Lars Erik Holmquist (Springer, 2002), 237–245.
Leonard, Peter 'Customer Data Analytics: Privacy Settings for "Big Data" Business' (2014) 4 *International Data Privacy Law* 53, 60.
Lindstrom, John 'Security Challenges for Wearable Computing a Case Study'. Fourth International Forum on Conference International Forum on Applied Wearable Computing (Tel Aviv, Israel, 2007).
Lioudakis, Georgios V, Eleftherios A Koutsoloukas, Nikolaos Dellas et al, 'IS: A Proxy for Privacy: The Discreet Box'. Paper presented at EUROCON 2007 – The International Conference on 'Computer as a Tool' (Warsaw, Poland, 2007).
Makker, Sona R 'Overcoming "Foggy" Notions of Privacy: How Data Minimization Will Enable Privacy in the Internet of Things' (2017) 85 *University of Missouri–Kansas Law Review* 895.
Mauritius Declaration on the Internet of Things (Balaclava, 14 October 2014). Available at: https://edps.europa.eu/sites/edp/files/publication/14-10-14_mauritius_declaration_en.pdf.
Metoui, Nadia and Michele Bezzi 'Differential Privacy Based Access Control' in *On the Move to Meaningful Internet Systems Conferences*, eds Christophe Debruyne, Hervé Panetto et al (Springer, 2016), 962–974.
Meola, Andrew 'The Roles of Cloud Computing and Fog Computing in the Internet of Things Revolution' *Business Insider* (20 December 2016). Available at: www.businessinsider.com/internet-of-things-cloud-computing-2016-10.
Motti, VG and K Caine 'Users' Privacy Concerns about Wearables: Impact of Form Factor, Sensors and Type of Data Collected' in *International Conference on Financial Cryptography and Data Security*, eds M Brenner, N Christin, B Johnson, et al (Springer Berlin 2015), 231–244.
Muro-de-la-Herran, Alvaro, Begonya Garcia-Zapirain and Amaia Mendez-Zorrilla, 'Gait Analysis Methods: An Overview of Wearable and Non-wearable Systems' Highlighting Clinical Applications (2014) 14 *Sensors* 3362.
Nissenbaum, Helen, *Privacy in Context: Technology, Policy and the Integrity of Social Life*, (Stanford Law Books, 2010).
Office of the Privacy Commissioner of Canada, Wearable Computing – Challenges and Opportunities for Privacy Protection (Ottawa: OPC, January 2014). Available at: www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/wc_201401/.
Ohm, Paul 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 *UCLA Law Review* 1701.
Oliveira, Stanley RM and Osmar R Zaiane 'Towards Standardization in Privacy-Preserving Data Mining' in Proceedings of the Third Workshop on Data Mining Standards, in Conjunction with KDD 2004 (Seattle, WA, 2004).
Oppit, Marcus and Peter Tomsu 'Fog Computing' in *Inventing the Cloud Century*, eds Marcus Oppitz and Peter Tomsu (Springer, 2018), 471–486, 473.
Padilla-López, José Ramón, Alexandros André Chaaraoui and Francisco Flórez-Revuelta 'Visual Privacy Protection Methods: A Survey' (2015) 42 *Expert Systems with Applications* 4177.
Pearson, Siani and Marco Casassa-Mont, 'Sticky Policies: An Approach for Managing Privacy across Multiple Parties' (2011) 44 *Computer* 60.
Perez, Alfredo J, Sherali Zeadally and Scott Griffith 'Bystanders' Privacy' (2017) 19 *IEEE IT Professional* 61.
Pingo, Zablon and Bhuva Narayan 'When Personal Data Becomes Open Data: An Exploration of Lifelogging, User Privacy, and Implications for Privacy Literacy' in *Digital Libraries: Knowledge, Information, and Data in an Open Access Society*, eds Atsuyuki Morishima, Andreas Rauber and Chern Li Liew(Springer, 2016), 3–9.
Pires, Ivan Miguel, Nuno M Garcia, Nuno Pombo, Francisco Flórez-Revuelta and Natalia Díaz Rodríguez 'Validation Techniques for Sensor Data in Mobile Health Applications' (2016) *Journal of Sensors*. Available at: http://dx.doi.org/10.1155/2016/2839372.
Price II, W Nicholson 'Black-Box Medicine' (2015) 28 *Harvard Journal of Law and Technology* 419.
Quevedo, Joseba, Diego GarciaVicenc et al 'Sensor Data Validation and Reconstruction' in *Real-time Monitoring and Operational Control of Drinking-Water Systems*, eds Vicenç Puig, Carlos Ocampo-Martínez et al (Springer, 2017), 175–193.
Rahman, Mahmudur, Bogdan Carbunar and Madhusudan Banik 'Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device' (2013). Available at: https://petsymposium.org/2013/papers/rahman-health.pdf.
Ramirez, Edith, Opening Remarks of FTC Chairwoman Edith Ramirez at 'The Internet of Things: Privacy and Security in a Connected World'. Available at: www.ftc.gov/sites/default/files/documents/public_statements/opening-remarks-ftc-chairwoman-edith-ramirez-federal-trade-commission-internet-things-privacy/131119iotremarks.pdf.
Rashid, Fahmida Y 'Don't Get Bit by Zombie Cloud Data', *InfoWorld* (20 April 2017).
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, L 119/1, 4.5.2016.
Raj, Pethuru and Anupama C Raman *The Internet of Things: Enabling Technologies, Platforms, and Use Cases* (Taylor and

Francis, 2017), 337.
Rao, Umesh Hodeghatta and Umesha Nayak 'Access Controls' in *The InfoSec Handbook*, eds Umesh Hodeghatta Rao and Umesha Nayak (Apress, 2014), 63–76.
Roosa, Steven, 'A Deep Dive into the Privacy and Security Risks for Health, Wellness and Medical Apps' (6 April 2015). Available at: https://iapp.org/news/a/a-deep-dive-into-the-privacy-and-security-risks-for-health-wellness-and-medical-apps/.
Roszak, Theodore, *The Cult of Information* (University of California Press, 1986), 95.
Schartum, Dag Wiese, 'Making Privacy by Design Operative' (2016) 24 *International Journal of Law and Information Technology* 151.
Schwartz, Ari, Looking Back at P3P: Lessons for the Future, Center for Democracy and Technology (November 2009). Available at: www.cdt.org/files/pdfs/P3P_Retro_Final_0.pdf.
Seipel, Peter, 'Nordic School of Proactive Law Conference, June 2005 Closing Comments' in *A Proactive Approach, Scandinavian Studies in Law Volume 49*, ed Peter Wahlgren, (Stockholm Institute for Scandinavian Law, 2006).
Shahzad, Muhammad and Munindar P Singh, Continuous Authentication and Authorization for the Internet of Things (2017) 21 *IEEE Internet Computing* 86.
Shrestha, Prakash and Nitesh Saxena 'An Offensive and Defensive Exposition of Wearable Computing' (2018) 92(1) *ACM Computing Surveys* 50.
Soghoian, Christopher 'Not an Option: Time for Companies to Embrace Security by Default, *Arstechnica* (8 September 2011). Available at: https://arstechnica.com/tech-policy/2011/08/not-an-option-time-for-companies-to-embrace-security-by-default/.
Soni, YS, SB Somani and VV Shete 'Biometric User Authentication Using Brain Waves' 2016 International Conference on Inventive Computation Technologies (Coimbatore, India, 2016), 1–6.
Spiekermann, Sarah 'The Challenges of Privacy by Design' (2012) 38 *Communications of the ACM* 55.
Sprager, SMB Juric 'Inertial Sensor-Based Gait Recognition: A Review' (2015) 15 *Sensors* 22089.
Templeman, Robert, Mohammed Korayem, David Crandall and Apu Kapadia 'Place Avoider: Steering First-Person Cameras away from Sensitive Spaces' in 21st Annual Network and Distributed System Security Symposium (2014).
US Department of Health, Education and Welfare, Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems (July 1973). Available at: www.epic.org/privacy/hew1973report/.
US Federal Trade Commission (FTC), Careful Connections: Building Security in the Internet of Things (January 2015). Available at: www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf.
US Federal Trade Commission (FTC), Internet of Things: Privacy & Security in a Connected World (January 2015). Available at: www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
US President's Council of Advisors on Science and Technology, Big Data and Privacy: A Technological Perspective (2014). Available at: https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf.
Urquhart, Lachlan, Tom Lodge and Andy Crabtree 'Demonstrably Doing Accountability in the Internet of Things' (2018). Available at: https://arxiv.org/abs/1801.07168.
Voigt, Paul, Axel von dem Bussche *Organisational Requirements, in the EU General Data Protection Regulation, A Practical Guide* (Springer, 2017), 31–86.
Wang, Bo, Jing Yang The State of the Art and Tendency of Privacy Preserving Data Mining. Paper presented at *International Conference on E-Business and E-Government* (ICEE)(6–8 May 2011).
Weik, Martin H *Access Control, in Computer Science and Communications Dictionary* (Boston, MA: Springer, 2001).
Weitzner, Daniel J 'The Jurisprudence of Accountability'. Paper presented at *Second International Workshop on Accountability: Science, Technology and Policy, MIT Computer Science and Artificial Intelligence Laboratory (29–30 January 2014)*. Available at: http://dig.csail.mit.edu/2014/AccountableSystems2014/.
Wolf, Christopher and Jules Polonetsky Future of Privacy Forum, An Updated Privacy Paradigm for the 'Internet of Things' (19 November 2013). Available at: www.futureofprivacy.org/wp-content/uploads/Wolf-and-Polonetsky-An-Updated-Privacy-Paradigm-for-the-'Internet-of-Things'-11-19-2013.pdf.
Yang, Po, Dainius Stankevicius et al 'Lifelogging Data Validation Model for Internet of Things Enabled Personalized Healthcare' (2018) 48 *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 50.
Zeng, Deze, Song Guo and Zixue Cheng 'The Web of Things: A Survey' (2011) 6 *Journal of Communications* 424.
Zhuang, Yongzhen, Lei Chen, X Sean Wang and Jie Lian 'A Weighted Moving Average-based Approach for Cleaning Sensor Data'. Paper presented at *27th International Conference on Distributed Computing Systems* (Toronto, Ontario,

25–27 June 2007).

---

[1] The support of the JPI More Years, Better Lives and the Swedish Research Council for Health, Working Life, and Welfare (grant number is 2017-02302) is gratefully acknowledged.

[2] The Swedish Law and Informatics Research Institute (IRI), Stockholm University.

[3] Francisco Flórez-Revuelta, Alex Mihailidis, Martina Ziefle, Liane Colonna and Susanna Spinsante 'Privacy-Aware and Acceptable Lifelogging Services for Older and Frail People: the PAAL Project' (2018) *IEEE 8th International Conference on Consumer Electronics – Berlin (ICCE-Berlin)*.

[4] Ibid.

[5] Ibid; Ian Brown 'GSR Discussion Paper Regulation and the Internet of Things, International Telecommunications Union' (Geneva, 2015). Available at: www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2015/Discussion_papers_and_Presentations/GSR_DiscussionPaper_IoT.pdf.

[6] E Cippitelli, S Gasparrini, S Spinsante and E Gambi 'Kinect as a Tool for Gait Analysis: Validation of a Real-Time Joint Extraction Algorithm Working in Side View' (2015) 15 *Sensors* 1417.

[7] A Akl, B Taati and A Mihailidis 'Autonomous Unobtrusive Detection of Mild Cognitive Impairment in Older Adults' (2015) 62 *IEEE Transactions on Biomedical Engineering* 1383.

[8] B Chikhaoui, B Ye and A Mihailidis 'Feature-Level Combination of Skeleton Joints and Body Parts for Accurate Aggressive and Agitated Behavior Recognition' (2017) 8 *Journal of Ambient Intelligence and Humanized Computing* 957.

[9] Lachlan Urquhart, Tom Lodge and Andy Crabtree 'Demonstrably Doing Accountability in the Internet of Things' (2018). Available at: https://arxiv.org/abs/1801.07168.

[10] Nissenbaum (n 3).

[11] Urquhart, Lodge and Crabtree (n 9).

[12] Michael Colesky, Jaap-Henk Hoepman and Christiaan Hillen 'A Critical Analysis of Privacy Design Strategies' (2016) IEEE Security and Privacy Workshops (SPW).

[13] See generally, Peter Seipel 'Nordic School of Proactive Law Conference, June 2005 Closing Comments' in A *Proactive Approach, Scandinavian Studies in Law Volume 49*, ed Peter Wahlgren (Stockholm: Stockholm Institute for Scandinavian Law, 2006).

[14] Dag Wiese Schartum 'Making Privacy by Design Operative' (2016) 24 *International Journal of Law and Information Technology* 151.

[15] Woodrow Hartzog and Frederic Stutzman 'Obscurity by Design' (2013) 88 *Washington Law Review* 392.

[16] Ann Cavoukian 'Privacy by Design: The Seven Foundational Principles' Information and Privacy Commissioner of Ontario, Canada (2010). Available at: www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

[17] Schartum (n 14) 151, 157.

[18] Cathal Gurrin, Rami Albatal, Hideo Joho and Kaori Ishii 'A Privacy by Design Approach to Lifelogging' in *Digital Enlightenment Yearbook* eds K O'Hara, C Nguyen, P Haynes (IOS Press, 2014), 49–73; Sarah Spiekermann 'The Challenges of Privacy by Design' (2012) 55 *Communications of the ACM* 38; see also M Alshammari and A Simpson 'Towards a Principled Approach for Engineering Privacy by Design' in *Privacy Technologies and Policy*, eds E Schweighofer, H Leitold, A Mitrakas and K. Rannenberg (Springer, 2017).

[19] See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, L 119/1, 4.5.2016 ('GDPR'), Art 25: Data protection by design and by default.

[20] GDPR, recital 78 ('Such measures could consist, inter alia, of minimizing the processing of personal data, pseudonymizing personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features').

[21] Schartum (n 14) 151.

[22] European Data Protection Supervisor, Opinion 5/2018, Preliminary Opinion on Privacy by Design (31 May 2018). Available at: https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf.

[23] FTC Staff Report, 'Internet of Things: Privacy and Security in a Connected World' (2015). Available at: www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf; see also Opening Remarks of FTC Chairwoman Edith Ramirez at 'The Internet of Things: Privacy and Security in a Connected World'. Available at: www.ftc.gov/sites/default/files/documents/public_statements/opening-remarks-ftc-chairwoman-edith-ramirez-federal-trade-commission-internet-things-privacy/131119iotremarks.pdf.

[24] Peter Leonard, 'Customer Data Analytics: Privacy Settings for "Big Data" Business' (2014) 4 *International Data Privacy Law* 53, 60.

[25] Paul Voigt and Axel von dem Bussche 'Organisational Requirements' in *The EU General Data Protection Regulation, A Practical Guide* (Springer, 2017), 31–86.

[26] Rob Corbet 'Internet of Things – Where Are We Now?' (2015) 15 *Privacy and Data Protection* 13. ('The fact that many IoT devices are not immediately visible to the eye creates difficulties in terms of meeting the legal standards typically imposed in the context of other forms of data capture. Privacy notices and privacy policies have traditionally been the means by which data controllers have tried to meet their disclosure obligations under the Data Protection Directive (95/46/EC) and under US fair trade laws. But is this workable in an IoT environment?').

[27] Ramirez (n 23).

[28] Ellen P Goodman 'The Atomic Age of Data: Policies for the Internet of Things' (2015) 1 *Aspen Institute* 38. Available at: http://csreports.aspeninstitute.org/documents/Atomic_Age_of_Data.pdf.

[29] Alfredo J Perez, Sherali Zeadally and Scott Griffith 'Bystanders' Privacy' (2017) 19 *IT Professional* 61. Available at:www.computer.org/cms/Computer.org/magazines/whats-new/2017/07/mit2017030061.pdf; Anita Allen 'Dredging Up the Past: Lifelogging, Memory, and Surveillance' (2008) 75 *University of Chicago Law Review* 47; Jane Bailey and Ian Kerr 'Seizing Control? The Experience Capture Experiments of Ringley & Mann' (2007) 9 *Ethics and Information Technology* 129.

[30] Paul Kelly, Simon J Marshall, Hannah Badland, Jacqueline Kerr, Melody Oliver, Aiden R Doherty and Charlie Foster 'An Ethical Framework for Automated, Wearable Cameras in Health Behavior Research' (2013) 44 *American Journal of Preventative Medicine* 314.

[31] Ibid. ('Third parties who encounter the wearer have their image (and possibly other data) captured without the opportunity to provide informed consent … These people may be photographed, knowingly or unknowingly, and will not have the opportunity to provide informed consent.').

[32] VG Motti and K Caine 'Users' Privacy Concerns about Wearables: Impact of Form Factor, Sensors and Type of Data Collected' in *International Conference on Financial Cryptography and Data Security*, eds M Brenner, N Christin, B Johnson, et al (Springer, 2015), 231–244.

[33] Kelly et al (n 30).

[34] Corbet (n 26) 13, 14.

[35] Rachel Batchelor, Ania Bobrowicz, Robin Mackenzie and Alisoun Milne 'Challenges of Ethical and Legal Responsibilities when Technologies' Uses and Users Change: Social Networking Sites, Decision Making Capacity and Dementia' (2012) 14 *Ethics and Information Technology* 99; see also Marcello Ienca, Fabrice Jotter, Constantin Vica and Bernice Elger 'Social and Assistive Robotics in Dementia Care: Ethical Recommendations for Research and Practice' (2016) 8 *International Journal of Social Robotics* 565.

[36] Tim Jacquemard, Peter Novitzky, Fiachra O'Brolcháin, Alan F Smeaton and Bert Gordijn 'Challenges and Opportunities of Lifelog Technologies: A Literature Review and Critical Analysis' (2014) 20 *Science and Engineering Ethics* 379.

[37] Ibid at 405.

[38] European Agency for Network and Information Security (ENISA), 'To Log or Not to Log? Risks and Benefits of Emerging Life-logging Applications' (2011). Available at: www.enisa.europa.eu/publications/to-log-or-not-to-log-risks-and-benefits-of-emerging-life-logging-applications ('design life-logging services with privacy-friendly default configurations

and settings, intelligible to a wide range of customers').

[39] Office of the Privacy Commissioner of Canada, 'Wearable Computing – Challenges and Opportunities for Privacy Protection' (OPC, January 2014). Available at: www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/wc_201401/.

[40] Ibid.

[41] Andy Crabtree, Tom Lodge, James Colley, et al 'Building Accountability into the Internet of Things: the IoT Databox Model' (2018) 4 *Journal of Reliable Intelligent Environments* 39.

[42] Ibid.; see also Julie Brill, Commissioner US Federal Trade Commission 'Weaving a Tapestry to Protect Privacy and Competition in the Age of Big Data'. Address Before the European Data Protection Supervisor's Workshop on Privacy, Consumer Protection and Competition in the Digital Age (2 June 2014). Available at: www.ftc.gov/system/files/documents/public_statements/313311/140602edpsbrill2.pdf (where former, FTC Commissioner Brill argues: 'Manufacturers should deploy signals or consumer-friendly online dashboards that explain – through sounds, pictures, or graphs – the data the device collects about consumers, the uses of the data, and who else might see it.').

[43] Office of the Privacy Commissioner of Canada (n 39).

[44] Ibid; see also, Voigt and von dem Bussche (n 25) 31–86 ('… the IoT poses an opportunity to redesign how consent is done with users').

[45] Office of the Privacy Commissioner of Canada (n 39).

[46] Giuseppe D' Acquisto, Josep Domingo-Ferrer, Panayiotis Kikiras, Vicenç Torra, Yves-Alexandre de Montjoye and Athena Bourka 'Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics' (2015) European Union Agency for Network and Information Security (ENISA). Available at: www.enisa.europa.eu/publications/big-data-protection.

[47] Article 29 Working Party, Opinion 8/2014 on the on Recent Developments on the Internet of Things (16 September 2014); FTC Staff Report, 'Internet of Things: Privacy and Security in a Connected World' (2015). Available at: www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[48] Salah Addin ElShekeil and Saran Laoyookhong 'GDPR Privacy by Design: From Legal Requirements to Technical Solutions' Thesis, Stockholm University Department of Computer and Systems Sciences Master's degree. Available at: www.isaca.org/chapters4/Sweden/OmOss/Documents/Stipendie2017_ElShekeil-Laoyookhong.pdf.

[49] Ibid.

[50] GDPR, Art 9.

[51] Perez, Zeadally and Griffith (n 29) 61.

[52] José Ramón Padilla-López, Alexandros André Chaaraoui and Francisco Flórez-Revuelta 'Visual Privacy Protection Methods: A Survey' (2015) 42 *Expert Systems with Applications* 4177.

[53] Ibid at 4179.

[54] Ibid.

[55] Ibid.

[56] Ibid.

[57] Perez, Zeadally and Griffith (n 29): 'A possible solution for managing reidentification can be achieved by substituting bystanders' faces with fake, computer-generated faces, or faces taken from public-domain photos to obfuscate real images obtained of bystanders.'

[58] Ibid at 61.

[59] Ibid.

[60] Ibid.

[61] Ibid.

[62] LED stands for 'light emitting diode'.

[63] Perez, Zeadally and Griffith (n 29) 61.

64 Ibid.

65 Crabtree et al (n 41) 39.

66 Urquhart, Lodge and Crabtree (n 9).

67 Zablon Pingo and Bhuva Narayan 'When Personal Data Becomes Open Data: An Exploration of Lifelogging, User Privacy, and Implications for Privacy Literacy' in *Digital Libraries: Knowledge, Information, and Data in an Open Access Society*, eds Atsuyuki Morishima, Andreas Rauber and Chern Li Liew (Springer, 2016), 3–9.

68 Mauritius Declaration on the Internet of Things (Balaclava, 14 October 2014). Available at: https://edps.europa.eu/sites/edp/files/publication/14-10-14_mauritius_declaration_en.pdf.

69 US Department of Health, Education and Welfare, Records, Computers and the Rights of Citizens 'Report of the Secretary's Advisory Committee on Automated Personal Data Systems (July 1973)'. Available at: www.epic.org/privacy/hew1973report/.

70 President's Council of Advisors on Science and Technology 'Big Data and Privacy: A Technological Perspective (2014). Available at: https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf.

71 Nadia Metoui and Michele Bezzi 'Differential Privacy-based Access Control' in *On the Move to Meaningful Internet Systems: OTM 2016 Conferences*, eds Christophe Debruyne, Hervé Panetto et al (Springer, 2016), 962–974, 971.

72 Elisa Bertino, 'Purpose Based Access Control for Privacy Protection in Database Systems' in *Database Systems for Advanced Applications*, eds Lizhu Zhou, Beng Chin, Ooi Xiaofeng Meng (Springer, 2005), 2–2 ('An important requirement in the development of such systems is the need of providing comprehensive and accurate privacy-related metadata, such as data usage purposes. Such metadata represent the core of access control mechanisms specifically tailored towards privacy.').

73 Jef Ausloos and Pierre Dewitte 'Shattering One-Way Mirrors – Data Subject Access Rights in Practice' (2018) 8 *International Data Privacy Law* 4.

74 Siani Pearson and Marco Casassa-Mont 'Sticky Policies: An Approach for Managing Privacy across Multiple Parties' (2011) 44 *Computer* 60.

75 Joe Ryan and exiting FTC Commissioner Julie Brill: 'Advertisers and Ad Networks Need to Provide More Usable Tools for Consumers' *Ad Exchanger* (23 March 2016). Available at: https://adexchanger.com/privacy/exiting-ftc-commissioner-julie-brill-advertisers-and-ad-networks-need-to-provide-more-usable-tools-for-consumers/.

76 Ari Schwartz, 'Looking Back at P3P: Lessons for the Future' Center for Democracy and Technology (November 2009). Available at: www.cdt.org/files/pdfs/P3P_Retro_Final_0.pdf.

77 Metoui and Bezzi (n 71) 962–974.

78 D'Acquisto et al (n 46).

79 Günter Karjoth, Matthias Schunter and Michael Waidner 'Platform for Enterprise Privacy Practices: Privacy-enabled Management of Customer Data' in *Proceedings of Second Workshop Privacy Enhancing Technologies*, eds Roger Dingledine and Paul Syverson (Springer, 2002), 69–84.

80 Schwartz (n 76).

81 Lorie Cranor et al 'The Platform for Privacy Preferences 1.0 (P3P1.0) Specification', W3C Recommendation, World Wide Web Consortium (16 April 2002). Available at: www.w3.org/TR/P3P.

82 Ibid.

83 Mike Hintze 'In Defense of the Long Privacy Statement' (2017) 76 *Maryland Law Review* 1044; see also Schwartz (n 76)('P3P is far too complex as it stands today.').

84 Schwartz, ibid at 83.

85 Ibid.

86 Ibid.

87 Georgios V Lioudakis, Eleftherios A Koutsoloukas, Nikolaos Dellas et al 'IS: A Proxy for Privacy: The Discreet Box'. Paper presented at EUROCON 2007 – The International Conference on 'Computer as a Tool' (Warsaw, Poland, 2007).

88 Marc Langheinrich 'A Privacy Awareness System for Ubiquitous Computing Environments' in *UbiComp 2002: Ubiquitous Computing*, eds Gaetano Borriello, Lars Erik Holmquist (Springer, 2002), 237–245, 241.

89 Ibid.

90 Lioudakis et al (n 87) 973.

91 Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant and Yirong Xu 'Hippocratic Databases' in *Proceeding VLDB '02 Proceedings of the 28th International Conference on Very Large Data Bases* (Hong Kong, 2002), 143–154.

92 Tyrone Grandison and Kristen LeFevre 'Hippocratic Database' in *Encyclopedia of Cryptography and Security*, eds Henk CA van Tilborg and Sushil Jajodia (Springer, 2011).

93 Rekha Bhatia and Manpreet Singh 'Preserving Privacy in Healthcare Web Services Paradigm Through Hippocratic Databases' in *Intelligent Computing, Communication and Devices*, eds Lakhmi C Jain, Srikanta Patnaik and Nikhil Ichalkaranje (Springer, 2015), 177–188, 178.

94 Agrawal et al (n 91) 143–154; for more see Grandison et al (n 92) 409–429.

95 Elizabeth A Brasher 'Addressing the Failure of Anonymization: Guidance from the European Union's General Data Protection Regulation' (2018) 2018 *Columbia Business Law Review* 209, 248; see also GDPR, Art 4(5).

96 Ibid.

97 Ibid, Art 25(1).

98 Ibid, recital 125.

99 Farzad Kamrani, Mikael Wedlin and Ioana Rodhe 'Internet of Things: Security and Privacy Issues'. Swedish Defence Research Agency (FOI), Report number, FOI-R–4362–SE (December 2016).

100 Bo Wang and Jing Yang 'The State of the Art and Tendency of Privacy Preserving Data Mining'. International Conference on E-Business and E-Government (ICEE)(6–8 May 2011).

101 Stanley RM Oliveira and Osmar R Zaiane 'Towards Standardization in Privacy-Preserving Data Mining', Proceedings of the Third Workshop on Data Mining Standards, in conjunction with KDD 2004 (Seattle, WA, 2004).

102 Cynthia Dwork 'Differential Privacy' in *33rd International Colloquium on Automata, Languages and Programming, Part II* (ICALP 2006), eds M Bugliesi, B Preneel et al (Berlin Heidelberg: Springer-Verlag 2006), 1–12.

103 Erica Klarreich and Simons Science News 'Privacy by the Numbers: A New Approach to Safeguarding Data' *The Scientific American* (31 December 2012). Available at: www.scientificamerican.com/article/privacy-by-the-numbers-a-new-approach-to-safeguarding-data/.

104 Corbet (n 26) 13, 15.

105 See Liane Colonna 'Mo' Data, Mo' Problems? Personal Data Mining and the Challenge to the Data Minimization Principle'. Workshop proceedings of 'Big Data and Privacy' hosted by the Future of Privacy Forum (FPF) and Stanford Law School's Center for Internet and Society (CIS) (September 2013). Available at: https://fpf.org/wp-content/uploads/Colonna-Mo-Data-Mo-Problems.pdf.

106 Jacquemard et al (n 36) 379.

107 Allen (n 29) 47.

108 Sarah Clinch, Paul Metzger and Nigel Davies 'Lifelogging for "Observer" View Memories: An Infrastructure Approach'. *UbiComp '14 Adjunct Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication* (Seattle, Washington, 2014), 1397–1404.

109 Allen (n 29) 47, 49.

110 Ibid at 49.

111 Clinch et al (n 108) 1397–1404, 1402.

112 Robert Templeman, Mohammed Korayem, David Crandall and Apu Kapadia 'PlaceAvoider: Steering First-Person Cameras away from Sensitive Spaces'. Paper presented at *21st Annual Network and Distributed System Security Symposium* (NDSS) (2014).

113 Crabtree et al (n 41) 39, 42.

114 Ibid at 42.

115 Paul Ohm 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 *UCLA Law Review* 1701, 1707.

116 GDPR, recital 26.

117 Flórez-Revuelta et al (n 3).

118 Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, 0829/14/ENWP216 (10 April 2014).

119 Ibid.

120 Kamrani, Wedlin and Rodhe (n 99); see also President's Council of Advisors (n 70) ('In general, as the size and diversity of available data grows, the likelihood of being able to re-identify individuals (that is, re-associate their records with their names) grows substantially.').

121 Farzaneh Karegar, Christoph Striecks, Stephan Krenn, Felix Hörandner, Thomas Lorünser and Simone Fischer-Hübner 'Opportunities and Challenges of CREDENTIAL: Towards a Metadata-Privacy Respecting Identity Provider' in *Privacy and Identity Management. Facing up to Next Steps*, eds Anja Lehmann, Diane Whitehouse, Simone Fischer-Hübner, Lothar Fritsch and Charles Raab (Springer, 2016), 76–91.

122 ElShekeil and Laoyookhong (n 48).

123 Flórez-Revuelta et al (n 3).

124 President's Council of Advisors (n 70).

125 Fahmida Y Rashid 'Don't Get Bit by Zombie Cloud Data', *InfoWorld* (20 April 2017).

126 Harald Gjermundrød, Ioanna Dionysiou and Kyriakos Costa 'Privacy Tracker: A Privacy-by-Design GDPR-Compliant Framework with Verifiable Data Traceability Controls' in *Current Trends in Web Engineering*, eds Sven Casteleyn, Peter Dolog and Cesare Pautasso (Springer, 2016), 3–15, 10.

127 Ibid.

128 Ibid.

129 ElShekeil and Laoyookhong (n 48).

130 Sona R Makker 'Overcoming "Foggy" Notions of Privacy: How Data Minimization Will Enable Privacy in the Internet of Things' (2017) 85 *University of Missouri–Kansas Law Review* 895; see also Marcus Oppit and Peter Tomsu 'Fog Computing' in *Inventing the Cloud Century*, eds Marcus Oppitz and Peter Tomsu (Cham: Springer, 2018), 471–486, 473 ('Both Fog and Edge Computing push intelligence and processing power closer to the source of data where the sensors are located. The key difference between both approaches is where intelligence and computing power is finally placed. Fog computing pushes the intelligence into the local area edge network, being a part of the complete network architecture … Edge computing pushes the intelligence and processing power as well as communication capabilities of an edge gateway or appliance into programmable automation controllers (PACs).').

131 Makker (n 130) 895.

132 Ibid.; Andrew Meola 'The Roles of Cloud Computing and Fog Computing in the Internet of Things' *Revolution, Business Insider* (20 December 2016). Available at: www.businessinsider.com/internet-of-things-cloud-computing-2016-10.

133 Makker (n 130) 895.

134 Rhys Dipshan 'The IoT Ambiguity: Secure Architecture, Vulnerable Data' *Legal Tech News* (2 February 2018). Available at: www.law.com/legaltechnews/sites/legaltechnews/2018/02/02/the-iot-ambiguity-secure-architecture-vulnerable-data/; Crabtree et al (n 41) 39.

135 Makker (n 130) 895.

136 Ibid at 903.

137 ENISA (n 38).

138 Ibid.

139 Office of the Privacy Commissioner of Canada (n 39).

140 Ibid.

141 Steven Roosa 'A Deep Dive into the Privacy and Security Risks for Health, Wellness and Medical Apps' (6 April 2015). Available at: https://iapp.org/news/a/a-deep-dive-into-the-privacy-and-security-risks-for-health-wellness-and-medical-apps/.

142 Office of the Privacy Commissioner of Canada (n 39).

[143] MB Barcena How Safe is Your Quantified Self? Symantec. Available at: www.symantec.com/content/dam/… /how-safe-is-your-quantified-self-en.pdf.

[144] Ibid.

[145] Ibid.

[146] Ibid.

[147] John Lindstrom 'Security Challenges for Wearable Computing a Case Study' in 4th International Forum on Conference International Forum on Applied Wearable Computing (Tel Aviv, Israel, 2007).

[148] Prakash Shrestha and Nitesh Saxena An Offensive and Defensive Exposition of Wearable Computing, (2018) 92(1) *ACM Computing Surveys* 2.

[149] Lindstrom (n 147).

[150] Ibid.

[151] Ibid.

[152] Mahmudur Rahman, Bogdan Carbunar and Madhusudan Banik 'Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device' (2013). Available at: https://petsymposium.org/2013/papers/rahman-health.pdf.

[153] Ibid.

[154] Martin H Weik 'Access Control' in *Computer Science and Communications Dictionary* (Boston, MA: Springer, 2001).

[155] Umesh Hodeghatta Rao, Umesha Nayak 'Access Controls' in *The InfoSec Handbook*, eds Umesh Hodeghatta Rao and Umesha Nayak (Apress, 2014), 63–76, 64.

[156] Ibid.

[157] Ibid.

[158] Ibid at 63.

[159] Corey Ashby, Amit Bhatia, Francesco Tenore and Jacob Vogelstein, 'Low-cost Electroencephalogram (EEG) Based Authentication' *5th International IEEE/EMBS Conference on Neural Engineering* (Cancun, Mexico, 2011), 442–445.

[160] John Chuang, Hamilton Nguyen, Charles Wang and Benjamin Johnson 'I Think, Therefore I am: Usability and Security of Authentication Using Brainwaves' in *Financial Cryptography and Data Security*, eds Andrew A Adams, Michael Brenner and Matthew Smith (Springer, 2013), 1–16.

[161] YS Soni, SB Somani and VV Shete 'Biometric User Authentication Using Brain Waves' *2016 International Conference on Inventive Computation Technologies* (ICICT)(Coimbatore, India, 2016), 1–6.

[162] Muhammad Shahzad and Munindar P Singh, 'Continuous Authentication and Authorization for the Internet of Things' (2017) 21 *IEEE Internet Computing* 86.

[163] Shrestha and Saxena, (n 148).

[164] Cory Cornelius, Ronald Peterson, Joseph Skinner, Ryan Halter and David Kotz 'A Wearable System that Knows Who Wears It' in *Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys'14)* (Bretton Woods, New Hampshire, 2014): 55–67.

[165] Alvaro Muro-de-la-Herran, Begonya Garcia-Zapirain and Amaia Mendez-Zorrilla 'Gait Analysis Methods: An Overview of Wearable and Non-wearable Systems,' Highlighting Clinical Applications, (2004) 14 *Sensors* 3362; S. Sprager, MB Juric 'Inertial Sensor-Based Gait Recognition: A Review' (2015) 15 *Sensors* 22089.

[166] Po Yang, Dainius Stankevicius et al 'Lifelogging Data Validation Model for Internet of Things Enabled Personalized Healthcare' (2018) 48 *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 50.

[167] Rao and Nayak (n 155) 63–76.

[168] Elena Ferrari, 'Access Control' in *Encyclopedia of Database Systems*, eds Ling Liu, M Tamer Özsu (New York, New York: Springer, 2014).

[169] Shahzad and Singh (n 162) 86, 88.

[170] Ibid.

171 Ibid.

172 Ibid.

173 Ibid at 88.

174 US Federal Trade Commission (FTC), Careful Connections: Building Security in the Internet of Things (January 2015). Available at: www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf.

175 US Federal Trade Commission (FTC), Internet of Things: Privacy & Security in a Connected World (January 2015). Available at: www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

176 Pethuru Raj and Anupama C Raman *The Internet of Things: Enabling Technologies, Platforms, and Use Cases* (Taylor and Francis, 2017), 337.

177 US Federal Trade Commission (n 174).

178 Ibid.

179 See generally, Christopher Soghoian 'Not an Option: Time for Companies to Embrace Security by Default' *Arstechnica* (8 September 2011). Available at: https://arstechnica.com/tech-policy/2011/08/not-an-option-time-for-companies-to-embrace-security-by-default/.

180 Madhan Kanagavel 'Security by Default – Five Principles for Building More Secure Apps' *Enterprise Innovation* (23 August 2018). Available at: www.enterpriseinnovation.net/article/security-default-5-principles-building-more-secure-apps-2017033942/page/0/1.

181 See Liane Colonna *Legal Implications of Data Mining: Assessing the European Union's Data Protection Principles in Light of the United States Government's National Intelligence Data Mining Practices* (Tallin: Ragulka, 2016).

182 Joel W Branch, Chris Giannella, Boleslaw Szymanski, Ran Wolff and Hillol Kargupta 'In-network Outlier Detection in Wireless Sensor Networks' (2013) 34 *Knowledge and Information Systems* 23.

183 Joseba Quevedo, Diego GarciaVicenc et al 'Sensor Data Validation and Reconstruction' in *Real-time Monitoring and Operational Control of Drinking-Water Systems*' eds Vicenç Puig, Carlos Ocampo-Martínez et al. (Springer, 2017), 175–193.

184 Ivan Miguel Pires, Nuno M Garcia, Nuno Pombo, Francisco Flórez-Revuelta and Natalia Díaz Rodríguez 'Validation Techniques for Sensor Data in Mobile Health Applications' *Journal of Sensors* (2016); see also Deze Zeng, Song Guo, Zixue Cheng, 'The Web of Things: A Survey' (2011) 6 *Journal of Communications* 424.

185 Branch et al (n 182) at 23.

186 Theodore Roszak, *The Cult of Information* (University of California Press, 1986), 95.

187 Ibid.

188 Nicholas Diakopoulos and Sorelle Friedler 'How to Hold Algorithms Accountable', *MIT Technology Review* (17 November 2016).

189 Colonna (n 181).

190 Gehan Gunasekara 'The "Final" Privacy Frontier? Regulating Trans-border Data Flows' (2007) 17 *International Journal of Law and Information Technology* 147.

191 Quevedo et al (n 183) 175–193.

192 Ibid.

193 Pires et al (n 184); see also Zeng et al (n 184) 424.

194 Yongzhen Zhuang, Lei Chen, X Sean Wang, Jie Lian 'A Weighted Moving Average-based Approach for Cleaning Sensor Data' in *27th International Conference on Distributed Computing Systems* (ICDCS '07) (Toronto, Ontario, 25–27 June 2007).

195 Urquhart, Lodge and Crabtree (n 41).

196 Paul Daugherty 'The Rise of Digital Ecosystems in the "We Economy"' *Forbes* (9 March 2015). Available at: www.forbes.com/sites/ciocentral/2015/03/09/the-rise-of-digital-ecosystems-in-the-we-economy/#401b2c655514.

197 W Nicholson Price II ‘Black-Box Medicine’ (2015) 28 *Harvard Journal of Law and Technology* 419.

198 Ibid.

199 See IMB White Paper ‘Integrating and Governing Big Data’. Available at: www-950.ibm.com/events/wwe/grp/grp037.nsf/vLookupPDFs/Integrating_Governing_BigData/$file/Integrating_Governing_BigD

200 President’s Council of Advisors (n 70).

201 See eg, the papers submitted to the *2nd International Workshop on Accountability: Science, Technology and Policy, MIT Computer Science and Artificial Intelligence Laboratory (29–30 January 2014)*. Available at: http://dig.csail.mit.edu/2014/AccountableSystems2014/.

202 Christopher Wolf and Jules Polonetsky ‘Future of Privacy Forum, An Updated Privacy Paradigm for the “Internet of Things”’ (19 November 2013). Available at: www.futureofprivacy.org/wp-content/uploads/Wolf-and-Polonetsky-An-Updated-Privacy-Paradigm-for-the-’Internet-of-Things’-11-19-2013.pdf.

203 D'Acquisto et al (n 46).

204 Ibid.

205 Daniel J Weitzner ‘The Jurisprudence of Accountability’. Paper presented at *2nd International Workshop on Accountability: Science, Technology and Policy, MIT Computer Science and Artificial Intelligence Laboratory (29–30 January 2014)*. Available at: http://dig.csail.mit.edu/2014/AccountableSystems2014/.

206 Lalana Kagal ‘Designing for Accountability: A Checklist for Accountable Information Systems’. Paper presented at *2nd International Workshop on Accountability: Science, Technology and Policy, MIT Computer Science and Artificial Intelligence Laboratory (29–30 January 2014)*. Available at: http://dig.csail.mit.edu/2014/AccountableSystems2014/.

207 Ibid.

208 Ibid.

209 Ibid.

210 Ibid.

211 Ibid.

212 Ibid.

213 Voigt and von dem Bussche (n 25) 31–86 citing Simitis S (ed) *Bundesdatenschutzgesetz*, 8th edn, Nomos: Baden-Baden.

214 Christoph Bauer, Frank Eickmeier and Anna Täschner ‘White Paper: What Are the Changes Regarding Data Protection in the Future General Data Protection Regulation?’ ePrivacy GmbH (Hamburg, 2017). Available at: www.eprivacy.eu/fileadmin/Redakteur/News/Whitepaper_GDPR.pdf.

8

Public Registers Caught between Open Government and Data Protection – Personal Data, Principles of Proportionality and the Public Interest

GEERT LOKHORST[1] AND MIREILLE VAN EECHOUD[2]

Abstract

For governments across the globe, public registers are an increasingly popular means to help achieve a range of objectives. These include safeguarding the independence of judiciary, upholding food hygiene and safety standards, fostering proper use of subsidies, and protecting the public from unqualified professionals. Most public registers are subject to data protection laws because they contain some form of personal data. In the Netherlands, the number of online public register has risen dramatically. On the basis of exploratory research on Dutch public registers, we hypothesised that governments easily assume that public registers serve their designated goals, but rarely adequately assess their effectiveness. A comprehensive analysis of registers confirms that hypothesis is correct. This is problematic from the perspective of the EU's General Data Protection Regulation (GDPR) and the human right to privacy as enshrined in, for example, Article 8 of the European Convention of Human Rights (ECHR). Both require that the means used to serve a (legitimate) purpose are proportionate to the (potential) privacy harms. Based on the experience in the Netherlands, in this chapter we query to what extent and by which means policy and lawmakers actually test effectiveness of public registers and analyse the privacy implications from the perspective of proportionality. The adoption of open government policies combined with technological possibilities result in a strong growth of online public registers, and possibilities to link data from multiple sources multiply. The potential privacy impacts on individuals need to be better understood and safeguarded already at the design stages of public registers.

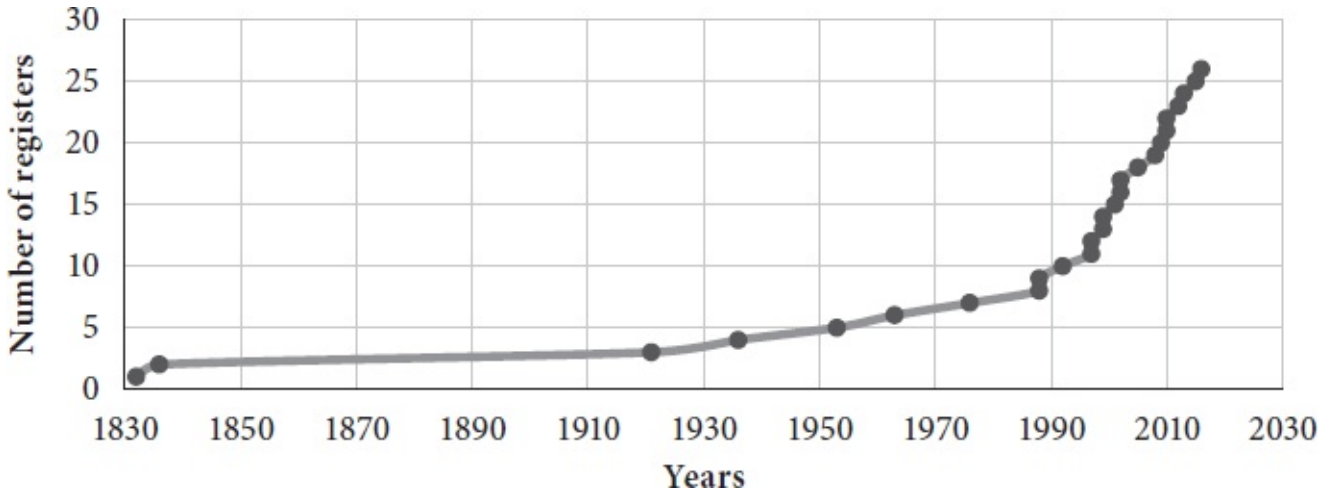
Keywords

Public register, personal data, privacy protection, government, processing, open, transparency.

I. The Growth of Public Registers

Public registers serve a variety of societal interests and have been in existence for centuries.[3] In the Netherlands, among the oldest national registers still operative today are the land registry (*Kadaster*, 1832) and the companies register (*Handelsregister,* 1921). These and other public registers are created and operated based on specific laws. The number of registers has grown slowly for a century and a half, only to explode in the past 20 years or so (see Figure 8.1). In part this is caused by EU law. Various recent and planned registers are the direct result of EU Directives, including the register of interpreters and translators and the forthcoming ultimate beneficial owners register.[4] The majority of recent registers involve the (online) publication of names of natural persons active in certain professions. The upward trend seems to continue. Currently discussed in Dutch Parliament are, among others, registers for mediators,[5] ultimate beneficial owners of legal persons,[6] fireworks experts[7] and professionals in building quality assurance.[8]

Figure 8.1 Growth of public registers contaning personal data in the Netherlands



Virtually all public registers can now be accessed online, greatly enhancing the accessibility of (personal) information contained in them. For example, if anyone wants to know if an incapacitated person domiciled in the Netherlands is under legal guardianship, all it takes is to key in last name and date of birth in the online register. Curious as to whether your local doctor has been subject of disciplinary measures? Simply download a list from the healthcare providers' register. Wondering how many square metres your boss' apartment is? The national building and addresses register returns data on size, type of dwelling, building year and a unique identifier (enabling access to ownership data in the land registry), if one performs an address search or uses the map tool.

Registers must comply with privacy and data protection law, in the EU especially with the GDPR and national implementing legislation.[9] There is no comprehensive research on whether they do. It may seem reasonable to assume that privacy and data protection concerns are consistently addressed by policymakers at the design stage of registers. An exploratory survey of the legislative record raised doubts as to whether this is indeed the case. On the basis of the exploratory research, we hypothesised that governments and lawmakers (a) easily assume that public registers serve their intended purposes and that these purposes justify the disclosure of personal information, and (b) rarely adequately assess their

effectiveness and actual impact on privacy. We then did an extensive survey of official records on Dutch public registers. What does the legislative record show about if and how Dutch authorities weigh the purposes served by a public register against the right to privacy and data protection? The relevant laws at the fundamental rights level include Article 10 of the Dutch constitution, Article 8 ECHR and, for EU-based law, also Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFREU).[10] The relevant data protection laws are the General Data Protection Regulation and prior data protection laws.[11] When looking at if and how privacy interests were considered, the focus was on requirements of proportionality that flow from the fundamental right to privacy and the GDPR. What we found is that the official record, if at all, often shows evidence of a very superficial balancing of privacy interests, ex ante or ex post.

An in-depth description of all the characteristics (legal, operational, technical) of all public registers is outside the scope of this chapter. We will highlight some design aspects because the way in which (personal) information is disclosed affects the potential for privacy harms. Other data protection aspects (ie on data security, the rights of data subjects or enforcement) are not discussed.

The chapter is structured as follows. After first explaining concepts and methodology (Section II), we elaborate on the requirement of proportionality (Section III). Section IV discusses findings of the empirical research for four categories of public registries in more depth. Section V concludes.

II. Concepts and Methodology

This section gives background to the (legal) concepts used and the methodology for the empirical research. With respect to concepts, we delineate what we mean by public registers and explain how these can be categorised on the basis of public interest goals pursued (II.A). Next, Section II.B sets out how the inventory and selection of public registers was constructed, and which resources were used for the analysis. Finally, in Section II.C we reflect a little more on the public nature of registers and what this means in a networked environment before we take a closer look at proportionality requirements in Section III.

A. Public Registers and their Purposes

For our purposes, the term public registers denotes: *systematic collections of information, that are accessible to the (general) public, held by public authorities, contain personal data and are intended to provide (some) information on natural persons*. For this chapter we studied 27 such national registers. There are many more registers held by public authorities, but personal information in those is either incidental or not publicly available (see Section II.B on selection). The idea was that for registers *designed* to give *public* access to *personal* information, one is more likely to find evidence of reflection on the need for these registers, on their effectiveness and on balancing potential privacy and data protection harms. If little

attention was given to privacy and data protection interests in the design and operation of these registers (and, as noted, our exploratory research indicated that this is indeed the case), it seems likely that this is even less so for other registers. Of note, the fact that a public register does not fit our definition does not mean it has no bearing on privacy. Registers such as the abovementioned building and addresses register (which does not contain names of persons, or person identifiers), may have privacy implications because data from it can be combined with other public information, such as title to real estate from the Land Registry and thus enable identification of an individual.

Broadly speaking, the primary goal served by public registers studied here can be categorised as promoting:

(1) Accountability in the public sector: registers that help ensure the integrity of public offices, (eg through disclosure of ancillary positions of court officials, government ministers, registers of gifts and donations received by Members of Parliament).
(2) Economic and social transparency: registers that promote legal certainty in (commercial) transactions, attenuate information asymmetries between market actors (market regulation) and/or help maintain quality standards in a particular domain (eg healthcare).

These purposes have been assessed on the basis of relevant regulations and legislative records of the selected registers. These were then grouped according to similarity of purpose, as this allowed for a higher-level assessment of proportionality aspects. We will elaborate on these categories in Section IV.

B. Methodology

With respect to the survey, an initial set of 300 registers were identified by searching for legal instruments that regulate registers. The Dutch legislator itself recognises that a specific legal basis must exist for registers containing personal data.[12] Since legislative and parliamentary records and all legislation in force is accessible online (dating back to 1815), this produced a complete picture.[13] Further searches of key websites across government were carried out in the event not all public registers turned out to be regulated through (delegated) legislative acts or mentioned in the parliamentary records.[14] The resulting set was then validated against the Dutch government's own inventory, which can be found on the website of the Dutch Government Reference Architecture (*Nederlandse Overheid Referentie Architectuur – NORA*).[15] No additional registers were identified. The set was narrowed down to exclude those registers in which the inclusion of personal data is incidental. The set was then reduced further by considering only those registers that are publicly accessible. The latter means that registers to which access is limited to 'privileged parties' were excluded, like the central credit information system *CKI*. Also excluded were registers that limit access through technical design, for example, by requiring the keying in of detailed data that are only available to select people (ie unique identifiers combined with other attributes such a date of birth).[16] The resulting list contained 27 registers.

The question if and how the legislature weighs the societal interests of public registers was answered by looking at official parliamentary records. A caveat is in order here. The records do not necessarily give a full picture: it is conceivable, for example, that White Papers or external advice have informed public register legislation but that these documents were not sent to Parliament. In those circumstances it cannot be confidently established if proper consideration was given to questions of effectiveness and/or proportionality. Rather, the issue becomes one of transparency and accountability: should it be visible to the public that privacy interests have been considered?

It is a general principle that the processing of data must be transparent for the data subject (Art 5(1) GDPR) and that the processor is accountable for such transparency (Art 5(2) GDPR). But the GDPR does not, of course, explicitly require that considerations of proportionality are reflected in the legislative record on public registers. The GDPR does not require that a data protection impact assessment carried out by or for a public authority be publicly disclosed. Nor do the specific transparency requirements in Articles 13 and 14 GDPR require publication. The GDPR does provide for general principles on transparency of processing and the purposes of processing.[17] Transparency is highly desirable as it promotes the legitimacy and accountability of government actions, also with respect to compliance with data protection laws.[18] This has also been recognised by the Dutch Senate in 2011, when it carried a motion asking government to ensure that any legislative proposal with privacy implications is accompanied by an explanatory memorandum addressing the need, effectiveness and proportionality of the measures proposed.[19]

It is fair to assume that since public registers almost invariably are instituted by formal legislative acts (ie adopted by Parliament), certainly ex ante privacy concerns are reflected in the legislative record. Of note, older registers may predate data protection legislation, and this explains why the relevant original records do not show there has been debate on the privacy implications. But as will be detailed below, most registers are recent.

C. Publicness in a Networked Society

The digitisation of paper-based public registers, the growth in digital registers and the widespread availability of fast internet connections has changed the ‘publicness’ of registers. From systems of practical obscurity, where one had to physically go to a government office or request documents via post, they have evolved to systems of ubiquitous access, worldwide and instantaneous.[20] Of course, technical means can be used to limit access, for example by using authentication technologies to reserve access to certain specific user groups, by geo-blocking or the use of APIs that prevent large-scale extraction of data. They matter when it comes to protecting privacy. Because we are primarily interested in how public goals served by registers are weighed ex ante against privacy interests, we do not detail how specific registers provide access to personal data. The selection of registers is of *public* registers, and the tendency among Dutch public authorities is not to restrict access.

The creation of public registers has become a standard policy tool since the 1990s. It is not just digitisation that drives this trend, but also new public management policies that see

‘transparency’ as an effective tool for quality control in (notably) regulated professions and semi-public domains. Furthermore, open government and open data policies at national and EU level promote the wide availability of public sector information. ‘Open government’ is a rather loose concept, or perhaps better seen as an ideal to make governments ‘transparent, more accountable, and more responsive to their own citizens’.[21] An important instrument in open government policy is open government data: making data available to all is thought to promote ‘transparency, accountability and value creation’.[22] This notion has gained considerable traction globally and in the EU.

The 2013 Public Sector Information Directive[23] has been revamped into the Open Data and Public Sector Information Directive. It tightens the rules that must ensure more public sector data becomes available for (commercial) reuse by default. It must be implemented by Member States in 2021.[24] Data protection laws and privacy rights must be respected when releasing data for reuse (eg by anonymisation). This assessment tends to be done on a case-by-case basis: does release of this particular data set or using this particular API on that particular public register satisfy data protection rules? The Public Sector Information Directive and the GDPR do not focus on systemic effects that arise when ever more resources become available online, in machine-readable, open formats, which greatly facilitate the linking of data from different sources. Open data policies are designed to promote just that development.

Publication of personal data in a register can have varying effects on the private life of the persons concerned. Names, addresses and unique identifiers from public registers enable third parties to engage in direct marketing but also facilitate significant harms, like identity theft or the making of direct threats.[25] Combining data from public registers with information from other sources may help profiling.[26] The possibility to combine information exacerbates risks, meaning that governments should not assess the impacts of disclosure of personal data in public registers on (just) a case-by-case basis.

That information is accessible *online* has additional privacy implications, as the Court of Justice of the EU (CJEU) noted first in *EDate* and then in *Google Spain*. The fact that (injurious) information is available on a world-wide basis can aggravate the privacy harm.[27] The persistence of information on the internet once released is another factor. Also, that information is publicly available in registers does not mean that subsequent publications are unproblematic. In *Satakunnan Markkinapörssi Oy & Satamedia Oy v Finland*, the European Court of Human Rights (ECtHR) held that the use of already public information on a much larger scale can in itself constitute an interference with the right to private life.[28] In this case, the availability of personal data through a text messaging service was considered an interference with the right to private life, even though this information was readily available at local administrative offices.[29] In *Satakunnan*, ‘downstream’ companies using data from public tax records were the offending party (the Finnish data protection authority and courts had issued orders to desist). While the Court did not have to consider the role of government, it does show that governments may limit re-use of public data if personal data is concerned.

III. Requirements of Proportionality

In this section we look to key principles of the GDPR (or equivalent principles from its precursor Directive 95/46/EC) that are the most relevant for public registers. First, the principle that personal data may only be processed if it complies with one of a limited number of *lawful grounds*; second, that the *purpose*(s) for which processing takes place is legitimate; and third, that such processing (in our setting: public disclosure) is *necessary* to achieve the stated purposes. The 'necessity' requirement will function as a key for applying proportionality standards from Article 8 ECHR and Articles 7 and 8 of the EU's Charter of Fundamental Rights (CFREU) in the GDPR.

A. Lawfulness for Public Register Processing

Lawmakers must establish a lawful ground for the processing of personal data in registers. That lawful ground must also cover publication. Two of the GDPRs lawful grounds are of particular relevance to public registers: compliance with a legal obligation (Article 6(c) GDPR) and performance of a task carried out in the public interest or exercise of official authority (Article 6(e) GDPR).[30] As to the first, the law that imposes the legal obligation must fulfil 'all conditions to make it valid and binding and in compliance with data protection law, including necessity, proportionality and purpose limitation'.[31]

In the absence of a legal obligation, institutions may be able to rely on Article 6(e) GDPR if publication is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.[32] The Article 29 Working Party (the EU's former advisory body of representatives from all national data processing authorities) has stated that institutions will need to consider the public interests served, whether processing is appropriate for attaining the objective pursued and that they further will need to 'bear in mind the various interests at stake'.[33] This suggests proportionality must be assessed.

The legal grounds in Articles 6(c) and (e) overlap to some extent. According to the Working Party, processing based on the (e)-ground should be directly or indirectly based on a legal provision.[34] Furthermore, the Working Party argued that if the processing implies an invasion of privacy, this legal provision should be specific and precise, detailing the data processing allowed under it.[35] Such a legal provision would then also be a legal obligation within the meaning of Article 6(c). However, the Working Party has stated on a different occasion – in its opinion on legitimate interest – that public interest or official authority is 'typically attributed' through statutory or other laws.[36] This could mean that it does not exclude the possibility of processing based on Article 6(e) GDPR in absence of a (specific) legal obligation, but only if the processing of personal data does not imply an invasion of privacy in the sense of Article 8 ECHR.

Consent could, in theory, be a further legal ground, but will be problematic in most cases.[37] After all, public disclosure is often based on statutory laws that oblige the data subjects to provide data (eg land registry, commercial register, health care providers'

register).[38] Even without a legal obligation, to provide data 'voluntarily' or agree to its disclosure will not normally meet the strict standard that the GDPR sets for consent.[39] Consent may be undermined by the negative consequences of not agreeing to provide and disclose personal data (eg if economic duress results).[40] But there may also be cases where consent is an appropriate ground. For example, while interpreters are obliged to register with the Dutch register of interpreters (without registration interpreters will not be hired by large parts of government, including the police, public prosecutor's offices and courts),[41] they are free to refuse public disclosure of their data.

B. Necessity as Proportionality

Processing personal data is bound by a legitimate purpose that must be specified before processing commences.[42] A legal provision mandating disclosure as such does not constitute a legitimate purpose; the GDPR requires a specific purpose for the register legitimising the legal provision mandating a public register. For example: the ancillary jobs register of judges is based on Article 44a of the Act on the Legal Position of Judicial Officers.[43] Its purpose lies in ensuring judicial independence and impartiality, and public trust in the judiciary.[44] Considering the importance of trustworthy, impartial courts for the rule of law, these purposes are legitimate within the meaning of the GDPR. The requirement of 'necessity' is central to the assessment of the legitimacy of processing for Articles 6(c) and (e) GDPR.[45] 'Necessary' presupposes that maintaining a public register is in fact needed for the controller to meet a legal obligation under Article 6(c) GDPR, or to properly exercise a public task under Article 6(e) GDPR.

According to the Article 29 Working Party, the ECtHR approach to 'necessity' should be adopted in the context of the lawful grounds for processing.[46] Under Article 8 ECHR, the proportionality principle follows from the ECtHR's interpretation of the requirement that an interference with the right to private life has to be 'necessary in a democratic society'.[47] The classic three-part proportionality test that the ECtHR applies for all human rights requires (1) that interests have been balanced, (2) that the processing is a suitable means to attain the underlying legitimate (policy) purpose(s) and that (3) the least intrusive means are used.[48] The first two parts will be discussed further below. In a nutshell, the purpose specification and balancing of interests must take place before public disclosure commences.[49] Furthermore, suitability means that public disclosure has to be an effective instrument to obtain the legitimate purpose; an ineffective policy will not be proportionate to the interference it poses.[50] The availability of less intrusive means is less relevant for this study, as it concerns mostly the choices for precise instruments.[51] This step in the analysis focuses more on specific implementation issues (eg modalities of access through restrictive APIs) and not the broader discussion on whether public disclosure as such is proportionate.

The requirements of proportionality apply not only to Article 8 ECHR, but also the right to private life under Article 7 CFREU. Limitations to this right are subject to the general principle of proportionality enshrined in Article 52(1) CFREU. Additionally, Article 52(3)

CFREU explicitly states that the meaning and scope of rights corresponding to those guaranteed in the ECHR should be the same as those laid down by said Convention.

It is debatable whether the requirements for proportionality in Article 8 ECHR also apply to the data protection right. Protection of personal data can be construed as part of the right to privacy of Article 8 ECHR in cases where processing interferes with privacy interests.[52] But not all personal data processing affects privacy. Since the right to data protection of Article 8 CFREU has no equivalent in the ECHR, this suggests the extended application of the ECHR through Article 52(3) CFREU does not apply. However, the *Handbook on European Data Protection Law* issued by the European Union Agency for Fundamental Rights and the Council of Europe states that the proportionality principles applicable to data processing are reminiscent of Article 8(2) ECHR.[53] We therefore assume that proportionality for the data protection right also follows the classic three-part proportionality test.

i. Proportionality as Effectiveness

Embedded in the lawful processing grounds is a requirement that the processing (ie operation of the public register) is an effective means to achieve the purpose it serves. In their report to the Dutch Data Protection Authority, Versmissen and De Heij argue that the legislator should take account of the effects of their policies to assess whether the intended purpose of a public register is actually achieved.[54] It is, therefore, important to assess what is known about the effectiveness of the various public registers. An absence of effectiveness in reaching the legitimate purpose pursued indicates a disproportionate interference in the right to private life and personal data protection.

This approach also finds support in the case law of the CJEU. In *Digital Rights Ireland*, the referring domestic court queried whether the Data Retention Directive, requiring storage of all telephone traffic and location data, was not just disproportionate, but also inappropriate to achieve the aims pursued.[55] The CJEU answered that proportionality entails, among others, that the interference need to be appropriate for attaining the legitimate objectives pursued.[56] Applied to public registers, the disclosure of personal data must be suitable for attaining the desired policy purpose. That is: if a measure does not provide actual opportunities to achieve the public interest (ie it is not effective) it cannot be seen as an appropriate tool to attain the objective.[57] This is also evident from the CJEU's *Huber* case,[58] which revolved around the question whether plans to centralise pre-existing population registers are 'necessary' to facilitate application of residential laws and for statistical purposes.[59] The Court held that this is so if 'its centralised nature enables that [residence] legislation to be more effectively applied …'[60]

ii. Proportionality and Balance of Interests

A public register should not only be appropriate to obtain the objective, but also proportional in the strict sense: the balance of interests must fall in favour of the purpose served by public disclosure. It is difficult to discern substantive criteria for proportionality as a reasonable

balance between the interference and the rights to private life and personal data protection. Case law of the ECtHR and CJEU are very context specific, relying heavily on suitability and least interfering means instead of a more abstract balance of rights and interests.[61] Still, the CJEU concluded in the case of *Volker und Markus Schecke and Eifert* – on the publication of the names of recipients of EU agricultural subsidies – that institutions are obliged to balance the interests prior to disclosure.[62] This has also been stressed by the Dutch Senate. Just after publication of the *Volker und Markus Schecke and Eifert* case, the Senate carried a Motion that explanatory memoranda to legislative proposals should contain, inter alia, information on necessity, effectivity, proportionality, and the results of a data protection impact assessment.[63]

The need to take the interests of data subjects into account at an early stage also follows from new norms introduced by the GDPR. Data protection by design and by default, as introduced in Article 25 GDPR, obliges the controller to implement appropriate measures at the time of the determination of the means for processing. Furthermore, the controller should carry out an ex ante data protection impact assessment if data processing is likely to result in a high risk to the rights and freedoms of natural persons.[64] This should contain an assessment of the necessity and proportionality of the processing in relation to the purposes.[65] Whilst the assessment is not always mandatory, the Dutch Government has opted to perform such an assessment in all cases where the development of new policies and regulations concern the processing of personal data.[66] As already discussed in the section on methodology, a caveat to these new rules is that there are no requirements to publish the results of data protection by design and impact assessments.

An important aspect to the balance of interests is the question whether publication should necessarily be in the form of an online publication. The Article 29 Working Party argues it is necessary to consider the potential risk of online disclosure.[67] The Dutch DPA insists that public bodies should reflect on the question whether publication should always mean publication on the internet.[68] An obligation to publicly disclose personal data does not automatically mean that it should be available online,[69] let alone in a form that allows easy bulk retrieval. Offline access comes with practical limitations which may limit the extent to which data is actually disseminated. Online availability without strict access limitations may lead to a much wider distribution, even if this is not strictly necessary to achieve the register's purposes. Furthermore, online accessibility facilitates the combination of personal data from multiple sources. This means that there can be further proportionality issues with online publications. This is especially important for registers that have existed since before the advent of the internet and are now increasingly migrated online.

If we look to Dutch Government practice, disclosure of data in public registers can range from online publication of datasets in downloadable CSV- or XML-format, to more limited disclosures through APIs, requiring input of last names or other identifiers. How robust such technical measures are is another matter. A 2017 study found that many registers that list professionals for purposes of qualification checks actually provide more data than is needed to check their qualifications.[70] Researchers used wildcards and SQL-injects to obtain the complete dataset of registered doctors in the Dutch health care providers (so-called '*BIG*-

register') and other registers maintained by government.[71]

IV. Types of Public Registers and their Purposes

Above we identified two broad categories of purposes of public registers. The first category is primarily concerned with ensuring (political) accountability of public institutions and, through such openness, promote trust in the legislature, judiciary and executive branches of government. Registers in this category are concerned mostly with the integrity of public offices. The second broad category is concerned with economic and social domains: to promote legal certainty in (commercial) transactions and attenuate information asymmetries between market actors (market regulation), and/or help maintain quality standards in a particular domain. Here we discuss in a little more detail examples of registers in both categories and the extent to which their creation and further existence is supported by sufficient privacy and data protection considerations.

Of note, public registers may predate modern data protection norms following from the GDPR and its predecessor, the European Data Protection Directive 95/46/EC. The Dutch Data Protection Act (*Wet bescherming persoonsgegevens*) of 1998 implemented Directive 95/46/EC and also applied to public registers. The earlier Data Protection Act of 1989 (*Wet Persoonsregistratie*), however, explicitly excluded public registers from its scope. The explanatory memorandum to that Act stated that the law should not apply to registers because 'in these cases, the legislator has decided that these registers are intended for publicity.'[72]

A. Accountability in the Public Sector

Dutch public registers on government transparency that disclose personal data are mostly registers on ancillary jobs held by politicians and judges. These are the ancillary jobs registries for Members in both houses of Parliament, the European Parliament, the Provincial Executive, the board of the *Waterschappen* (regional authorities tasked with water management), mayors and aldermen and judges.[73] In addition, publication is required for gifts and foreign travels subsidised by third parties for politicians in the *Tweede Kamer* (Lower House of Parliament).[74] Most of these registers have existed for quite some time, but have only fairly recently been regulated in (delegated) acts. For example, the publication of ancillary jobs for Members of parliament exists since 1976 but was only formalised in the rules of procedure (*Reglement van Orde*) in 2002.[75]

i. Purposes

Two arguments recur in the parliamentary record: to prevent conflict of interests or the appearance of such conflict, and to assess whether an ancillary job compromises the exercise of a public function.[76] There has been some discussion in Parliament on the need to balance

privacy interests of registered persons with transparency interests,[77] but hardly any on later decisions to make the registers freely available online. For example, the legal history of the judges' register merely states that the register should be placed on the internet because trust in the judiciary benefits from maximum publicity.[78] It does not provide any reasoning on what this 'maximum publicity' may entail for data subjects.

ii. Effectiveness and Proportionality

With respect to effectiveness of the register, the absence of evaluations is conspicuous. Only the judges' register has been evaluated, but that did not include questions of effectiveness of the disclosures in relation to the interferences with privacy and data protection.[79] The evaluation reported that registers maintained by local courts were often incomplete, outdated or merely described an ancillary job vaguely, such as 'member of a Supervisory Board'.[80] The register was centralised and standardised in reaction to the evaluation, to provide greater transparency.[81] News magazine *De Groene Amsterdammer* reported similar issues for the registers of public officials in decentral government.[82] As such, it seems that these registers are sparsely regulated. There is some anecdotal evidence that the media use the jobs registers; for example, newspaper *Brabants Dagblad* regularly advertises any ancillary jobs such as mayor in the Brabrant province.[83] However, the absence of publicly available information of the suitability of these registers makes it impossible to assess whether they are actually proportional.

B. Economic and Social Transparency

In this broad domain we find registers that promote legal certainty in (commercial) transactions and attenuate information asymmetries between market actors (market regulation) and/or help maintain quality standards in a particular domain. Based on the type of information contained, a further distinction can be made in registers focusing on:

- professional qualifications
- financial information and
- legal representation of persons and companies.

i. Professional Qualifications

The registers dealing with professional qualifications have grown considerably in numbers the past decades. Of 15 registers, 13 date from the late 1980s and six were created this last decade, long after EU data protection law was in place.

(a) Purposes

A particular register may be informed by subsets of goals. For example, the register of health

care providers such as doctors, nurses, physiotherapists and dentists serves more than one purpose. It informs (prospective) patients on who is qualified to provide a certain service. This attenuates information asymmetries. But the register is also supposed to help maintain quality standards in the regulated professions. In order to keep a valid registration, health care providers must show evidence of continued training and comply with other quality standards. The disciplinary measures taken against health care providers are also publicised, not only to warn patients (and prospective employers, health insurance companies and the like), but also to act as a punishment. In fact, many of the public registers on regulated professions serve such a mixture of these three goals.

An exception to the rule that public registers have a clear legal basis is the 'social hygiene register'. The Minister of Health should have appointed an organisation to maintain a register of workers in hospitality with food and drink safety certificates and regulate it.[84] The examination board for social hygiene certificates *LEC-SVH* took up the task, without having been officially appointed.[85] The register is currently accessible to everyone, although the law stipulates that it is meant only for relevant civil servants and mayors. The legislative record states that the Minister will make a privacy assessment, but there is no clear sign that this has been done.[86]

(b) Effectiveness and Proportionality

The situation for the category of 'professionals registers' is quite typical of results found for other registers. In half the cases, the legal history is silent on the relation between the purpose of the register and privacy and data protection. This is true for the auditors register, the architects register, the social hygiene register and the bailiffs register. Some of these pre-date the European data protection norms and the earlier Dutch Persons Registration Act of 1989 (*Wet Persoonsregistratie*) categorically excluded public registers from its scope.[87] All that can be found in the legal history of the notaries register is a statement that 'it goes without saying that the register must be public'.[88]

A number of older registers have been supplemented with a purpose specification (eg to inform interested parties) following the implementation of the Data Protection Directive, but without any further assessment of proportionality.[89] Of note, four registers created after the implementation of the Data Protection Directive still lack a visible assessment on purpose and proportionality.

For one-third of registers evidence of some balance of interests exists. On the register of forensic experts, the former Minister of Justice argued that disclosure should be based on consent of the registered persons (one may ask whether forensic experts are really free to withhold their consent, if doing so has economic ramifications),[90] and that disclosure is necessary to inform potential clients about experts' qualifications.[91] The same reasoning is used for the register of youth care professionals: public disclosure is deemed necessary to assess which professionals qualify for certain tasks.[92] As such, the human rights interferences of these registers are deemed proportionate as the only way for the public to ascertain the qualifications of professionals. However, this does not explain why enabling the public to

ascertain the qualities is necessary for these professionals specifically, but not for other professions. That would come down to a political consideration on the societal value of specific professions, the public role they play and whether this publicity actually serves the public interest.[93] It also depends on the question to what extend citizens should be ascertaining these qualifications and not government institutions charged with safety in certain professions.

Public disclosure of disciplinary actions is also balanced in some cases. Disclosing disciplinary actions in the veterinary register is only deemed justified if it concerns a total or partial prohibition to practice veterinary medicine.[94] The central advocates register contains a similar balance.[95] The former Junior Minister of Justice Teeven argued that disclosing all disciplinary actions would result in a disproportionate interference with privacy.[96] Teeven argued that disclosure is only necessary for clients to assess whether certain advocates may still perform their profession.[97] The situation is very different with respect to the disclosure of disciplinary actions in the doctors register. In this case, all disciplinary actions are made public. The then Minister of Health, Schippers, argued that it ensures that patients, employers and stakeholders are better informed,[98] so the right to know must trump privacy and data protection interests.[99] This does not seem to be a weighing of interests, but merely a choice for the preferred policy.

Overall, formal evaluations and studies on the effectiveness of professional qualifications registers are rare. The healthcare providers' register is an exception. Research shows that patients hardly ever ask medical professionals about their registration.[100] Research carried out for the national medical sciences funding agency concluded that of the respondents who knew about the healthcare providers' register (N = 542), 83 per cent of respondents had never used it.[101] Eight per cent stated that they had used the register when choosing a new health care professional.[102] Of note, registration is seen as the least important factor when choosing a new professional.[103] Research institute Nivel questioned a larger group of respondents (N = 862) and concluded that a mere 1.4 per cent of respondents looked at the register when choosing a new health care professional.[104] This does not seem to be an impressive number, particularly as the register covers virtually all types of health care professionals, not just general practitioners (family doctors) with whom the patient may already have a long-standing relationship. Part of the stated goals discussed above is to promote quality of health care provision by empowering citizens with information. If, in effect, registers are used so little, one might ask if they are effective instruments.

ii. Financial Information

Another type of register provides financial information to promote legal certainty. These registers aim to reduce risks for potential contracting parties.[105]

(a) Purposes

This purpose is not necessarily made explicit in the relevant regulatory instruments but can be inferred from the register's effect. The legal guardian register (*Curateleregister)* discloses who is legally incapacitated; the receivership register (B*ewindregister*) warns creditors about problematic debtors, meaning creditors unable to enforce their claims through a court procedure;[106] and the insolvency register (*Faillissementsregister*) informs creditors that natural persons no longer have power of disposition on their property.[107] Similarly, the prenuptial agreement register informs creditors about marital conditions, which may limit the power of disposition of one spouse regarding goods owned by the other spouse.[108] These registers all inform (potential) creditors about the restraints put upon the natural person they have or may want to have economic relations with. The legal restraints and receivership registers have the secondary function of protecting the registered subject from creating further debts.[109]

Public disclosure of the land registry similarly has the purpose of ensuring 'an equal information position between parties'[110] involved in real estate transactions. It details ownership, as well as mortgages and other security interests attached to a property.

Of a somewhat different nature are the two registers held by the Financial Markets Authority (*AFM)* with information on management owned shares and other financial products. Disclosure of such information has the purpose of minimising asymmetric information between managers, directors and supervisory directors and other (potential) shareholders.[111] This only promotes trust of (potential) shareholders and other investors in the company, but also functions as a remedy against insider trading.[112] These registers are, therefore, somewhat different than the others in this category as they seek to promote both a level playing field in the stock market and honest trading.[113]

(b) Effectiveness and Proportionality

The public records are almost completely silent on the privacy and data protection interests pertaining to financial information registers. Only with regard to the legal restraints and receivership registers does the legislative record state that privacy and date protection interests are outweighed. In these cases, disclosure is also deemed to be in the data subject's financial interests.[114] The legal history of the insolvency register, the Land Registry, the register on shares and other financial products held by (supervisory) directors remain silent. The *AFM* register on transactions by managers would at first remain closed due to privacy interests, only to disclose it anyway 'to align the system with the Anglo-Saxon model'.[115] It is also questionable whether the purpose of this register is to provide information in trade at all or only to check upon illegal insider trading. Public disclosure would perhaps not be necessary in the second case, as long as the *AFM* remains informed.[116]

As to the effectiveness of the public registers, this does not seem to be questioned by lawmakers and policymakers. Legal certainty is certainly served by the Land Registry because registration of deeds is required for transfer of property to have effect. Other registers produce legal effects too (eg by limiting the ability of creditors to make certain claims in court).

iii. Legal Representation of Persons and Companies

A smaller but relatively old set of registers, these inform the public about their capacity to act on behalf of a natural or legal person (eg a company, foundation, association, etc.). The commercial register discloses the names of directors and other authorised representatives of a company.[117] The guardianship register details which persons (parents, guardians) have the legal power of representation over minors.[118] These registers provide legal certainty in trade by providing information on the representatives of a natural or legal person and related risk liability.[119] Legal certainty as a legitimate purpose for disclosure in commercial registers has been recognised by the CJEU in *Camera di Commercio v Manni*.[120] To improve his chances in business, Salvatore Manni sought to have information about prior bankruptcies removed from the commercial registers.[121] For this he relied on data protection law – including the 'right to be forgotten' as elaborated in *Google Spain and Google*.[122] The CJEU held that the publication of personal data was necessary for the commercial register to serve the purpose of legal certainty;[123] not just for creditors, but also for potential trade partners of other companies which Manni represented as a director.[124]

(a) Effectiveness and Proportionality

The public records show no evaluation or other research on the effectiveness of these registers. Registers preceding the Data Protection Act (*Wet Bescherming Persoonsgegevens*) generally lack a balancing of the public interest in disclosure and the rights to private life and personal data protection. This is also the case for the commercial register. The only mention made on necessity of disclosure at all is in 1983. Former Minister of Justice Korthals Altes argued that disclosure is necessary to have certainty about the natural persons that have decisional or representational authority over a company or other legal person.[125] No balancing of proportionality can be found in later amendments, including the amendment of 1997 which made the commercial register electronically accessible.[126] The explanatory memorandum to the overhaul of the Commercial Register Act in 2007 merely mentions that the Data Protection Directive applies to the Commercial Register.[127] It does not provide a discussion on the balance between data protection and disclosure in the public register.[128] As a matter of interest, The Dutch DPA (*Autoriteit Persoonsgegevens*) announced in August 2018 that the Dutch Chamber of Commerce (*KvK*), responsible for maintaining the Commercial Register, may even violate European data protection laws by providing advertisers access to personal data from the register.[129]

C. Findings

Overall, the legislator seems to make little effort to set out the purpose(s) of a particular register and what considerations inform the decision to fashion access in a certain way. Both in the relevant regulations and in the public record, the purpose of registers tends to be described very briefly and in general terms. The land registry is a clear example. The relevant

act states that the purpose of this register is to promote legal certainty regarding registered real property and to support and promote economic activities.[130] While it may be impossible to provide all specific purposes, this general description for the land registry could be considered the other extreme.[131] A lack of specific purposes means that it is difficult to assess what processing operations are compatible with the legal basis.[132]

Also noteworthy is the fact that the published legislative record (ie legislative proposals and explanatory memoranda, reports of parliamentary debates in both houses of parliament, outcome of public consultations and official reviews of registers) hardly ever testifies to a considered balancing of interests between the interests served by disclosure and countervailing privacy and data protection interests. It may not come as a surprise that on the issue of effectiveness of registers – do they achieve the public interest purposes they are meant to serve – few actual assessments seem to take place. As we have seen, where effectiveness has been reviewed, the outcome tends to be disappointing. Evaluations of the health care providers' register shows that patients hardly ever use it in their choice for a professional.[133] We elaborate on possible reasons for such outcomes below.

The absence of a substantive balance of interests in public legislative record is, in part, due to the long legal history of some public registers. Public registers have been in existence since as early as the sixteenth century.[134] Some public registers currently in existence have preceded more modern interpretations of privacy and data protection discussed in Section III. These include the application of Article 8 ECHR in the context of personal data;[135] the implementation of the Personal Data Protection Directive in the Dutch Data Protection Act in 2001;[136] and the CJEU's 2010 decision in *Volker und Markus Schecke and Eifert* that a disclosure of personal data should be preceded by a balance of interests.[137] Prior to the creation of EU data protection laws, the Dutch Persons Registration Act of 1989 (*Wet Persoonsregistratie*) also categorically excluded public registers from its scope without providing a balance of interests in this regard.[138]

Old registers, therefore, often lack extensive discussions on privacy and data protection. These should still comply with modern EU data protection laws. This has also been recognised by the Dutch legislator: during the implementation of the Data Protection Directive 95/46/EC, some purpose specifications were introduced for some – but not all – public registers already in existence.[139] The implementation would have been a great opportunity to show transparency about the proportionality of these registers. However, this did not happen. Neither did this occur during the entry into force of the CFREU or the implementation of the GDPR. As such, a broader review of the older registers may be expedient to assess compliance with current privacy and data protection standards. This may be even more important in view of the risks posed by the combined use of public registers or public registers and other public information. We found hardly any discussion about the risk the combined use of public registers might impose on privacy and data protection.

V. Conclusions

The empirical analysis of Dutch public registers and the relevant legislative records indicates there is a persistent lack of attention for the question whether the objectives pursued by public registers justify the potential privacy harm. Also, government does not seem to assess whether public registers are actually effective instruments, whereas practice suggests they may not be.[140] What is more, to the extent that policy makers do visibly assess the effectiveness, the focus is on one particular register, not on the broader effects it may have because of what it adds to the existing pools of data. Broad empirical analyses of the kind done here, enable us identify trends and potential privacy problems. In a nutshell, the trend is towards more public registers and more online publication. The problems are that insufficient attention is paid to privacy concerns and to the systemic effects of increased availability of public register data. A key requirement in both EU data protection law and fundamental right to privacy (Article 8 ECHR) is proportionality. A public register, in its existence, design and operation, must be necessary (which also implies that it be effective) to achieve its legitimate purpose and not be more intrusive than necessary.

The number of registers that disclose information on citizens (whether in professional roles or not) is substantial and growing. Typically, they can be consulted online. These registers seek to balance information asymmetries on the market, promote trade and legal certainty with respect to (commercial) transactions.[141] However, it is unclear whether they are effective instruments in the pursuit of such goals. Yet new registers are constantly being introduced.

This is all the more worrisome since our research shows what can only be called a persistent lack of reflection by policy and lawmakers on the privacy risks posed by public registers. What justifies the level of ‘publicness’ of public registers is seldom well argued in the legislative record. The existence of older registers is used to justify the appropriateness and proportionality of new ones,[142] without the older registers themselves having been properly assessed on privacy and data protection interests. Some ad hoc interventions based on incidents do occur.[143] It may, therefore, be good policy to regularly assess the compliance of these older registers with current privacy and data protection standards. How they contribute to potential adverse effects of having a network of growing number of online registers is also an issue to consider.

The use of (technological) security measures and access restrictions can obviously mitigate privacy risks. Such restrictions may limit bulk downloads or API limiting the uses that can be made of data. Our focus was not on such modalities of access. We would note, however, that the official records suggest that lawmakers generally pay little attention to these aspects. Shortcomings on the political level may trickle down into the actual design of a public register. This is not to say that government bodies tasked with designing and operating registers do not consider privacy issues in access design at all; but if and how this happens is not transparent.

The consistent use and publication of Privacy Impact Assessments (PIAs) can improve matters. Dutch central government has decided to run PIAs in all instances where a policy is developed, or a regulation proposed, that involves the processing of personal data. This can help improve design choices (what data to include in a register, how to make it available to

the public). It also makes it easier to do ex-post evaluations. PIAs are, however, not necessarily published and the GDPR does not require them to be. Routine publication would be one way to stimulate that careful assessment of privacy implications is made, and to enable public scrutiny.[144] Research on these combined PIAs could also be valuable in identifying systemic risks.

Although the empirical work focused on Dutch public registers, it has broader implications. Public registers increasingly result from EU legislation. Furthermore, EU open government and open data policies, and global initiatives like the Open Government Partnership seek to increase the availability of existing public sector data resources for commercial and non-commercial use in the private sector.[145] Awareness is growing that the vast majority of data sets held by governments contain personally identifiable information, and that on various levels, data protection law is at odds with the notion that data should be 'shared' freely. The increased availability of non-personal, public sector data eventually becomes personal data if it can be linked with an expanding amount of public registers containing personal data (and also private sector sources), adding to the exposure of citizens.

References

Literature

Article 29 Working Party, 'Opinion 01/2012 on the Definition of Consent' (2011) WP 187.

——, 'Opinion 03/2013 on Purpose Limitation' (2013) WP 203.

——, 'Opinion 01/2014 on the Application of Necessity and Proportionality Concepts and Data Protection within the Law Enforcement Sector' (2014) WP 211.

——, 'Opinion 8/2014 on the Notion of Legitimate Interests of the Data Controller' (2014) WP 217.

——, 'Guidelines on Transparency under Regulation 2016/679' (2016) WP 260.

——, 'Opinion 02/2016 on the Publication of Personal Data for Transparency Purposes in the Public Sector' (2016) WP 239.

Ausloos, J 'Giving Meaning to Lawfulness under the GDPR – CITIP Blog' (2017). Available at: www.law.kuleuven.be/citip/blog/2761-2/ (last accessed 17 February 2019).

Bagger Tranberg, C 'Proportionality and Data Protection in the Case Law of the European Court of Justice' (2011) 1 *International Data Privacy Law* 239.

Berlee, A 'Volledige Openbaarheid : Het Doel Voorbij' (2017) 2017 *WPNR* 844.

——, *Access to Personal Data in Public Land Registers, Balancing Publicity of Property Rights with the Rights to Privacy and Data Protection* (Eleven International Publishing, 2018).

'Bijbaan Voor de Burgemeester' *Brabants Dagblad* (2017).

'Burgemeester Wikt, Weegt En Zegt Die Ene Bijbaan Op' *Brabants Dagblad* (16 November 2017).

CBP, 'Actieve Openbaarmaking En Eerbiediging van de Persoonlijke Levenssfeer' (2009).

College Bescherming Persoonsgegevens, 'Publicatievan Persoonsgegevens Op Internet' (2007).

Eshuis, RJJ and Dijkhoff, N, 'Nevenfuncties Zittende Magistratuur' (2000) 185.

European Commission, 'European Legislation on the Re-Use of Public Sector Information | Digital Single Market' (2019). Available at: https://ec.europa.eu/digital-single-market/en/european-legislation-reuse-public-sector-information (last accessed 17 February 2019).

European Union Agency for Fundamental Rights and The Council of Europe, *Handbook on European Data Protection Law* (2014).

Friele, R et al, 'Zorgverleners En Burgers over Het Openbaar Maken van Door de Tuchtrechter Opgelegde Berispingen En Geldboetes'. Available at: www.nivel.nl/sites/default/files/bestanden/Tuchtrecht_impact_van_openbaar_making.pdf (last accessed 19 February 2019).

Frissen, P *Het Geheim van de Laatste Staat Kritiek van de Transparantie* (Boom uitgevers, 2016).
Fung, A, Graham, M and Weil, D, *Full Disclosure: Perils and Promise of Transparency* (Cambridge University Press, 2007).
Gerards J, 'How to Improve the Necessity Test of the European Court of Human Rights' (2013) 11 *International Journal of Constitutional Law* 466.
Hulst, EH, 'Naming En Shaming van Artsen Die Tuchtrechtelijk Zijn Veroordeeld' (2017) 2017 *Tijdschrift voor Gezondheidsschade, Milieuschade en Aansprakelijkheidsrecht* 1.
Kloek-tromp, IJ, 'Kadaster En Privacy in Praktijk' (2017) *WPNR* 853–858.
Lind, A-S and Strand, M, 'A New Proportionality Test for Fundamental Rights?' (2011) 7 *European Policy Analysis* 1–11.
McDonagh M, 'The Protection of Personal Information in Public Registers: The Case of Urban Planning Information in Ireland' (2009) 18 *Information & Communications Technology Law* 19.
Ministry of the Interior and Kingdom Relations, 'Model Gegevensbeschermings- Effectbeoordeling Rijksdienst (PIA)' (2017).
NORA, 'NORA Online'. Available at: www.noraonline.nl (last accessed 19 February 2019).
Oostveen, M, *Protecting Individuals Against the Negative Impact of Big Data: Potential and Limitations of the Privacy and Data Protection Law Approach* (Wolters Kluwer, 2018).
Partnership OG, 'About OGP'. Available at: www.opengovpartnership.org/about/about-ogp (last accessed 19 February 2019).
Rijksoverheid, 'Informatie over Bedreigde Personen Niet Langer in Kadaster' *29* (2018).
Schellevis, J, 'Gegevens KvK-Inschrijvingen Gebruikt Voor Reclames Op Facebook | NOS' *NOS* (18 April 2018).
Schellevis, J and Hekster, K, 'Privacywaakhond in Actie Tegen Datadelen Kamer van Koophandel | NOS' (*NOS*, 17 April 2018). Available at: https://nos.nl (last accessed 17 August 2018).
Sijmons, JG et al., 'Tweede Evaluatie Wet Op de Beroepen in de Individuele Gezondheidszorg' (2014) 4 *Tijdschrift voor Gezondheidsrecht* 264–281.
Tomesen WBM, 'Advies Voorstel Lerarenregister' (2015).
Van der Hoorn, S, 'Gegevensopstraat.Nl'. Available at: www.gegevensopstraat.nl/ (last accessed 17 August 2018).
Van Eechoud, M and Prins, C, 'Directive on Public Sector Information Re-Use' in Serge Gijrath and others (eds), *Concise European Data Protection Law, E-commerce and IT Law* (Kluwer Law International, 2018).
Van Rein, E, Verwiel, E and Van Zoggel, M, 'Het College Klust Bij' [2017] *De groene Amsterdammer*.
Versmissen. JAG and De Heij ACM, 'Elektronische Overheid En Privacy' (Den Haag, College bescherming persoonsgegevens, 2002).
'Wat Is Persoonsregistratie? | Persoonsregistratie | Arboportaal'. Available at: www.arboportaal.nl/onderwerpen/persoonsregistratie/wat-is (last accessed 18 August 2018).
Winter, H, Geertsema, B and Krol, E, 'Evaluatie LEC-SVH' Available at: www.dhwinspecteur.nl/wp-content/uploads/2016/10/evaluatie-lec-svh.pdf (last accessed 18 August 2018).
Zuiderveen-Borgesius, FJ, *Improving Privacy Protection in the Area of Behavioural Targeting* (Wolters Kluwer Business 2015).
Zuiderveen Borgesius, F, Van Eechoud, M and Gray, J, 'Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework' (2015) 30 *Berkeley Technology Law Journal* 2073.

Case law

European Court of Justice

Case C-398/15 *Camera di Commercio v Manni* ECLI:EU:C:2017:197, [2017] 3 CMLR 18.
Case C-131/12 *Google Spain and Google* ECLI:EU:C:2014:317, [2014] 3 CMLR 50.
Joined Cases C-293/12 an C/594/12 *Digital Rights Ireland* ECLI:EU:C:2014:238, [2014] 3 CMLR 44.
Joined Cases 509/09 and C-161/10 *eDate Advertising ao* ECLI:EU:C:2011:685, [2011] ECR I-10269.
Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* ECLI:EU:C:2010:662, [2010] ECR I-11063.
Case C-524/06 *Huber* ECLI:EU:C:2008:724, [2008] ECR I-09705.

European Court of Human Rights

Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland [GC], no 931/13, ECHR 2017 (extracts).
Leander v Sweden, judgment of 26 March 1987, Series A no 116, p 23.

[1] Institute for Information Law, University of Amsterdam.

[2] Institute for Information Law, University of Amsterdam.

[3] E.g. some date back to the sixteenth century. See Anna Berlee, *Access to Personal Data in Public Land Registers, Balancing Publicity of Property Rights with the Rights to Privacy and Data Protection* (Eleven International Publishing 2018) 214–216.

[4] Article 5(2) Directive 2010/64/EU on the right to interpretation and translation in criminal proceedings, OJ L 280, 26; Directive 2015/849/EU on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing ('Fourth Anti-money Laundering Directive'), OJ L 141, 73; Directive (EU) 2018/843 ('Fifth Anti-money Laundering Directive'), OJ L 156, 43.

[5] *Kamerstukken* II 2012–13, 33722, nr 2 (Legislative proposal Mediators Register Act).

[6] Act implementing the Market Abuse Regulation, Stb. 2018, 239.

[7] 'Wat Is Persoonsregistratie? | Persoonsregistratie | Arboportaal'. Available at: www.arboportaal.nl/onderwerpen/persoonsregistratie/wat-is (last accessed 18 August 2018).

[8] *Kamerstukken* II 2015–16, 34453, nr 2 (Legislative proposal Act quality assurance for building).

[9] GDPR does not apply eg to data processing in the sphere of criminal justice and crime prevention (see Art 2(2)), but in this field registers are usually not public.

[10] Charter of Fundamental Rights of the European Union, OJ C 2012/326, 391.

[11] The Dutch constitution guarantees protection of the right to private life and this includes informational privacy. In legal practice Art 8 of the ECHR dominates because under Dutch constitutional law, treaties are hierarchically above national law (and provisions with direct effect can be invoked against application of domestic laws), and because Dutch courts are barred from assessing the constitutionality of legislation (Article 120 Dutch Constitution).

[12] *Kamerstukken* II 2008–09, 31896, nr 3 (Explanatory memorandum alcolock programme).

[13] Official publications include legislative proposals, explanatory memoranda, reports of legislative debates in both houses of parliament (plenary, committee meetings), parliamentary questions, motions, references to external reports, etc.

[14] These are the websites of all Dutch Ministries, umbrella bodies of decentralised government entities (eg the Association of Netherlands Municipalities and Interprovincial Consultative Committee), the land register, and the Dutch Government open data portal data.overheid.nl.

[15] NORA, 'NORA Online'. Available at: www.noraonline.nl.

[16] An example is the register of certification for drivers of (construction) cranes, the 'TCVT' register, see www.tcvt.nl/persoonsregister/item12. To access it one needs to enter a unique crane driver certificate number and the date of birth of the holder of the certificate.

[17] Artice 5(1)(a) and (b) GDPR. The principle of fairness in Art 5(1)(a) GDPR also supports transparency in the broadest meaning: Jef Ausloos, 'Giving Meaning to Lawfulness under the GDPR – CITIP Blog' (2017). Available at: www.law.kuleuven.be/citip/blog/2761-2/ (last accessed 17 February 2019).

[18] Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (2016) WP 260 6.

[19] *Kamerstukken I* 2010–11, 31051, nr D (Motion Franken).

[20] Berlee (n 3) 214–216; College Bescherming Persoonsgegevens, 'Publicatie van Persoonsgegevens Op Internet' (2007) 3.

[21] See the mission of the Open Government Partnership (an international initiative joined by nearly 80 countries including EU Member States). Available at: https://www.opengovpartnership.org/mission-and-strategy/.

[22] See, for the involvement of the OECD: www.oecd.org/gov/digital-government/open-government-data.htm and United Nations: https://publicadministration.un.org/en/ogd.

[23] Mireille Van Eechoud and Corien Prins, 'Directive on Public Sector Information Re-Use' in Serge Gijrath and others (eds), *Concise European Data Protection Law, E-commerce and IT Law* (Kluwer Law International 2018).

[24] Proposal for a Directive of the European Parliament and of the Council on the re-use of public sector information, COM/2018/234 final (file 2018/0111(COD)). Adopted by Council and European Parliament (Adopted P8_TA-

PROV(2019)0352 on 04/04/2019).

[25] Maeve McDonagh, 'The Protection of Personal Information in Public Registers: The Case of Urban Planning Information in Ireland' (2009) 18 *Information & Communications Technology Law* 19, 21; Joost Schellevis, 'Gegevens KvK-Inschrijvingen Gebruikt Voor Reclames Op Facebook | NOS' *NOS* (18 April 2018).

[26] McDonagh (n 25) 21.

[27] Case C-131/12 *Google Spain and Google* ECLI:EU:C:2014:317, [2014] 3 CMLR 50, para 80, referring to Joined Cases 509/09 and C-161/10 *eDate Advertising a.o.* ECLI:EU:C:2011:685, [2011] ECR I-10269, para 45.

[28] *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* [GC], no 931/13, ECHR 2017 (extracts), para 98.

[29] Ibid, para 134.

[30] According to Article 29 Working Party, the most important legal basis for the publication of personal data for transparency purposes is Art 6(c) GDPR. The Dutch DPA also expects that this ground will increasingly be used by public and private parties mandated by law to maintain public registers. See: Article 29 Working Party, 'Opinion 02/2016 on the Publication of Personal Data for Transparency Purposes in the Public Sector', 2016, 5; College Bescherming Persoonsgegevens (n 20) 23.

[31] Article 29 Working Party, 'Opinion 8/2014 on the Notion of Legitimate Interests of the Data Controller', (WP 217) 2014, 19.

[32] Article 29 Working Party, 'Opinion 02/2016 (n 30); Case C-398/15 *Camera di Commercio v Manni* ECLI:EU:C:2017:197, [2017] 3 CMLR 18, para 42.

[33] Ibid.

[34] Article 29 Working Party, Opinion 02/2016 (n 30) 5.

[35] Ibid.

[36] Article 29 Working Party, Opinion 8/2014 (n 31) 22.

[37] Since the entry into force of the GDPR, it is not or no longer possible for public authorities to rely on the lawful ground of legitimate interest when processing is in the performance of their tasks, see Art 6(f) and final sentence GDPR.

[38] Anna Berlee, 'Volledige Openbaarheid: Het Doel Voorbij' (2017) 2017 *WPNR* 844, 848.

[39] F Zuiderveen Borgesius, M Van Eechoud, and J Gray, 'Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework' (2015) 30(3) *Berkeley Technology Law Journal* 1–32; Article 29 Working Party, 'Opinion 01/2012 on the Definition of Consent' (WP 187) 2011, 12–13.

[40] Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* ECLI:EU:C:2010:662, [2010] ECR I-11063, Opinion of AG Sharpston, paras 82–83.

[41] Article 28 Sworn Interpreters and Translators Act (*Wet Beëdigde Tolken en Vertalers*), Stb 2007, 471.

[42] GDPR recital 39.

[43] Art 44a *Wet Rechtspositie Rechterlijke Ambtenaren.*

[44] *Kamerstukken II* 1994–95, 24220, nr 3 (Explanatory Memorandum).

[45] This requirement of 'necessity' is central to the assessment of the legitimacy of processing for Arts 6(c) and (e) GDPR, see: Frederik J Zuiderveen-Borgesius, *Improving Privacy Protection in the Area of Behavioural Targeting* (Wolters Kluwer Business 2015) 143.

[46] Article 29 Working Party, 'Opinion 01/2014 on the Application of Necessity and Proportionality Concepts and Data Protection within the Law Enforcement Sector' (2014) WP 211 13–14. See also Article 29 Working Party, Opinion 02/2016 (n 30) 5. Also arguing that the term 'necessary' directly reflects the proportionality principle of Art 8 ECHR: JAG Versmissen and ACM De Heij, 'Elektronische Overheid En Privacy', (2002) 25 *Achtergrondstudies En Verkenningen* 37.

[47] CBP, 'Actieve Openbaarmaking En Eerbiediging van de Persoonlijke Levenssfeer' (2009) 5; Zuiderveen-Borgesius (n 45) 143.

[48] Janneke Gerards, 'How to Improve the Necessity Test of the European Court of Human Rights' (2013) 11 *International Journal of Constitutional Law* 466, 469.

[49] Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* ECLI:EU:C:2010:662, [2010] ECR I-11063, para. 85. See also GDPR, recital 39.

[50] Charlotte Bagger Tranberg, 'Proportionality and Data Protection in the Case Law of the European Court of Justice' (2011) 1 *International Data Privacy Law* 239. See also as applied in Joined Cases C-293/12 an C/594/12 *Digital Rights Ireland*, ECLI:EU:C:2014:238, [2014] 3 CMLR 44, paras 49–52.

[51] Gerards (n 48) 470.

[52] Anna-Sara Lind and Magnus Strand, 'A New Proportionality Test for Fundamental Rights ?' (2011) 1 *European Policy Analysis* 6.

[53] European Union Agency for Fundamental Rights and The Council of Europe, *Handbook on European Data Protection Law* (2014) 67.

[54] Versmissen and De Heij (n 46) 37.

[55] Joined Cases C-293/12 an C/594/12 *Digital Rights Ireland*, ECLI:EU:C:2014:238, [2014] 3 CMLR 44, para 18.

[56] Ibid, para 46.

[57] Ibid, para 49, where the CJEU concluded that the Data Retention Directive allowed national authorities to shed light on serious crimes and may consequently be considered to be appropriate.

[58] Judgment of 16 December 2008, *Huber*, C-524/06, ECLI:EU:C:2008:724, para 62.

[59] Art 7(e) Data Protection Directive, equivalent to GDPR, Art 6(e).

[60] Ibid. A further condition is that the register 'contains only the data which are necessary for the application by those authorities of that legislation'. The Court did not accept that a centralised register is necessary for statistical purposes.

[61] Manon Oostveen, *Protecting Individuals Against the Negative Impact of Big Data: Potential and Limitations of the Privacy and Data Protection Law Approach* (Wolters Kluwer 2018) 87–88.

[62] Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* ECLI:EU:C:2010:662, [2010] ECR I-11063, paras. 83, 85.

[63] *Kamerstukken I* 2010–11, 31051, nr D (Motion Franken).

[64] GDPR, Art 35.

[65] Ibid, Art 35(7)(b).

[66] Ministry of the Interior and Kingdom Relations, 'Model Gegevensbeschermings-Effectbeoordeling Rijksdienst (PIA)' (2017) 6.

[67] Article 29 Working Party, 'Opinion 02/2016 (n 30) 8.

[68] College Bescherming Persoonsgegevens (n 20) 41.

[69] Ibid 23.

[70] Sjoerd Van der Hoorn, 'Gegevensopstraat.Nl'. Available at: www.gegevensopstraat.nl/ (last accessed 17 August 2018).

[71] Ibid.

[72] *Kamerstukken* II 1984–85, 19095, nr 3 (Explanatory Memorandum *Wet persoonsregistratie*), 18; Art 2(2) Persons Registration Act.

[73] See Art 5 *Wet Schadeloosstelling leden Tweede Kamer* and Art 150a *Reglement van Orde Tweede Kamer*; Art 3b *Wet vergoedingen leden Eerste Kamer* and Art 256d *Reglement van Orde Eerste Kamer*; Art 6 *Wet Schadeloosstelling, uitkering en pensioen leden Europees Parlement* (Stb 2010, 122); Art 40b *Provinciewet*, Art 41b *Gemeentewet*, Art 44a *Waterschapswet* (Stb 2010, 110); and finally Art 44a *wet rechtspositie rechterlijke ambtenaren* (Stb 1996, 590).

[74] Art 150a *Reglement van Orde Tweede Kamer*.

[75] *Handelingen* II 2002–03, nr 62, 3719.

[76] *Kamerstukken* II 2005–06, 30425, nr 3 (Explanatory Memorandum).

[77] *Kamerstukken* II 2004–05, 29937, nr 3 (Explanatory Memorandum); *Kamerstukken* II ibid.

[78] *Kamerstukken* II 2004–05 ibid.

[79] RJJ Eshuis and N Dijkhoff, 'Nevenfuncties Zittende Magistratuur', (2000) *Onderzoek En Beleid* 185.

[80] Ibid, 58, 60.

[81] *Handelingen* II 2002–03, *aanhangselnummer* 7 (24 September 2002).

[82] Erik Van Rein, Erik Verwiel and Marlie Van Zoggel, 'Het College Klust Bij' [2017] De groene Amsterdammer.

[83] 'Burgemeester Wikt, Weegt En Zegt Die Ene Bijbaan Op,' *Brabants Dagblad*, 16 November 2017; 'Bijbaan Voor de Burgemeester', *Brabants Dagblad*, 23 February 2017.

[84] Alcohol and Food Service Industry Act, Art 8(5).

[85] Heinrich Winter, Bieuwe Geertsema and Erwin Krol, 'Evaluatie LEC-SVH' (2016) 9.

[86] *Kamerstukken* II 2008–09, 32022, nr 41 (Third rectifying letter).

[87] *Kamerstukken* II 1984–85, 19095, nr 3 (Explanatory Memorandum *Wet Persoonsregistratie*), 18; Persons Registration Act, Art 2(2).

[88] *Kamerstukken* II 1995–95, 23706, nr 6 (Note on the report). The names of notaries were already disclosed to the public in the Government Gazette before the creation of a public register.

[89] See Art 3(5) *Wet op de Beroepen in de Individuele Gezondheidszorg; Kamerstukken* II 1999–2000, 26410 nr 8 (Rectification letter); TK II 1999-00, 26410, nr 3 (Explanatory Memorandum Amendment of provisions relating to the processing of personal data); Stb 2002, 336; Stb 2003, 159; *Kamerstukken* II 2000–01, 27193 nr 6 (Rectification letter).

[90] Decree on the register of forensic experts, Stb 2009, 330.

[91] Ibid.

[92] Decree to the Youth Act, Stb 2014, 441.

[93] *Kamerstukken* II 2010–11, 32382, nr 8 (Rectification letter); *Kamerstukken* II 2015–16, 34458, nr 4 (Advice Council of State and further report).

[94] *Kamerstukken* II 1982–83, 17646, nr 3 (Explanatory Memorandum).

[95] *Kamerstukken* II 2010–11, 32382, nr 8 (Rectification letter).

[96] Act on the status and oversight over the legal profession, Stb 2014, 354; Stb 2014, 429 (entry into force); *Kamerstukken* II 2010–11 (n 95).

[97] *Kamerstukken* II 2010–11 (n 95).

[98] *Kamerstukken* II 2014–15, 29282, nr 203 (Letter of the Minister of Health on labour market policy and education health care sector).

[99] EH Hulst, 'Naming En Shaming van Artsen Die Tuchtrechtelijk Zijn Veroordeeld' (2017) 1 *Tijdschrift voor Gezondheidsschade, Milieuschade en Aansprakelijkheidsrecht* 1.

[100] JG Sijmons et al., 'Tweede Evaluatie Wet Op de Beroepen in de Individuele Gezondheidszorg', Reeks Evaluatie Regelgeving, 2013, 53.

[101] Ibid.

[102] Ibid.

[103] Ibid at 54.

[104] Roland Friele et al., 'Zorgverleners En Burgers over Het Openbaar Maken van Door de Tuchtrechter Opgelegde Berispingen En Geldboetes' (2017) 35.

[105] These constraints also apply *erga omnes*, as opposed to limitations under contract law, meaning that registration can be invoked against anyone.

[106] *Kamerstukken* II 2011–12, 33054, nr 6 (Note on the report).

[107] Insolvency Act, Art 23.

[108] Article 1:116 Dutch Civil Code; Article 1:121 in connection to Article 1:94 Dutch Civil Code.

[109] *Kamerstukken* II 2011–12, 33054, nr 3 (Explanatory Memorandum).

[110] IJ Kloek-tromp, 'Kadaster En Privacy in Praktijk' (2017) *WPNR* 854.

[111] *Kamerstukken* II 1996–97, 25095, nr 3 (Explanatory Memorandum); *Kamerstukken* II 2000–01, 27900, nr 3 (Explanatory Memorandum).

[112] Ibid.

[113] The legal title of Regulation 596/2014 imposing the publication of transactions by managers is aptly called the 'Market Abuse Regulation'.

[114] *Kamerstukken* II, 2011–12 (n 109).

[115] *Kamerstukken* II 1997–98, 25095, nr 12 (Amendment Voute-Droste).

[116] However, public disclosure could in this case merit accountability of the *AFM*. This would have to be made an explicit and proportional purpose of the register.

[117] Art 2 Commercial Register Act (*Handelsregisterwet*).

[118] Article 1:244 Dutch Civil Code (*Burgerlijk Wetboek).*

[119] NORA (n 15); Berlee (n 38) 844.

[120] Case C-398/15 *Camera di Commercio v Manni* ECLI:EU:C:2017:197, [2017] 3 CMLR 18.

[121] Ibid.

[122] Ibid; Case C-131/12 *Google Spain and Google* ECLI:EU:C:2014:317, [2014] 3 CMLR 50, para 91.

[123] Case C-398/15 *Camera di Commercio v Manni* ECLI:EU:C:2017:197, [2017] 3 CMLR 18, para 42.

[124] Ibid, para 63.

[125] *Kamerstukken* II 1982–83, 16143, nr 9 (Note on the final report Trade Register Act Amendment), 2.

[126] *Handelsregisterwet*, Stb 1996, 181.

[127] *Kamerstukken* II 2005–06 (n 76).

[128] Ibid.

[129] Joost Schellevis and Kysia Hekster, 'Privacywaakhond in Actie Tegen Datadelen Kamer van Koophandel | NOS' (*NOS*, 17 April 2018). Available at: https://nos.nl(last accessed 17 August 2019).

[130] Art 2a Land Registry Act (Kadasterwet).

[131] Berlee (n 38) 848.

[132] Article 29 Working Party, 'Opinion 03/2013 on Purpose Limitation' (WP 203) 2013, 54.

[133] Friele and others (n 104) 35.

[134] Berlee (n 3) 214–216.

[135] *Leander v Sweden*, judgment of 26 March 1987, Series A no 116, p 23.

[136] Entry into force of the Dutch Personal Data Protection Act, Stb 2001, 337.

[137] Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* ECLI:EU:C:2010:662, [2010] ECR I-11063, para 85.

[138] *Kamerstukken* II 1984–85, 19095, nr 3 (Explanatory Memorandum *Wet Persoonsregistratie*), 18; Art 2(2) Persons Registration Act.

[139] Act amending provisions related to the processing of personal data, Stb 2001, 180.

[140] Archon Fung, Mary Graham and David Weil, *Full Disclosure: Perils and Promise of Transparency* (Cambridge University Press, 2007) 40; Van Rein, Verwiel and Van Zoggel (n 82); Eshuis and Dijkhoff (n 79).

[141] Paul Frissen, *Het Geheim van de Laatste Staat Kritiek van de Transparantie* (Boom uitgevers 2016) 131–137; Fung, Graham and Weil (n 140) 5 and 40.

[142] College Bescherming Persoonsgegevens, 'Advies Voorstel Lerarenregister' (2015).

[143] Eg when it became clear that persons who are threatened by, eg, former spouses, disgruntled employees or random stalkers can easily be traced by perpetrators on the basis of information from the Land Registry, the Dutch Government announced measures, Rijksoverheid, 'Informatie over Bedreigde Personen Niet Langer in Kadaster' 29 (2018).

[144] Ausloos (n 17).

[145] European Commission, 'European Legislation on the Re-Use of Public Sector Information | Digital Single Market' (2019). Available at: https://ec.europa.eu/digital-single-market/en/european-legislation-reuse-public-sector-information (last

accessed 17 February 2019); Open Government Partnership, ‘About OGP’. Available at: www.opengovpartnership.org/about/about-ogp (last accessed 19 February 2019).

9

Examination Scripts as Personal Data

The Right of Access as a Regulatory Tool against Teacher-Student Abuses in Cameroon Universities[*]

ROGERS ALUNGE[1]

Abstract

Global legal trends are increasingly focused on giving individuals some level of protection of their information, especially information about their personal lives held in online servers of public and private institutions. These trends are particularly concentrated in Europe and are reflected in the Data Protection Directive (DPD) of 1995 and its 2016 successor the General Data Protection Regulation (GDPR) and the 2014 African Union (AU) Convention on Cybersecurity and Data Protection. A right of access to personal data to verify and rectify their accuracy, among other rights, is guaranteed to individuals under these international instruments. With personal data comprising evaluated examination scripts as illustrated in the *Nowak* case, this right of access consequently involves the right to access, verify and rectify the accuracy of an examiner's evaluations on examination scripts.

In this light, this chapter advocates that an EU approach to interpreting the AU Data Protection Convention and granting personal data protection rights on examination scripts could yield positive regulatory impacts on African countries in general and Cameroon in particular, in terms of tackling professor–student abuses in university campuses. Granting Cameroonian citizens (and thus university students) an EU-interpreted data protection right to access and rectify the accuracy of their personal data (evaluated examination scripts) could provoke transparency and accountability and consequently encourage more responsible behaviour from staff who are abusing their power in institutions of higher learning in the country.

Keywords

Examination scripts, right of access, teacher–student abuse, African Union, Cameroon.

I. Introduction

Access to information, considered a basic human right, is guaranteed in a number of international instruments,[2] is a primordial factor of economic development and democratic governance especially in view of meeting the challenges of an information society and has always occupied one of the top positions in development agendas for developing countries.[3] However, while the literature and development programmes in most developing countries focus much more on promoting access to and verification of public information through measures such as open data initiatives,[4] not so much effort has or is being directed towards access to and verifying the accuracy of personal information. Taking its cue from the European approach to personal data protection law, specifically its material scope under the Data Protection Directive (DPD) and its successor the General Data Protection Regulation (GDPR),[5] this paper generally intends to show that the right to access and rectification of personal data processed by public or private institutions could be a source of empowerment and could provoke consequential auto-regulation within certain sectors with specific regulatory needs. In particular, the chapter argues that an interpretation of the notion of personal data under the African Union Convention on Cybersecurity and Data Protection similar to the EU approach to personal data protection, coupled with a corresponding right of access to personal data, could help curb teacher–student abuse in institutions of higher learning in Cameroon.

Such interpretation is not so far-fetched: while the AU Data Protection Convention adopts an identical, almost word-for-word definition of personal data as the DPD and GDPR, and also incorporates a right of access to personal data, Cameroon legal practitioners, like in many other former European colonies, in some areas of law, still rely on European (that is, English and French) case law and instruments to render justice in national courts. The EU notion of personal data protection law appears to be an extension of the EU legislator's objective to provide individuals with a high standard of protection as regards their online information, including vesting in them the widest possible rights to control and decide what happens to their data after it is collected from them, who has access to its exploitation, to whom it is transferred, even who as much as sees it. These rights, as shall be discussed later, also include access to their data at any time, to verify that they accurate and up to date.

The intention by the EU legislator to offer a high standard of protection to individuals as regards information they share about their online lives has led the former to adopt a very broad interpretation of what constitutes 'personal data'. Some authors think this already broad interpretation is bound to expand even further as we increasingly approach what has been referred to as an onlife[6] experience, where our daily existence is mediated by information technology, and everything around us – weather, waste water, transportation – is being increasingly 'datified' and literally any data can be plausibly argued to be personal.[7] Despite criticism by some authors that the concept of personal data is becoming too broad because current available technology can be used to trace just about any information back to an identified individual,[8] the fact remains that this approach is leading to the development of new rights which were hardly addressed before, or may been difficult to enforce under other branches of law. This is particularly evident in the judgment of the European Court of Justice (ECJ) in the case of *Peter Nowak v Data Protection Commissioner*[9] where the court ruled

that the examiner's notes on an evaluated examination script constituted the examination candidate's personal data within the context of European data protection law. One would imagine that prior to this decision or the emergence of data protection law, the legal bearing on whether or not examination candidates could request to view their evaluated examination script was limited solely to their contract with the examining institution or to specific sectoral rules regulating the higher education sector. Now EU case law has established such access to personal data (operating alongside the right to personal data protection) as constituting a fundamental right for every EU resident, which automatically enables enforcement, by a student, of the right to verify his/her script and confirm the accuracy of the examiner's corrections. Also worth noting is the fact that the development of European data protection law, though currently a fundamental right on its own,[10] was prompted as a result of the limitations of the right to privacy guaranteed under Article 8 of the 1950 Convention on Human Rights in the wake of new developments especially in the area of information technology.[11] But this broad interpretation, in terms of protecting individuals, appears to extend the material scope of EU law back in time, to protect elements which existed before the digital era, is not affected by technology, yet at that time, appeared to be out of the reach of the right to privacy.

The ECJ decision in the *Nowak* case, with regard to the education sector in developing countries, could be groundbreaking from an educational point of view, as it introduces a new dimension to the rights which an examination candidate or student may have vis-à-vis their examining institution or university respectively. This could not only empower examination candidates and students in public and private institutions of higher learning but could also automatically oblige these institutions and their staff, as data controllers and processors, to adopt more responsible behaviour vis-à-vis their students. Such an approach, if followed by African judges in their interpretation of the AU Data Protection Convention, could play a significant role in regulating teacher-student abuses in universities of developing countries, which include sexual favours for grades, 'sorting' or failing students for non-academic or personal reasons. It is in this light that this chapter investigates the potential regulatory role which an EU-based interpretation of the AU Data Protection Convention's right of access to personal data could play in limiting teacher–student abuse on Cameroon university campuses. With no comprehensive legislation in the country specifically governing personal data processing, no related case law and the AU Data Protection Convention not yet in effect, this chapter aims to demonstrate that offering and enforcing EU-inspired data protection rights of access to students in Cameroon vis-à-vis their evaluated examination scripts as personal data could be a major incentive in promoting the appropriate conduct from potentially offending professors and lecturers. In doing so, it also engages the argument that personal data protection law, in particular the right of access, could complement government efforts and other areas of law where these may be inadequate in dealing with teacher–student abuses in a third world setting.

In the following section, the chapter identifies some instances of teacher–student abuse in Cameroon universities and discusses the current national efforts and related inadequacies in addressing the issue. The third section features a brief synopsis of the notion of personal data in EU data protection law, a discussion on the right of access to personal data under EU law

and an overview of the *Nowak* case, while the fourth section focuses on the concept of personal data and the right to access evaluated examination scripts as personal data under the AU Data Protection Convention. The fifth section first examines current state of the right of access to evaluated examination scripts in Cameroon universities before discussing the regulatory effects which a potential EU-inspired interpretation of the notion of personal data and right to access under the AU Data Protection Convention could have in deterring teacher–student abuses in institutions of higher learning in Cameroon. It equally identifies and discusses a few hindrances which could be encountered in the practical enforcement of a right of access on university professors and staff. The sixth and final section presents the final conclusions.

II. Teacher–Student Abuses in Cameroon Universities: An Overview

This section examines the phenomenon of teacher–student abuses in Cameroon universities. It shall briefly identify some known examples of teacher-student abuses which affect the sector, before discussing any available (though limited) means of protection for the students affected.

A. Some Forms of Teacher–Student Abuse in Cameroon Universities

Here, the chapter identifies some of the teacher-student mistreatments which plague universities and other institutions of higher learning in Cameroon. The abuses identified here are not exhaustive and, in view of the objective of this chapter, are selected on the basis of how the enforcement of a right of access to personal data could significantly reduce their prospective occurrences and incentivise more responsible behaviour on the part of professors or lecturers.

i. Sexual Abuse for Grades

Sexual abuse for grades in institutions of higher learning is not peculiar to Cameroon alone;[12] it is also a systematic occurrence in other African states.[13] It is not uncommon for offending lecturers to demand sexual favours from students in exchange for either awarding them a pass grade (where the student performed poorly) or even for recording a pass grade which is well deserved by the student (ie the student receives a fail grade if he/she declines the proposal).[14] Cameroon universities do play host to this phenomenon, but as these forms of sexual violence are not often reported,[15] data for quality research on the issue is rare. However, the incidents are not: a guidance counsellor for the Faculty of Social and Management Sciences of the University of Buea, in a 2012 interview, stated that a majority of female students have experienced one or two forms of sexual abuse from male academic

staff on campus. These assaults often happen in the office and in lecture halls, when students are requesting make-up tests or extra lectures, submitting overdue assignments and making other pleas to male academic staff.[16] In her 2011 article on sexual violence on university campuses, Zoneziwoh notes that research studies on sexual violence in the University of Buea were highly underexplored. Victims preferred to report their sexual victimisation to friends, family, colleagues and peers – instead of seeking formal counselling. She blamed this on the fact that there are no established bodies on campus to specifically handle cases of sexual violence on university campuses.[17]

ii. 'Sorting'

'Sorting' refers to the negotiation of examination scores with course instructors and school authorities using incentives.[18] This dimension of examination malpractice is currently gaining ground in the universities of some developed countries and is one of the practices which academic staff who seek personal enrichment involve themselves in.[19] There is a high manifestation of sorting in examinations in Cameroon universities.[20] In the University of Buea, a study shows that sorting is also initiated by lecturers who force students to purchase their handouts (photocopies of lecture notes). To ensure that students get these handouts, they take down the names of the students who have paid for them. Students who then have their names on the list are compensated through the marking scheme, while those who did not buy the handouts are penalised.[21] Because exam scripts are usually marked only by the professor and with virtually no direct oversight and feedback, he/she remains in total control of the grading; this makes it extremely difficult for the affected students to prove (or even be aware) that they had been cheated.

iii. Failing Students for Personal Reasons

There has been considerable literature on the unequal balance of power between professors and students in institutions of higher learning.[22] Within the educational context, there often is a struggle between asymmetrically positioned individuals [professors and students, in this case], which renders one individual as powerful and the other as powerless.[23] The teacher–student relationship has also been described in terms of a transactional process, whereby teachers are in control of curriculum links and teaching styles and students are oppressed receivers of selected information.[24]

This power imbalance is quite glaring in institutions of higher learning in Cameroon, where the lecturer or professor dictates the rules of his/her course and reigns supreme thereon. Due to this somewhat unrivalled status, some professors sometimes tend to abuse their power, even – and not unusually – for selfish or personal reasons. In Cameroon, as well as in other African universities, reports of lecturers giving undeserved grades to students because of personal disagreements, off-campus rivalries or for other purely non-academic reasons are not totally unheard of.[25]

This state of affairs generally favours the victimisation of students by members of staff, contributing to the bulk of educational troubles in the country. The state has tried to establish a legal framework to sanction abusive lecturers, but this is inadequate and reflects a lack of vehemence in state action to address the issue.

B. Regulating Teacher-Student Abuse in Cameroon: Inadequacies in National Efforts

Unfortunately, very little has been done by government agencies and lawmakers in Cameroon to directly and actively address teacher–student abuse in the country. Action so far has been limited to the adoption of legal texts on education which provide general protection for students on school campuses and, to a lesser extent, general criminal law.

i. Higher Education Regulatory Texts

For higher education (ie universities) Law No 005 of 16 April 2001 prohibits 'any violation of human dignity' in state and private institutions of higher learning,[26] while Law No 98/04 of 14 April 1998 guarantees the physical integrity of the secondary school student and prohibits 'any form of abuse' on secondary school campuses.[27] There is currently no national law or decree which clearly defines and directly addresses teacher–student abuse with clearly laid down enforcement mechanisms against the phenomenon. Most university student guidelines and administrative texts in the country are practically silent as regards available means of redress which students may have against abusive members of staff or university authorities.

Admittedly, however, Decree 93/035 of 19 January 1993 on the Special Status of Higher Education Staff contains some provisions in this direction. Article 48 of the Decree mentions the obligation by university professors and staff to ensure the smooth functioning of the teaching activity and safeguard academic dignity. The Decree does not specifically address teacher-student abuse, though Article 51 provides for unspecified disciplinary sanctions on university staff for, inter alia, 'violations of the general rules listed in Article 48', for 'professional misconduct' and for 'participating in any activity incompatible with academic dignity and ethics'. The Decree also provides for the creation of a Disciplinary Council in each state university with the powers to sanction personnel.[28] Though it is not expressly mentioned that this Council can entertain cases of student abuse, it can be inferred by analogy that an abused student can, in theory, report their dilemma to the university Rector who, as per Article 55, has the power to convene the Disciplinary Council and summon a lecturer to a hearing, which takes place *in camera*.[29] However, in cases involving examination scripts, as will be discussed later, the lack of a right of access to evaluated examination scripts prevents students from being absolutely certain they have been discriminated against. They would generally therefore prefer silence than risk having a Disciplinary Council convened for an unfounded claim.

ii. National Criminal Law

Situations of student–teacher abuse, being purely educational issues, are generally less likely to fall within the ambit of criminal law. However, criminal law could be triggered when it comes to abuse of a sexual nature. Cameroon criminal law punishes the use of one's position of power to obtain sexual favours from a vulnerable individual,[30] a provision which can be invoked by students who face similar situations with a professor. However, in a Cameroon university setting, as has been mentioned above, these cases are hardly reported[31] not only because they are difficult to prove, but also because of the dominant psychological position professors enjoy vis-à-vis their students. Also, criminal law requires inquiries, investigations, interviews and convocations which may lead to unwanted publicity. And in a third world country like Cameroon, such processes are almost always plagued by bureaucracy bottlenecks, are very slow or lack the input of qualified staff and trained judicial investigators to carry them out efficiently.[32]

iii. Absence of an Official Code of Ethics for University Professors

Unlike other sectors of activity such as the medical and legal professions in the country, the higher education sector of Cameroon is yet to adopt an official code of ethics for university professors and lecturers. The closest rules in force for regulating this sector of activity in terms of professional conduct are those cited above in the Decree of 19 January 1993 sanctioning general misconduct by university staff. Though acts of abuse such as sexual harassment or grading discrimination are normally frowned upon in university settings, the lack of an official code of conduct guiding the higher learning profession only reflects the current apathy of the government and its competent agencies towards robustly addressing teacher–student abuse in university campuses in the country. Nonetheless, this could change soon: the Ministry of Higher Education officially launched discussions on 30 May 2019 towards the elaboration of an official code of ethics for university professors and staff members in the country.[33]

This section has identified some instances of teacher–student abuse as well as the current inadequacies in national efforts to seriously address the phenomenon. This chapter argues that providing individuals with a right to access and verify the accuracy of their personal data (in this case, evaluated examination scripts to verify the accuracy of the examiner's evaluation) would, besides complementing the current efforts, significantly contribute to checking the prevalence of this malpractice in the country's universities. This right of access, inherently offered and successfully applied under European data protection law, as discussed in the next section, is also offered in the main regional text on African data protection law. However, there is yet to be a legal interpretation or case law applying this right to examination scripts on Cameroonian or anywhere in Africa. It is the view of this chapter that a legal interpretation, in Cameroon and by Cameroon legal practitioners, first of what constitutes personal data and subsequently the right of access to personal data as it has been so interpreted and applied in Europe, could help regulate this misconduct and foster responsible behaviour by university staff. The following section, briefly examines the notion

of personal data and the right of access to personal data (including evaluated examination scripts) as it applies within the European legal system.

III. Personal Data and the Right of Access in EU Data Protection Law

European data protection law has been hailed as offering the highest protection for individuals with regard to the processing of their digital personal information by private companies or public institutions.[34] The regional legal regime not only aims to protect the privacy of online users with regard to how their information is collected and with whom it is shared, but also gives them the a high level of control over how the information is used and who gets to use it. As described by De Hert et al, while privacy law protects the opacity of the individual by prohibitive measures (non-interference), data protection calls for transparency of the processor of personal data enabling its control by the concerned individuals, states and special authorities. It puts the activity of the processor in the spotlight, gives the individual subjective rights to control the processing of his/her personal data and enforces the processor's accountability.[35] In other words, the European legislator has adopted a sort of 'defence by attack' strategy of protection: protecting individuals not only by imposing processing restrictions on the data controller, but also by enabling them to leave the shell of their 'privacy' and oversee the activity of the data controller over their data by providing them with a right of access to (the processing of) their personal data. Or generally, by granting control to individuals over data processing activities which might affect them.[36] This section first examines the concept of personal data, before focusing on the right of access (to personal data) under European data protection law.

A. The Concept of Personal Data

Perhaps the most fundamental notion of data protection, personal data determines the material scope of the two main texts of reference of European data protection law, the 1995 Data Protection Directive (DPD now repealed) and the GDPR.[37] The data protection mechanism is triggered only when personal data is processed (Article 3(1) DPD and Article 2(1) GDPR), hence its major significance.

Under the GDPR, which closely follows the DPD, 'personal data' is defined as:

> 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.[38]

If there is one striking thing about the concept of personal data under European law, it is its very broad scope. In its quest to offer a high standard of protection to information society

service users, the EU legislator chose to adopt a definition of personal data which could be stretched, it has been argued, to include virtually every type of information.[39] As noted by the Article 29 Working Party,[40] the European Commission's original proposal explained that 'as in Convention 108, a broad definition is adopted in order to cover all information which may be linked to an individual' and the Commission's modified proposal noted that 'the amended proposal meets Parliament's wish that the definition of "personal data" should be as general as possible, so as to include all information concerning an identifiable individual'.[41] The EU approach is clear: any information 'concerning' an individual should be treated as personal data; this further makes a case for evaluated examination scripts to constitute personal data. In this light, and to further elucidate this point, close attention should be paid to the terms 'any information' and 'relating to'.

i. 'Any Information'

The term 'any information' contained in the Directive clearly signals the willingness of the legislator to design a broad concept of personal data and calls for a wide interpretation of the concept.[42] It should be pointed out that while explaining the meaning of 'any information' within the meaning of the 1995 Data Protection Directive, the Working Party does not define or elucidate the concept of information itself, but rather goes on to explain what kinds of information would be considered 'any information' in EU data protection law. This only leaves the definition of information in a personal data protection context open to interpretation and tends to further expand the scope of what may constitute personal data, stretching the limits of the material scope of EU data protection law. The Working Party noted that personal data could be information not limited *strictu sensu* to private or family life, but information 'regarding whatever types of activity is undertaken by the individual, like that concerning working … the economic or social behaviour of the individual'.[43] Considering that an evaluated examination script contains data showing an individual's behaviour when confronted with a given set of problems (even hypothetical or imaginary problems), it should still be regarded as personal data in EU data protection law.

Another interesting interpretation advanced by WP136 is that information could be personal data whether processed by non-electronic means[44] and regardless of the format or medium in which the information is contained. It could be numerical or, ideally, information kept on paper.[45] An examiner's written evaluation on an examination script perfectly fits these criteria.

ii. 'Relating to'

The WP29 referred to this building block of the definition of personal data as 'crucial as it is very important to precisely find out which are the relations/links that matter and how to distinguish them'.[46] It advances, in general terms, that information can be considered to 'relate' to an individual when it is *about* that individual.[47] In a prior Opinion, in 2005, on data protection issues raised by RFID tags, the WP29 had established that 'data relates to an

individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated'.[48] Seen in this light, evaluating examination scripts serves one main purpose: that of evaluating the student, the result of which will determine his/her future both within and outside of an institution.

WP29 further establishes that information could 'relate to' a person in terms of 'content', 'purpose' or 'result'.[49] The 'content' element is fulfilled when the information is clearly about the person (eg medical examination results under a person's name); the 'purpose' element 'can be considered to exist when the data are used or are likely to be used, taking into account all the circumstances surrounding the precise case, with the purpose to *evaluate*, treat in a certain way or influence the status or behaviour of an individual (emphasis added); and as regards the 'result' element, data can be considered to 'relate to' an individual because their use is likely to have an impact on a certain his/her rights and interests.[50] The European Court of Justice concurred with this reasoning as regards an examiner's evaluative information on an examination script in the case of *Peter Nowak v Data Protection Commissioner.*[51]

*iii. Evaluated Examination Scripts as Personal Data in EU Data Protection Law (*Peter Nowak v Data Protection Commissioner*)*

In 2017, a landmark decision was reached in the case of *Peter Nowak v Data Protection Commissioner*, with regard to data protection law in the education sector. In 2009, Peter Nowak, a registered student with the Institute of Chartered Accountants of Ireland (CAI) asked to view his scripts for an accounting exam after failing it for the fourth time, with a view to challenging the result. The CAI declined to release the exam script, saying it did not constitute personal data under data protection legislation. Mr Nowak sought assistance from the Data Protection Commissioner but was rejected on the same grounds as with the CAI. After appealing to the Circuit Court, then the High Court, the case got to the Supreme Court which decided to ask the European Court of Justice for guidance. In its reference for a preliminary ruling, the Irish Supreme Court essentially asked whether the exam script containing the candidate's answers and the examiner's comments regarding those answers might constitute personal data.[52] Both the response by Advocate General of the European Court of Justice (in her Opinion) and the Court were in the affirmative.

The Advocate General's reasoning was consistent with the WP29 approach to consider information as personal data when it is processed with a purpose of evaluating the status or behaviour of an individual. Even though the examination exercises are 'formulated in abstract terms or relate to hypothetical situations',[53] 'the script is a documentary record that that individual has taken part in a given examination and how he performed'.[54] She further states that 'in every case, the aim of an examination […] is to identify and record the performance of a particular individual (ie the examination candidate). Every examination aims to determine the strictly personal and individual performance of an examination candidate'.[55]

The Court followed the reasoning of the Attorney General. It reaffirmed the notion 'personal data' as potentially encompassing any information, as long as it 'relates' to the data subject,[56] stating that the condition is met where the information is linked to a particular person 'by reason of its content, purpose or effect'.[57] More significant, the Court found that the link between the information and the individual relevant because both the candidate's answers and the examiner's comments relate to the data subject in all three aspects: they reflect the information about the candidate (his knowledge, thought process and, in the case of a handwritten answer, information about his handwriting, as well as the examiner's opinion regarding the candidate's performance);[58] the purpose of their processing is to evaluate the candidate in terms of his professional abilities; the use of this information is 'liable to have an effect on his or her interests'.[59]

B. Right of Access to (and Rectification of) Evaluated Exam Scripts in EU Data Protection Law

European data protection law has, from the outset, pursued dual objectives. One of these objectives is economic – to facilitate the establishment of the internal market – while the other is rights-based – to protect fundamental rights when personal data is processed.[60] The right of personal data protection as well as a right of access to personal data are well established in the EU Charter of Fundamental Rights (CFR) of 18 December 2000. Captioned 'protection of personal data', Article 8 of the Convention states:

> 'Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.'

This Article not only explicitly mentions a right to data protection, but also explicitly creates a concurrent right of access to personal data, as well as the right to have it rectified, to ensure accuracy. The right of access to personal data is therefore expressly guaranteed as a functional tool of the right to data protection in EU law. The Data Protection Directive states that the principle of data protection should be reflected both in the obligations imposed on data controllers for responsible processing as regards quality and technical security, and also in the right conferred on individuals 'to consult the data, to request corrections and even to object to processing in certain circumstances".[61] The right of access under Article 12 of the Directive is a four-fold: the data subject may ask confirmation as to whether or not his data are being processed; he has the right to obtain communication of these data (ie have copies of the data being made available to him); he can have the data rectified, erased or blocked if they do not conform to the Directive, in particular if they are incomplete or inaccurate; and has the right to be informed about the logic used in automated decisions. The right of access to personal data under the 1995 Directive, it can be concluded, incorporates two important components in relation to this chapter: the right of data subjects to be presented with their personal data, and their right to have that data rectified.[62]

The GDPR closely follows this approach, recommending that a data subject should have 'the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing'.[63] However, moving slightly away from the approach of the CFR, it provides for the right of access (Article 15) and the right of rectification (Article 16) in two separate Articles, which suggests that these rights are two separate rights under the GDPR. Nevertheless, the enforcement of a right of access, in event of established data inaccuracy, will most likely involve the right to rectification by ricochet. In other words, the former is necessary for the realisation of the latter.[64] It follows that if examination scripts are personal data under European law, then a student is apparently well within his/her data protection rights if they request access to their evaluated examination script being processed by an examining institution in order to verify the accuracy of the evaluation, and demand its rectification if need be.

This was apparently the view of AG Kokott in the *Nowak* case. In response to the question as to whether the examination candidate had a right to access his data, her opinion was in the affirmative, stating that he 'has a legitimate interest, based on the protection of his private life' to be able to object to the processing of his or her examination script outside the examination procedure.[65] The ECJ upheld this view,[66] ruling further that the rights of access and rectification provided for in Article 12(a) and (b) of the Directive 'may also be asserted in relation to the written answers submitted by a candidate at a professional examination and to any comments made by an examiner with respect to those answers'.[67] The above show that EU data protection law not only qualifies examination scripts as personal data, but also guarantees a right of access to verify that these scripts have been fairly evaluated. As was seen in *Nowak*, this enabled the examination candidate (plaintiff) to at least see how his script was evaluated and, if he so desired, demand that they be changed if they are inaccurate within the meaning of Article 6(1)(d) of the 1995 Directive.

It should be noted, however, that the right of access to (and rectification of) personal data is not an absolute right and may be limited in some instances in EU law.[68] As a matter of fact, it has been rejected by the ECJ in a case which, if granted, would have laid a precedent for access to administrative documents of a country's immigration office.[69] Wachter and Mittelstadt are also of the opinion that the ECJ does not intend to use data protection law as a tool to ensure accuracy or total transparency in decision-making processes involving personal data, leaving that to specific sectoral laws.[70] However, as noted by the Article 29 Working Party, data protection law envisages the possibility of personal data being incorrect and provides for a right for data subjects to access their personal data to rectify it.[71] And a careful analysis of the ECJ's interpretation of inaccuracy of examination results in *Nowak* within the meaning of Article 6(1)(d) would lead to the understanding that an examiner's unfair comments which do not reflect the answers on the script could be regarded as inaccurate data,[72] especially considering the premise that the candidate's answers themselves, with or without any grades, are personal data, because they *relate to* the candidate's intellectual level.[73] And if processing (checking the correctness, hence evaluation and which itself is supposed to be fair, reflecting the data protection principle of fair processing[74]) carried out on

this set of personal data yields inaccurate results which will impact a data subject's career, then right to rectification and prior right of access are likely to (or should) be triggered. It should nevertheless be pointed out here that the essence of this chapter is not to present data protection and particularly the right of access and rectification as a 'silver bullet' solution for ensuring fair grading of examination answers. Rather, these rights are presented as a tool for reducing the power imbalance between students and professors by making it possible for a graded script to be accessed and even made public (by the candidate) for everyone to see and have an opinion; this could discourage unfair grading by abusive professors.

Across the Mediterranean, the AU Convention on Cybersecurity and Data Protection adopts definitions and rights attached to personal data inspired by and strikingly similar to those of the EU. It therefore is not too far-fetched for African judges and lawyers to interpret these notions and rights similarly to their interpretation by the ECJ. The following section presents a brief synopsis of the AU Convention, as well as its adopted notion of personal data.

IV. Personal Data under the AU Data Protection Convention

This section shall be an overview of the AU Data Protection Convention, which is inspired by Europe's DPD model. It shall first present a brief background of the Convention before examining the similarities between its notion of personal data and that of the DPD and GDPR. After which it features a discussion on its right of access to personal data and, by interpretation, to evaluated examination scripts.

A. African Union Convention on Cybersecurity and Personal Data Protection

The AU was established in 2001 to replace the Organization of African Unity and has its headquarters in Addis Ababa, Ethiopia. Its aims include, inter alia, to 'accelerate the political and socio-economic integration' of the African continent and to 'coordinate and harmonize the policies between the existing and future regional economic communities for the gradual attainment of the objectives of the Union'.[75] These mandates create a broad legal basis for the AU to establish regional policy and regulatory regimes on issues that affect Africa's economic integration and development, such as telecommunications/ICTs and personal data protection. From 2008, a series of high-profile meetings were held between ICT policy makers and economic stakeholders of AU Member States, culminating in the adoption, by AU Member State ministers in charge of ICTs, of a set of declarations known as the Oliver Tambo Declaration on 5 November 2009 in Johannesburg, South Africa.[76] The Declaration directed the AU to 'jointly develop with the United Nations Economic Commission for Africa (UNECA), under the framework of the African Information Society Initiative, a

Convention on cyber legislation based on the continent's needs and which adheres to the legal and regulatory requirements on electronic transactions, cybersecurity, and personal data protection'.[77] Five years later, at the 23rd Ordinary Session of the Assembly of Heads of State of the African Union in Malabo on 27 June 2014, the Convention on Cyber Security and Personal Data Protection (hereinafter the AU Data Protection Convention) was adopted.

The Convention provides a legal framework regulating three distinct domains and divided into as many corresponding sections: Electronic Commerce, Data Protection and Cybercrime/cybersecurity. It has as objective, as regards personal data protection, the establishment of a legal framework 'aimed at strengthening fundamental rights and public freedoms, particularly the protection of [personal] data, and punish any violation of privacy without prejudice to the principle of free flow of personal data'.[78] It should be pointed out that, unlike the EU, legal integration within the AU is hardly a reality;[79] the Union has been likened to an interstate organisation (with focus on the nation state and regarding regionalism simply as an arena for international politics) rather than a supranational organisation, hence the inability to adopt enforceable decisions which prevents the establishment of a regional legal system through institutional action.[80] As a result, Conventions adopted by the General Assembly of the African Union, when they become effective, are not directly binding on Member States. Only a further Act by a Member States incorporating a Convention into its national legislation renders the Convention applicable in the said state.

The AU Data Protection Convention in question, at the time of writing, is not yet effective, and will attain this status only upon ratification by 15 Member States.[81] Once this quorum is attained, the Convention will serve more like a model law for national data protection purposes. It should be pointed out that the provisions of the Convention are not very detailed, provoking an interpretation that they serve rather as a basis for national data protection in legislation in African countries, but nevertheless requiring only a modest amount of detail to be added.[82] So far (June 2019), only 14 Member States have signed the Convention, among whom only four (Senegal, Namibia, Guinea and Mauritius) have ratified it.

B. Evaluated Exam Scripts as Personal Data: A Prospective AU Interpretation

In delimiting its material scope, the AU Data Protection Convention defines personal data, as follows:

> 'Personal data means any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by African Union Legal Instrument reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.'[83]

The closeness to the definition of the notion of personal data by the European DPD and GDPR is quite obvious in these definitions, with the terms 'any information' and 'relating to', appearing in all three. As has already been discussed in the preceding section of this chapter, these terms allow for a very broad range of data to fall under data protection law and

data determined to be personal data automatically requires protection and processing restrictions in accordance with the said legal framework. And considering that, so far, there have been no official guidelines produced by the AU or case law from any intergovernmental African court providing a detailed, succinct, legal and African interpretation of the above definitions of personal data, it seems fairly logical that in applying (and hence interpreting) the above instruments in African courts, reference shall still be made to European legal opinions and case law to reach a decision as regards what should or should not constitute personal data. It therefore can be comfortably concluded that evaluated examination scripts, as was decided in *Nowak*, will most likely be equally interpreted as personal data in an African court.

This tendency of African legislators to follow and apply existing European approaches to solve legal disputes is not at all new. Makulilo has advanced two reasons for this trend in relation to data protection law: first, major legal systems in Africa namely common and civil law legal systems which are Western in origin, create fertile grounds for adaptability of European law. Though these systems were forcibly imposed on Africa by European countries during colonial rule as part of the colonial superstructure and an instrument of coercing Africans to participate in the colonial economy, they were inherited by African countries upon independence. African countries are therefore no strangers to the adaptation of 'foreign law'.[84] The second reason is economic motivation: Makulilo purports that African data protection legislations are modelled on the EU Data Protection Directive due to the desire of African countries to meet the 'adequacy' standard of the European law to attract foreign investment,[85] a consequence of the so-called 'Brussels Effect".[86] Europe represents the world's largest community of consumers[87] and is accompanied by powerful regulatory institutions capable of directly imposing decisions and sanctions on Member States, making it one solid, lucrative economic bloc. Given its economic weight, it remains a very attractive market for any ambitious business operator anywhere, rendering its regulations the benchmark to comply with even at global level.

It should also be pointed out that eventuality of an EU-interpretation, of personal data to include evaluated examination scripts as personal data on Cameroon soil is not very unlikely, if not certain. Not only are African countries (slowly but surely) adopting data protection laws[88] inspired by related EU legislations, Cameroon, like most formerly colonised African countries, is by no means a stranger to European statutory or case law. The country is bijurial, with the common law and civil law operating simultaneously on the territory, inherited from pre-independence British and French administration. To date, based on sections 11 and 15 of the 1955 Southern Cameroon's High Court Law, common law courts in the English-speaking regions of the country still rely on British jurisdiction and case law in litigations on matrimony, probate, tort and contracts between individuals,[89] while the French-orientated civil law courts still rely on legal reasoning from French judicial courts in rendering judgments in a range of civil litigations, especially on aspects not yet addressed by national law. Cameroon legal grounds therefore appear fertile enough for the adaptation of EU-inspired interpretation of data protection law within its national territory. This further favours the likely interpretation, upon an incorporation of the AU Data Protection Convention into

the country's national law, of evaluated examination scripts as personal data, including a corresponding right of access and verification.

C. Right of Access to Evaluated Exam Scripts as Personal Data under the AU Data Protection Convention

The AU Data Protection Convention also grants a right of access to individuals whose personal data are undergoing processing in the possession of the data controller. Without expressly using the term 'access', it states:

> 'Any natural person whose personal data are to be processed may request from the controller, in the form of questions, the following:
>
> Such information as would enable him/her to evaluate and object to the processing …'[90]

Paragraph (a), by obliging the data controller to provide the data subject with information which will enable him/her evaluate and object to the processing, creates an implied right of direct access to the processing, especially considering that the term 'information' is not defined under the Convention, and could include anything: from meaningless data[91] to a tangible, evaluated information script. Also, the phrase 'such information as would' and not 'such information about' widens the scope of what the data subject can actually request from the data controller, as information 'about' a data source could be made available to an individual without making available the data source itself. So under this provision, the data subject is not constrained to ask only for information about how his/her data is being processed, but can also ask to be provided with the data source itself, in so far as his/her evaluation and possible objection to the processing can be effectively done only by (directly) examining the data source. Just as in the DPD and GDPR therefore, there also is a right of access to personal data and hence evaluated examination scripts guaranteed under mainstream international African data protection law. The AU Convention also provides for a right of rectification in Article 17, which could be very useful in terms of requesting the re-evaluation of a marked examination script.

Worthy of note is the fact that unlike the DPD and GDPR, the AU Convention does not specify any limits to the right of access to processed personal information. With the Convention not yet in force and, to the best of the author's knowledge, the absence of case law or published African DPA decisions on the right of access to personal data, it is not clear to which exceptions they may be subject to in practice. Nevertheless, considering the relatively low level of privacy awareness in Africa[92] (which, interestingly, is not even listed in the catalogue of rights of the African Charter on Human and People's Rights of 1981), it can be expected that the right will be trimmed with a significant amount of restrictions in its practical enforcement. Current lack of case law in African courts on the subject, however, prevents the formulation of an informed decision on the issue in this chapter.

D. Right of Access to Personal Data under the AU Data Protection

Convention: Enforcement Mechanisms

Compared to Europe, data protection is new in Africa, with the first concrete steps taken jointly by African ICT ministers to protect online information privacy across the continent being in 2009.[93] This novelty is also reflected in its enforcement mechanisms, with the Data Protection Authority (DPA) appearing to be the sole entity with powers to ensure compliance with data protection rules; it is responsible for 'entertaining claims, petitions and complaints regarding the processing of personal data and informing the authors of the results thereto".[94] Interestingly (and rather unfortunately), the AU Data Protection convention does not provide for direct action against data controllers in the courts by individuals who feel their data protection rights have been violated, nor does it specifically create a liability relationship between the data controller and data subjects. This suggestively leaves all forms of redress to be addressed solely to the DPA, who is prescribed to be an independent national data protection authority with immunity from lawsuits (Article 11). The DPA is attributed broad powers in terms of data protection enforcement, including to investigate, issue opinions and warnings, inform judicial authorities of offences, impose monetary fines, or discontinue processing where fundamental rights are threatened (Article 12). The details and limits of these powers appear to be left to the discretion of Member States. The DPA's decisions, however, are subject to appeal before national courts.[95]

This section illustrates that an EU-inspired interpretation of AU data protection law by African legal practitioners would not only lead to evaluated examination scripts being considered personal data on African soil, but would also institute a right of access to these scripts for verification and possible re-correction. This would arguably play a significant role in deterring teacher–student abuses hinged on examination evaluations within the university and higher education in an African and third world setting. The following section examines some potential impacts which such a development would have on the fight against this phenomenon in Cameroon and also identifies and discusses some difficulties which could obstruct the practical enforcement of the right on university staff in the country.

V. Right of Access to Evaluated Exam Scripts as Personal Data in Cameroon: Potential Impacts on Teacher-Student Abuses

One of the objectives of the EU data protection reform of 2012 was 'reinforcing the right to information so that individuals fully understand how their personal data is handled'.[96] An objective upheld by the ECJ held in *Nowak*, granting a right of access to information (albeit personal information) to enable an individual appreciate the processing of data which shall have an impact on him. The literature already portrays the right to (public) information as a promotor of transparency and good governance,[97] but so too could it be a right to private (personal) information in terms of ensuring control by individuals over the processing of

their personal data. Access to data processing implies control over data, empowers the data subject[98] and indirectly imposes a duty of transparency on the data controller, which acts as a regulatory tool. Moreover, such access also gives the data subject the necessary tools to defend himself/herself (in this case, the marked examination script) as required by law in the event of a dispute or criminal proceeding.

This final section first presents a brief review of the current situation of the right of access to examination scripts in Cameroon universities. This is followed by a discussion on some potential regulatory effects which could result from an EU-inspired interpretation and application of students' data protection right of access to their examination scripts, as regards deterring teacher–student abuse and, subsequently, an examination as to how this right complements current criminal law in combatting this societal ill. This will then be followed by a brief identification and discussion of some hindrances which may be encountered in the practical enforcement of a right of access to evaluated examination scripts as a data protection right in Cameroon universities.

A. Right of Access to Evaluated Exam Scripts in Cameroon: A Brief Overview

Cameroon is yet to enact and adopt a comprehensive national data protection law and there currently is no legal mechanism explicitly providing students with a right to access their examination scripts after they have been corrected. The above-mentioned Decree No 93/035 of 19January 1993 and Law No 005 of 16 April 2001 are silent on the issue. So too is Decree No 08/0249/MINESUP of 11 September 2008 on the Common Status of Students in University Institutions of Cameroon. This implies that it is up to the discretion of the universities to determine whether to grant such a right to their students. The internal rules of the state universities are equally silent on this aspect; the closest thing to such a right being the right to request for a re-evaluation of the script if a student is dissatisfied with their grade; whether any re-evaluation shall be done is completely at the discretion of the Faculty Dean. In the University of Yaoundé I, for example, the student has a time limit of up to three days after the official date of publication of the examination results to file a complaint with the Faculty Dean and the latter retains the power whether to order such re-evaluation.[99] Also, the student can request apply to the Faculty Dean for a verification of the total count of marks on his/her script.[100] However, in both cases, the student does not have a right of direct access to the evaluated script.

This is strikingly different to what obtains in Europe, where some universities expressly provide their students with a right of access and verification of their evaluated examination scripts. Leiden University, for example, explicitly grants this right to its Master's students.[101]

B. Right of Access to Evaluated Exam Scripts: Deterring Sexual Abuse for Grades

Despite having ratified most international conventions protecting women's and children's rights, Cameroon is yet to develop and adopt specific, comprehensive, national policies directly addressing sexual abuse in institutions of higher learning in the country. Given this state of affairs, an EU-interpreted access to personal data in Cameroon could very well be a useful complementary tool to deter sexual abuse. If offering natural persons some level of control over their personal data empowers them with a right of access and verification, as illustrated in *Nowak*, then providing students with control over their evaluated examination scripts represents an opportunity to put some checks on the powers of their lecturers or professors. Students who enjoy a right to access their evaluated examination scripts and to verify the accuracy of this evaluation are, as a result, indirectly protected from being compelled by a university professor or member of staff to perform sexual favours for better grades.

If students have a fundamental right to access their evaluated examination script as personal data in the sense of Article 8 CFR, then they can always expose the unfair grading by a professor because the student rejected their sexual demands. This certainly would also auto-regulate related the conduct of such professors and discourage them from demanding sexual favours in return for allowing a student pass their course; being aware that a student can always verify and hence publicly question the professor's grading will certainly be a strong deterrent against unfair grading. Granting some personal data control over evaluated examination scripts could contribute significantly to ridding the university milieu of this behaviour.

C. Right of Access to Evaluated Exam Scripts: Checking the Teacher-Student Power Imbalance

As discussed above, professor–student relations can be viewed as an imbalanced relationship, with the student being the weaker party. Some professors tend to abuse such powers, which could take the form of failing a student for personal reasons, or if the student refuses to succumb to their 'sorting' antics, for example by failing to buy their handouts. Coupled with the fact that the professor reigns supreme in his course with very little or no supervision from the university administration, victimised students prefer silence than protest.

However, qualification of examination scripts as students' personal data in Cameroon could be a useful tool in balancing the professor–student power equation. As discussed above in *Nowak*, personal data protection guarantees a right of access to evaluated examination scripts. Consequently, as data controller institutions, universities shall suddenly have an obligation towards students to, upon request by the latter, grant them access to their evaluated examination scripts and proceed to process any reasonable rectification claims. Such right to access and rectification, because it exposes and subjects the professor's grading to the scrutiny of the student and that of any other person the student choses to share that data with, manifestly reduces the risk of abuse by the professor. As similarly concluded in the preceding subsection, knowing that their evaluation can be accessed (and hence questioned before others) at any time by their students would most certainly represent a strong incentive for

professors to grade the former accurately and fairly, thus tipping the balance of power in the students' favour.

D. Right of Access to Evaluated Exam Scripts: Complementing Criminal Law

As discussed in section II, Cameroon's criminal law offers protection to abused students principally in relation to sexual abuse, with the other identified incidents of teacher-student abuse being more of an educational discipline nature. Such protection is not easily enforced because most cases go unreported and the Cameroon criminal process, in practice, faces problems of logistics and trained personnel, similar to most third world countries. In light of this state of affairs, this chapter argues that the introduction of a right of access to evaluated examination scripts as personal data could lend a helping hand to criminal law by acting as an ex ante regulatory deterrent with regard to sexual abuse by lecturers in a Cameroon university setting.

Considering that lecturers usually use examination grades based on inaccessible evaluated examination scripts as bait to compel students to do their bidding, it appears much easier, instead of depending on criminal law for sanctions ex post, to deter such practices simply by rendering evaluated examination scripts accessible to students as a personal data protection right. Thus, giving them the opportunity to access and verify the accuracy and fairness of their grades. In other words, instead of relying on criminal procedure which is triggered only after the commission of an offence, a right of access to evaluated examination scripts will serve as a means of keeping professors in check; as knowing the student can have access to their script and see first-hand how they have been evaluated (and raise an alarm, if need be) would certainly compel the professor to grade the student fairly. This represents a less rigid and more practical defence mechanism for the students, instead of leaving everything to the bureaucracy of criminal procedure law which will require the issuing of warrants and other cumbersome investigatory processes to uncover evidence of teacher-student abuse.

E. The Right of Access to Evaluated Exam Scripts: Potential Enforcement Hindrances

In as much as a right of access to personal data, as illustrated above, could help regulate teacher–student abuse in Cameroon universities, its practical application may, however, be faced with some difficulties. The first probable hindrance can be deciphered in the overlapping and possible clash between the university administration as the state-instituted guarantor of the safety and well-being of the student on the one hand, and the national DPA as guarantor of the personal data protection of (Cameroon) citizens on the other. There could be a power struggle between both authorities: with the DPA being empowered by the AU Data Protection Convention to investigate and sanction data controllers, it appears to have the competence to order a professor or concerned/relevant university staff member (who, as

regards an evaluated examination script, is the data controller) to produce an evaluated script on the request of the evaluated student. However, professors generally are subject to administrative rules and regulations of their university and, such an order, depending on the circumstances, could possibly go against university rules or protocol. It, therefore, could be interesting to see, if the Convention is adopted and a DPA is created in Cameroon, how this and similar situation(s) will be managed between both authorities.

Another potential hindrance, closely related to the first, concerns the immunity status of both entities. While the AU Data Protection Convention grants judicial immunity to the DPA (Article 11), Cameroon university campuses also benefit from an inviolability status granted by national law. Article 49 of the Decree of 19 January 1993, for example, expressly forbids entry by any law enforcement officer into a university campus to investigate or establish a crime, or to execute any legal order on a university professor or member of staff without written authorisation from the regional state attorney (*Procureur Général*) presented to the Rector of the concerned university. Similarly, Article 9 of Decree No 2001/832/PM of 19 September 2001[102] also proclaims the inviolability of private university campuses. While looking forward to a regime of regulatory cooperation between university authorities and the DPA, this nevertheless leaves open the possibility of a university invoking its inviolability to block any investigatory mission into its campus by the DPA. Such situations may not be unusual especially where the investigation involves a high-ranking professor of the university, or an individual who holds significant political influence. Such circumstances could likely hinder the smooth investigation of an access complaint brought by an alleged abused student before the DPA, hence obstructing the practical applicability of a right of access. It is opined in any case that the national legislator will consider all these circumstances when adopting a national data protection framework guaranteeing a right of access to personal data (including evaluated examination scripts) in the country.

VI. Conclusion

This chapter argues that an EU-standard interpretation of the right of access to personal data under the AU Data Protection Convention (when it eventually becomes effective) in Cameroon by Cameroonian legal practitioners could contribute positively and significantly to prevent the propagation of teacher–student abuse on university campuses within the country. Professors do wield academic powers over students, which is necessary for the teaching and evaluation process. However, when such power is abused, there is a need for a system to provide checks and balances. *Nowak*, though not a case of on-campus abuse, happens to provide a useful tool to attain this need: giving examination candidates a data protection right of access and verification over their evaluated examination scripts. As noted by De Hert et al, data protection law tends to provoke the personal data processor into transparency and accountability by giving some level of control over that processing to the individual.[103] If individuals can verify and rectify their processed data, as they presently do under EU data protection law, then the processors will consequently adopt more responsible behaviour vis-

à-vis their personal data.

The same effect could be transposed into Cameroon's higher learning setting, to limit the progression teacher–student abuse. In the likely eventuality that personal data and a related right of access under the AU Data Protection Convention, when it becomes effective, are interpreted in Cameroon by Cameroonian legal practitioners as they are interpreted in Europe, then students could have a right of access and verification of their evaluated examination scripts, just as decided in *Nowak*. This, in turn, implies that professors or lecturers, who use unfair grading as their main weapon to force students into accepting their sexual propositions, 'sorting' transgressions or compel other forms of abuse, would suddenly be constrained to grade all students fairly. A student could then be able to gain access to and verify how their script was graded and, given the parallel data protection right to object to processing, could raise the alarm if he/she felt cheated. Moreover, the country does not currently have any official code of ethics binding university professors and lecturers, which further leaves room for ethical decadence within the higher learning corps. Also, despite abusive conduct such as sexual harassment being punishable by the Cameroon Penal Code, cases are rarely reported for fear of unwanted publicity or simply because students wish to avoid open confrontations with professors. Coupled with the problem, as in many third world countries, of slow judicial bureaucracy and the lack of qualified, trained judicial staff to effectively investigate such allegations. In light of the above, this chapter concludes that that the right of access under the AU Data Protection Convention, if interpreted as in *Nowak*, would provide another means of *ex ante* regulation against teacher-student abuse. This would complement the currently inadequate measures in place and ultimately provoke more responsible behaviour from university professors and members of staff, hence serving as a major deterrent against the phenomenon in Cameroon and other affected African countries in general.

References

Agborbechem, Peter Tambi, '"Sorting" in Examinations: Evaluating the Quality of Assessment in Universities in Cameroon' (2015) 4(5) *International Research Journal of Arts and Social Science* 93–97.

Bradford, Anu, (2012) 'The Brussels Effect' 1 *Nw UL Rev* 107.

De Hert, Paul and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in *Reinventing Data Protection?* (Springer, 2009) pp 3–44.

Floridi, Luciano, *The Online Manifesto: Being Human in a Hyperconnected Era* (Springer, Heidelberg New York Dordrecht London, 2015).

Galetta, Antonella, and Paul de Hert, 'A European Perspective on Data Protection and the Right of Access' in *The Unaccountable State of Surveillance* (Springer, Cham, 2017) pp 21–43.

Gellert, Raphael and Serge Gutwirth, 'The Legal Construction of Privacy and Data Protection' (2013) 29(5) *Computer Law & Security Review* 522–530.

Greenleaf, Graham and Marie Georges, 'The African Union's Data Privacy Convention: A Major Step Toward Global Consistency?' (2014) 131 *Privacy Laws & Business International Report* 18–21.

Hijmans, Hielke, 'Understanding and Assessing the Contribution of the CJEU to the Mandate Under Article 16 TFEU' in *The European Union as Guardian of Internet Privacy* (Springer, Cham 2016) pp 185–261.

Hustinx, Peter, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' *Collected Courses of the European University Institute's Academy of European Law, 24th Session on*

European Union Law (2013): 1–12.
Ladkin, Sharnae, 'Exploring Unequal Power Relations within Schools: The Authenticity of the Student Voice' (2017) 3 *Journal of Initial Teacher Inquiry* 37.
Lynskey, Orla, *The Foundations of EU Data Protection Law* (Oxford University Press, 2015).
Makulilo, Alex B, '"One Size Fits All": Does Europe Impose its Data Protection Regime on Africa?' (2013) 37(7) *Datenschutz und Datensicherheit-DuD* 447–451.
Makulilo, Alex B, 'The Context of Data Privacy in Africa' in *African Data Privacy Laws* (Springer, 2016) pp 3–23.
Menick, Mbassa D, 'Sexual Abuse at Schools in Cameroon: Results of a Survey-action Program in Yaounde' (2002) 62(1) *Medecine tropicale: revue du Corps de sante colonial* 58–62.
Morley, Louise, 'Sex, Grades and Power: Gender Violence in African Higher Education' in *CHEER Symposium, Annual SRHE Conference*, Newport, Wales, 14–16 December 2009.
Manyika, James, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh and Angela H. Byers, '*Big Data: The Next Frontier for Innovation, Competition, and Productivity*' (2011) Mckinsey Global Institute.
Ngwafor, Ephraim, 'Cameroon: The Law Across the Bridge: Twenty Years (1972–1992) of Confusion' (1995) 26(1) *Revue générale de droit* 69–77.
Nouwt, Sjaak, *Reinventing Data Protection?* eds Serge Gutwirth, Yves Poullet, Paul de Hert and Cécile de Terwangne (Springer, 2009).
Ohm, Paul, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2009) 57 *UCLA Law Review* 1701–1777.
Olivier, Michèle E, 'The Role of African Union Law in Integrating Africa' (2015) 22(4) *South African Journal of International Affairs* 513–533.
Purtova, Nadezhda, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10(1) *Law, Innovation and Technology* 40–81.
Rich, Cynthia, 'Privacy Laws in Africa and the Middle East' *The Bureau of National Affairs Privacy and Security Law Report* (2014) Bloomberg.
Rouvroy, Antoinette and Yves Poullet, 'The Right to Informational Self-determination and the Value of Self-development: Reassessing the Importance of Privacy for Democracy' in *Reinventing Data Protection?* (Springer, 2009) pp 45–76.
Schwartz, Paul M and Solove, Daniel J, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) *NYUL Rev* 86 1814.
Stamp, Mark, *Information Security: Principles and Practice* (John Wiley & Sons, 2011).
United Nations Economic Commission for Africa (UNECA) 'Harnessing ICT, Science and Technology for Development in Africa' UNECA Report. November 2007.
Wachter, Sandra and BD Mittelstadt, 'A Right to Reasonable Inferences: Re-thinking Data Protection Law in the age of Big Data and AI'. Available at: www.law.ox.ac.uk/business-law-blog/blog/2018/10/right-reasonable-inferences-re-thinking-data-protection-law-age-big.
Willott, Chris, 'Factionalism and Staff Success in a Nigerian University: A Departmental Case Study' (2014) *States at Work: Dynamics of African Bureaucracies* 91–112.
Zoneziwoh, MW, 'Sexual Violence on University Campuses: The Case of University of Buea' ALC Working Paper, 2011.

---

* This research is funded by the Erasmus Mundus program LAST-JD (Joint International PhD in Law, Science and Technology) coordinated by the University of Bologna.

1 Erasmus Mundus Doctoral Fellow, LAST-JD program, CIRSFID, University of Bologna.

2 Art 9 of the African Charter on Human and Peoples' Rights, Art 19 of the Universal Declaration of Human Rights, Art 10 of the European Convention on Human Rights, Art 19 of International Covenant on Civil and Political Rights.

3 See eg, s 72(b) of the African Union's Agenda 2063, published April 2015. Also see the United Nations Economic Commission for Africa (UNECA). '*Harnessing ICT, Science and Technology for Development in Africa*' UNECA Report. November 2007.

4 See eg, the United Nations Development Program 'The Africa Data Revolution Report', May 2016. Also see generally Manyika et al 'Big Data: The Next Frontier for Innovation, Competition, and Productivity' McKinsey Global Institute (2011).

5 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of

natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), published in Official Journal of the European Union, L 119, 4 May 2016.

[6] The 'onlife' coined by Luciano Floridi to denote 'the new experience of a hyperconnected reality within which it is no longer sensible to ask whether one may be online or offline' (Luciano Floridi, 'Introduction' in Luciano Floridi (ed), *The Online Manifesto. Being Human in a Hyperconnected Era* (Springer, 2015), 1.

[7] Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10(1) *Law, Innovation and Technology* 40–81, 41.

[8] See Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2009) 57 *UCLA Law Review* 1701–1777, 1756–1758. Also see Paul Schwartz and Daniel Solove (2011) 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' *NYUL Rev* 86 1814, 1877.

[9] Case C-434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECLI:EU:C:2017:994.

[10] Art 8 of the Charter of Fundamental Rights of the European Union of 7th December 2000 expressly provides for the right to 'The Protection of Personal Data'. This right was further reiterated in Art 16 of the Lisbon Treaty signed on 13 December 2007, which entered into force on 1 December 2009. See also Orla Lynskey, *The Foundations of EU Data Protection Law*. (Oxford University Press, 2015) pp 91–93.

[11] Paul de Hert and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in *Reinventing Data Protection*? (Springer, 2009) pp 5–6.

[12] For a general overview of the state of sexual abuse in Cameroon, see Mbassa D Menick, 'Sexual Abuse at Schools in Cameroon: Results of a Survey-action Program in Yaounde' (2002) 62(1) *Médecine tropicale: Revue du Corps de Santé colonial* 58–62.

[13] See generally Louise Morley, 'Sex, Grades and Power: Gender Violence in African Higher Education' in *CHEER Symposium, Annual SRHE Conference*, 14–16 December 2009, Newport, Wales.

[14] See Bukola Adebayo and Stephanie Busari, 'Lecturer demanded sex in return for better grades, Nigerian student says', CNN news article, published online on 23 May 2018. Available at: https://edition.cnn.com/2018/05/23/africa/sex-for-grades-university-nigeria-intl/index.html (last accessed 23 September 2018).

[15] See Francis Ajumane, 'Cameroon: female journalists rise up against sexual assault' Published online 15 August 2018. Available at: www.journalducameroun.com/en/cameroon-female-journalist-rise-sexual-harassment/ (last accessed 25 September 2018).

[16] Wondieh M Zoneziwoh, *Sexual Violence on University Campuses: The Case of University of Buea* (2011) 2 *ALC Working Paper* 7.

[17] Ibid at 6.

[18] Peter Tambi Agborbechem, '"Sorting" in Examinations: Evaluating the Quality of Assessment in Universities in Cameroon' (2015) 4(5) *International Research Journal of Arts and Social Science* 93–97 at 93.

[19] Chris Willott, 'Factionalism and Staff Success in a Nigerian University: A Departmental Case Study' (2014) *States at Work: Dynamics of African Bureaucracies* 91–112 at 95.

[20] Tambi (n 18). Ibid, 97.

[21] Ibid, 95.

[22] For a general literature review on power relations between teacher and student, see Sharnae Ladkin 'Exploring Unequal Power Relations within Schools: The Authenticity of the Student Voice' (2017) 3 *Journal of Initial Teacher Inquiry* 37.

[23] Ladkin (n 22) at 38.

[24] Ibid.

[25] This phenomenon also occurs in Western societies. See eg, Kaitlyn Schallhorn, 'Professor Fails Student for Refusing to Condemn her Christian Faith'. Published 5 May 2015. Available at: www.campusreform.org/?ID=6490 (last accessed 26 September 2018).

[26] Art 29(3) of Law No 005 of 16 April 2001 laying down Guidelines for Higher Education in Cameroon.

[27] Art 35 of Law No 98/04 of 14 April 1998 laying down Guidelines for Education in Cameroon.

[28] Ibid, Art 54.

[29] Ibid, Art 56.

[30] Ibid, Art 302, Law No 2016/007 of 12 July 2016 establishing the Cameroon Penal Code.

[31] See n 14.

[32] See generally Transparency International *Global Corruption Report 2007: Corruption in Judicial Systems* Cambridge.

[33] Jeanine Fankam, 'Enseignement supérieur: un code éthique pour les enseignants en gestation'. Published 7 June 2019. Available at: www.cameroon-tribune.cm/article.html/26118/fr.html/enseignement-superieur-un-code-ethique-pour-les-enseignants-en-gestation (last accessed 20 June 2019).

[34] Ameesh Divatia, 'GDPR and the "Security by Compliance" Mistake', 22 July 2018. Available at: www.forbes.com/sites/forbestechcouncil/2018/07/02/gdpr-and-the-security-by-compliance-mistake/#1ca90fb5ecc4 (last accessed 29 September 2018).

[35] Sjaak Nouwt, *Reinventing Data Protection?* eds Serge Gutwirth, Yves Poullet, Paul de Hert, and Cécile de Terwangne, (Preface) (Springer, 2009) p x.

[36] Peter Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation. *Collected Courses of the European University Institute's Academy of European Law,* 24th Session on European Union Law (2013): 1–12, 2.

[37] It should be pointed out that although the Data Protection Directive has now been repealed by the General Data Protection Regulation, this does not affect the concept of personal data as it was under the Directive. See Opinion No 3 of Advocate General Kokott in Case C-434/16 *Nowak v Data Protection Commissioner* (n 9).

[38] GDPR, Art 4(1).

[39] Purtova (n 7) 49, 66

[40] The former EU advisory authority on the matters of data protection, composed of national data protection authorities and headed by the European Data Protection Supervisor. With the coming into force of the GDPR in May 2018, it was replaced by the European Data Protection Board (EDPB).

[41] Article 29 Working Party Opinion 4/2007 on the concept of personal data, 20 June 2007 ('WP 136') 4.

[42] Ibid at 6.

[43] Ibid.

[44] Ibid at 5. Also GDPR, Art 2(1).

[45] Ibid at 7.

[46] Ibid at 9.

[47] Ibid.

[48] Ibid at 10.

[49] Ibid.

[50] Ibid at 10–11.

[51] *Nowak v Data Protection Commissioner* (n 9).

[52] Ibid; Opinion No 2 of Advocate General Kokott.

[53] Ibid at [19].

[54] Ibid at [21].

[55] Ibid at [24].

[56] *Nowak* (n 9) at [34].

[57] Ibid at 35.

[58] Purtova (n 7) at 71.

[59] *Nowak* (n 9) at [39]. But see *YS and others* (17 July 2014, ECLI:EU:C:2014:2081) [46] where the ECJ created a

precedent to the effect that the right to access a document affecting one's interest is not absolute and may be denied in certain circumstances (in this case, if it will lead to granting access to administrative documents). The courts usually balance the right of against other fundamental rights and interests, to determine its enforcement. See Antonella Galetta and Paul de Hert, 'A European Perspective Data Protection and the Right of Access' in *The Unaccountable State of Surveillance* eds Clive Norris, Paul de Hert, Xavier L'Hoiry, Antonella Galetta (Springer, 2017) pp 21–43.

60 Lynskey (n 10) 46.

61 Data Protection Directive, recital 25.

62 Galetta and de Hert (n 59) p 25. Also see generally Raphael Gellert and Serge Gutwirth 'The Legal Construction of Privacy and Data Protection' (2013) 29(5) *Computer Law & Security Review* 522–530.

63 GDPR, recital 63.

64 *YS and Others* (n 59) Note 58 [44].

65 *Nowak* (n 9), Opinion of Advocate General Kokott [26].

66 Ibid at [50].

67 Ibid at [51].

68 See GDPR, Art 23 which lists the preservation of 'general public interest' and, slightly relevant to *YS and Others*, independence of judicial proceedings among the reasons for which the right of access may be restricted.

69 *YS and Others* (n 59).

70 Sandra Wachter and BD Mittelstadt. 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI'. Available at: www.law.ox.ac.uk/business-law-blog/blog/2018/10/right-reasonable-inferences-re-thinking-data-protection-law-age-big.

71 WP 136 (n 41) 6.

72 *Nowak* (n 9) at [54].

73 Ibid at 51.

74 GDPR, Arts 5(1)(a), 13, AU Data Protection Convention.

75 Art 3, Constitutive Act of the African Union.

76 Extra-Ordinary Conference of African Union Ministers in Charge of Communication and Information Technologies (2009) *Oliver Tambo Declaration.* Johannesburg, South Africa: African Union.

77 Ibid at 4.

78 African Union Convention on Cyber Security and Personal Data Protection, Art 8(1).

79 'Legal integration' is significantly missing from the objectives of the AU enlisted under Art 3 of the Constitutive Act.

80 Michèle E Olivier, 'The Role of African Union Law in Integrating Africa' (2015) 22(4) *South African Journal of International Affairs* 513–533, 514.

81 African Union Convention on Cyber Security and Personal Data Protection, Art 38.

82 Graham Greenleaf and Marie Georges, 'The African Union's Data Privacy Convention: A Major Step Toward Global Consistency?' (2014) 131 *Privacy Laws & Business International Report* 18–21.

83 African Union Data Protection Convention, Art 1, para 36.

84 Alex B Makulilo, 'One Size Fits All: Does Europe Impose its Data Protection Regime on Africa?' (2013) 37(7) *Datenschutz und Datensicherheit-DuD* 447–451.

85 DPD Art 25 and now GDPR Art 45 restrict data transfers of EU residents to countries which do not have an 'adequate' standard of personal data protection. Also see Makulilo, ibid, 450.

86 Term coined in 2012 by Professor Anu Bradford to denote the soft power which EU regulations have worldwide, due to the size of its consumer base and strength of its regulatory institutions.

87 Anu Bradford, 'The Brussels Effect' (2012) 1 *NW UL Rev* 107.

88 By 2015, 17 African countries had adopted comprehensive personal data protection legislation, namely Angola, Benin, Burkina Faso, Cape Verde, Gabon, Ghana, Ivory Coast, Lesotho, Madagascar, Mali, Mauritius, Morocco, Senegal,

Seychelles, South Africa, Tunisia and Western Sahara. See Cynthia Rich, 'Privacy Laws in Africa and the Middle East' (2014) *The Bureau of National Affairs, Privacy and Security Law Report.* Bloomberg: 1.

89 Ephraim Ngwafor, 'Cameroon: The Law Across the Bridge: Twenty Years (1972–1992) of Confusion' (1995) 26(1) *Revue générale de droit* 69–77. 71

90 AU Data Protection Convention, Art 17.

91 Purtova (n 7) 52.

92 See generally Alex Makulilo, 'The Context of Data Privacy in Africa' in *African Data Privacy Laws* (Springer, 2016) pp 3–23.

93 On 2–5 November 2009, African Union state ministers in charge of ICTs in their various countries met in Johannesburg and adopted what was referred to as the Oliver Tambo Declaration, in which they urged the African Union Commission to 'develop … a convention on cyber legislation based on the Continent's needs and which adheres to the legal and regulatory requirements on electronic transactions, cyber security, and personal data protection'.

94 AU Data Protection Convention, Art 12(2)(e).

95 Ibid, Art 12(6).

96 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World, A European Data Protection Framework for the 21st Century, COM (2012) 9 final, at 6.

97 Hielke Hijmans, 'Understanding and Assessing the Contribution of the CJEU to the Mandate Under Article 16 TFEU' in *The European Union as Guardian of Internet Privacy* (Springer, 2016) pp 185–261, 236 et seq.

98 Ibid at 175.

99 Art III.2.3 of the Internal Pedagogical Regulations of the University of Yaoundé I of 27 December 2012. Available at: www.webuy1.uninet.cm/uy1/images/fichiers_attaches/Reglement_Interieur_UY1.pdf (last accessed 27 September 2018).

100 Ibid, Art III.2.6.

101 Art 4.8.1 of the Course and Examination Regulations of the Master's Programme in International Relations and Diplomacy, 2018–2019, Leiden University. Available at: www.organisatiegids.universiteitleiden.nl/binaries/content/assets/governance-and-global-affairs/oeren/oeren-juli-2018/oer-m-ird-2018-2019.pdf (last accessed 28 September 2018).

102 Decree No 2001/832/PM of 19 September 2001 to lay down general provisions applicable to Private Institutions of Higher Learning.

103 Nouwt (n 35).

10

The Proposed ePrivacy Regulation

The Commission's and the Parliament's Drafts at a Crossroads?

ELENA GIL GONZÁLEZ,[1] PAUL DE HERT[2] AND VAGELIS PAPAKONSTANTINOU[3]

Abstract

The EU's Digital Single Market Strategy aims to increase trust and security in digital services. A reform of the EU personal data protection regulatory framework through the introduction of the General Data Protection Regulation (GDPR) was a key step to increasing trust in the security of digital services. Following the reform of the GDPR, the strategy also includes the review of the ePrivacy Directive (Directive 2002/58/EC). Indeed, on 10 January 2017, the European Commission presented a proposal for an ePrivacy Regulation to be in force on 25 May 2018, simultaneously with the GDPR. However, this ambitious timeline has suffered delays and the proposal is currently going through the European Union legislative process. On 26 October 2017, the European Parliament voted in favour of the amendments proposed by the Committee on Civil Liberties, Justice and Home Affairs (LIBE) in plenary session. This chapter aims to highlight specific aspects of the ePrivacy Regulation draft, in its Summer 2019 state, to shed light upon certain of its most important elements. While the new Commission after the elections of June 2019 awaits appointment, we consider it important, during this stage of the law-making process, to take a photograph of developments so far, which include the Commission's original draft and the Parliament's response (the Council is yet to provide its final position). In this way, future comparisons with the final wording and the reasoning behind them, will be facilitated.

Keywords

ePrivacy, GDPR, tracking, metadata, consent.

I. Introduction

The EU's Digital Single Market Strategy aims at increasing trust and security of digital services. For this, the reform of the EU personal data protection regulatory framework

through the introduction of the General Data Protection Regulation[4] (GDPR) was a key step to increase trust in the security of digital services.[5] Following the reform of the GDPR, the strategy also included a review of Directive 2002/58/EC.[6] Indeed, on 10 January 2017, the European Commission presented a proposal for a Regulation on Privacy and Electronic Communications, repealing the ePrivacy Directive.[7] The future ePrivacy Regulation aims to achieve the establishment of a new personal data protection legal framework by complementing and particularising the GDPR.[8] The proposed ePrivacy Regulation takes account of the important technological and economic developments in the sector of electronic communications and aims to modernise existing principles according to the new practices.[9] It aims to promote a high level of protection of confidentiality in communications regardless of the technology used.[10]

While the ePrivacy Directive is formed by 49 recitals and only 19 Articles, the draft ePrivacy Regulation consists of 43 recitals and 29 Articles, being a larger corpus of provisions, divided into seven chapters. It is structured as follows: Chapter I contains general provisions dealing with the subject matter, the scope and definitions. Chapter II deals with the protection of electronic communications data, information stored in terminal equipment and information rights regarding privacy settings. Further, Chapter III refers to end users' rights regarding electronic communications. Chapter IV deals with supervisory authorities and their cooperation and consistency procedures, leaving Chapter V for remedies, liability and penalties. Chapter VI examines delegated and implementing acts, while some final provisions can be found in Chapter VII.

The aim was for the new ePrivacy Regulation to be in force on 25 May 2018, simultaneously with the GDPR. However, this ambitious timeline has suffered delays and the proposal is currently going through the European Union legislative process. On 26 October 2017, the European Parliament voted in favour of the amendments proposed by the Committee on Civil Liberties, Justice and Home Affairs (LIBE) in plenary session. The final version of the Council is not known at the time of writing (Summer 2019). In this scenario, there is an even more pressing reason to reach a final version of the text in light of the statement by the European Data Protection Board (EDPB) urging the Commission, Parliament and Council to replace the Directive 'as soon as possible'.[11]

The aim of this chapter is to highlight specific aspects of the draft ePrivacy Regulation in its summer 2019 state and to shed light upon certain of its most important elements. We consider it important, at this stage of the law-making process and while awaiting the appointment of the new Commission after the elections of June 2019, to take a photograph of developments so far, which include the Commission's original draft and the Parliament's response (the Council is yet to provide its final position). In this way, future comparisons with the final wording and the reasoning behind them, will be facilitated. To this end, this chapter is structured as follows. We begin by briefly reviewing the relationship between the ePrivacy Regulation and the GDPR, particularly with regard to the GDPR being *lex generalis* and the ePrivacy Regulation *lex specialis* or the fact that both normative frameworks are shaped as regulations, therefore directly applicable in all Member States (Section II).

We then comment on the material and territorial scope of the Regulation. The ePrivacy

Regulation has formally expanded its scope to cover Over-the-Top providers and to deploy extraterritorial effects, so that it will be enforceable even to providers located outside the EU or if the processing does not take place in the EU, as long as the other conditions are met (Section III).

Further, we review an important set of provisions of the ePrivacy Regulation, namely, the provisions dealing with the protection of confidentiality of communications, in particular information stored in and emitted by terminal equipment. For each case we describe the existing situation under the ePrivacy Directive (ePD) and the changes sought with the newer reform to provide a context that helps explain the development of the legal framework (Section IV). Our final section (Section V) focuses on the issue of consent. The Commission's proposal for an ePrivacy Regulation, departing from a general prohibition, provides exceptions that allow the processing of personal information in specific cases. In brief, these exceptions can be summarised as information being allowed to be processed when necessary or with users' consent. Indeed, the ePrivacy body heavily relies on users' consent to legitimise non-necessary uses of otherwise private data. We will remark upon this fact while commenting on how contemporary privacy settings could be affected under the proposed updated rules.

II. The Relationship between the ePrivacy Regulation and the GDPR: Is There Life Beyond Personal Data Processing?

The ambition of the EU during the efforts to update its data protection framework and related rules was, among other things, to ensure a more coherent application of the rules in the Union, leading to a greater degree of protection for people and legal certainty for organisations. To this end, is it important that the proposed ePrivacy Regulation is aligned with different sets of rules to provide a high level of protection for users of electronic communications services and a level playing field for all market players.

The GDPR is apparently the elephant in the law-making room, a point of reference the ePrivacy Regulation cannot possibly ignore. As regards their relationship, a number of points can be raised.[12] First, the GDPR sets the *lex generalis* of data protection in Europe; this, therefore, applies to all matters related to the processing of personal data, regardless of the sector, provided that there is no sector-specific law to apply. Electronic communication is one – if not the only one – of these fields. In this sense, the proposed ePrivacy Regulation is *lex specialis* to the GDPR and will particularise and complement it as regards electronic communications data that qualify as personal data. In particular, the areas of unsolicited marketing, tracking technologies (eg cookies) and confidentiality are covered in a more specific way in the ePrivacy Regulation. However, in those matters where the proposed ePrivacy Regulation is silent, the GDPR will apply by default (eg certain controllers' obligations). This has resulted, for instance, in the repeal of some provisions from the ePD,

such as the security obligations of Article 4, to avoid unnecessary duplication.[13]

Second, the selection of a Regulation instead of a Directive as the legal instrument of choice for both GDPR and the new ePrivacy framework is orientated towards creating a more uniform regime across Member States. Regulations eliminate the need to enact national legislation, thereby enhancing consistency among ePrivacy and the GDPR.

Most importantly, however, while the GDPR primarily enshrines Article 8 of the Charter of Fundamental Rights of the EU[14] to protect personal data, the ePrivacy Regulation is targeted at Article 7 of the Charter, which protects a person's private life, home and communications. Therefore, while the GDPR ensures the protection of personal data, the ePrivacy Regulation ensures the confidentiality of communications, which may also contain non-personal data and data related to a legal person. This is one of the reasons why it is useful to have a separate instrument to ensure an effective protection of Article 7 of the Charter.[15] However, some have argued that most of the processing operations covered by the ePrivacy Regulation would entail personal data and therefore would be covered by the GDPR in a more flexible way. Using this argument, the ePrivacy Regulation would impose unnecessary burdens on providers of electronic communications services.[16]

A final, fourth, point refers to supervision: consistency between the ePrivacy regime and the GDPR could also be enhanced through the decision to make the same independent supervisory authorities responsible for monitoring compliance of both sets of rules.

III. The Material and Territorial Scope of the Draft ePrivacy Regulation

As internet and digital technologies know no borders, the dimension of the problem goes beyond the territory of a single Member State; action at the EU level is an added value.[17] With that in mind, the Commission has, in its proposal, broadened the material and territorial scope of the ePrivacy Regulation in relation to that of the ePD. However, the Commission's proposal has raised several issues related to the scope of the ePrivacy Regulation, as well as its definitions and exceptions. This is why we will present the suggested changes relating to the material and territorial scope of ePrivacy Regulation in their current status (Summer 2019).

A. Material Scope (Article 2 ePrivacy Regulation)

The ePD deploys its effects only over traditional telecom operators, who were the main collectors of communications data at the time of its adoption. In addition, it covers only publicly available e-communications services in public networks, leaving aside the debated cases of publicly accessible private communications networks (such as WiFi connections in airports or restaurants).[18] This limitation was evident even at the time of its adoption.[19] Through advances in new technologies, new functionally equivalent services have arisen,

making clear that the scope of the ePD has become too narrow.

Due to all this, the Commission aims, in its proposal, to widen the ePrivacy Regulation scope to cover not only traditional telecom providers but also new market players, the so-called OTT providers such as voice-over IP, text message and e-mail providers. Article 2 of the ePrivacy Regulation contains the rules on its material scope. Although the main principle has remained untouched among the two versions examined in this chapter, the wording used by the Parliament clarifies that of the Commission.

Article 2 is drafted by the Commission stating that the Regulation applies to 'the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services and to information related to the terminal equipment of end-users'. However, the ePrivacy Regulation explicitly excludes its application over electronic communications services which are not publicly available (Article 2.2(c)). These include phone calls, Facebook messenger messages, e-mails, etc.

While these changes already represented an expansion in the scope of the law compared to the ePD, the Parliament amendments further clarify the scope of the ePrivacy Regulation on the basis of the LIBE report, which stated that the wording seemed too narrow.[20] Following this report, the amended version of the Parliament includes in the body of Article 2 what was already mentioned in recital 8. Therefore, the Parliament explicitly extended the scope of the ePrivacy Regulation to information processed by terminal equipment of end-users, the placing in the market of software permitting electronic communications (eg Google Chrome services), the provision of public available directories and the sending of direct marketing electronic communications.

In addition, the Commission proposal of Article 2 seems to protect only confidential communications in *transit*, but not when stored.[21] Under this interpretation, the ePrivacy Regulation would only apply during the time communications are taking place and the GDPR would apply after the recipient receives the data where personal data is at stake. This is particularly relevant in the current digital environment, where data remains stored after its transmission as part of the service (as could be the case for storage in the cloud or the services of WhatsApp) and the GDPR provides for more flexible options to process data than ePrivacy Regulation. In this scenario, following the recommendations of WP29,[22] the Parliament clarifies recital 15 to make clear that also stored data is to be protected under the ePrivacy Regulation.[23]

As regards another Parliament intervention, the Commission's proposal uses the definition of 'electronic communications services' set forth in the Electronic Communications Code to ensure an effective and equal protection of end-users when using functionally equivalent services.[24] Under this, the concept of electronic communications services is defined as services provided by means of electronic signals over, for example, telecommunications or broadcasting networks. The term, however, excludes services controlling editorial content and information society services which do not involve the transmission of signals.

However, the Parliament is of the idea that the ePrivacy Regulation should be a stand-alone instrument and contain its own provisions, not depending of the Electronic

Communications Code. Therefore, the Parliament suggests that the definitions from the Code be incorporated in the Proposal, taking into account any adaptation needed. In this regard, for instance, the definition of communications metadata has been amended to clarify the concept.

In any event, what seems clear is that, through this definition, the ePrivacy Regulation's current draft aims to expand its scope to include the so-called 'Over-the-Top' (OTT) communications services, which are not clearly included in the ePD, creating unequal rules for similar service providers. OTT communications services are those provided over the public internet and are functionally equivalent to more traditional communication means and therefore have a similar potential to impact on the privacy and right to secrecy of communications of people.[25] Where years ago it was only possible to make calls through ordinary telecom means, we can now make phone calls over the internet by using the services provided, for instance, by Skype. In addition to the OTT services covered by the definition of 'electronic communications services' of the Electronic Communications Code, the ePrivacy Regulation as amended by the Parliament also covers:

(a) interpersonal communications services, such as WhatsApp;
(b) services consisting wholly or mainly in the conveyance of the signals, like machine to machine services and for broadcasting services, when the information can be related to the identifiable end-user receiving the information, such as Netflix;[26] and
(c) services which are not publicly available, but provide access to a publicly available electronic communications network, for instance, a VPN of a company that gives access to the outside internet.

The explicit clarification that the ePrivacy Regulation also covers machine-to-machine interactions is relevant, as connected devices that communicate with each other is rapidly increasing due to the expansion of the Internet of Things.[27] As argued by the WP29, this is a desirable fact, as those communications can also reveal personal information. However, for this same reason, WP29 also reflects that pure machine-to-machine communications should be left out of the scope of the ePrivacy Regulation when they have no impact either on privacy or the confidentiality of communications.[28]

The expansion of the ePrivacy Regulation scope to include OTT providers is a relevant change and it was also one of the facts that questioned the most the effectiveness of the ePD to provide users' protection. It could be safe to state that, nowadays, the majority of EU consumers use OTT services on a daily basis. Nevertheless, it should also be noted that while debate has been generated around services that enable communication just as an ancillary service for another core service (eg videogames where players can chat or dating apps like Tinder), the version of the Commission included them in the scope of the ePrivacy Regulation, while the version of the Parliament excludes them.[29]

B. Territorial Scope (Article 3 ePrivacy Regulation)

One of the most important aspects of the ePrivacy Regulation proposal is the widening of its territorial scope. The ePD is directed to 'the processing of personal data in connection with

the provision of publicly available electronic communications services in public communications networks in the Community'.[30] The Commission's draft for the ePrivacy Regulation, however, follows the path of the GDPR and aims at an extraterritorial effect. Article 3 establishes that it will apply to the data processed in connection to the provision of electronic communications services provided to end users located in the EU, even if the provider is established outside the EU (ie even if the processing does not actually take place in the EU). Moreover, in order not to deprive end users in the EU of effective protection, the ePrivacy Regulation would also apply to electronic communications data processed in connection with the provision of electronic communications services from outside the Union to end users in the Union. Along the same lines in the Commission's original draft. In those cases where the provider is not located in the Union, a representative must be appointed in writing. Its duties would encompass provision of the necessary information to supervisory authorities and end-users on all issues derived from the ePrivacy Regulation.

The Parliament has detailed and clarified the provisions regarding the appointment of a representative to gain consistency with the changes made in relation to the activities added in the material scope. Thus, the Parliament's version states that representatives must also be named for providers not established in the EU in the case of offering of software permitting electronic communications, publicly available directories, or direct marketing electronic communications, irrespective of whether a payment of the end-user is required. Thus, it has amended this provision to state that the ePrivacy Regulation will apply to end-users in the EU, activities that are provided from its territory and the processing of information related or by a terminal equipment when the device is in the EU.[31]

Under this provision, for instance, Chinese social networks such as PengYouWan would need to name a representative if they wish to direct their services at users in the EU. This could lead, as has been the case with the GDPR, on some providers geo-blocking the EU area until they are compliant, an example of which can be seen in the image below.

Figure 10.1 Example of geo-blocking from *Los Angeles Times*



IV. Confidentiality of Communications: Protection of Electronic Communications of Natural and Legal Persons in the Draft ePrivacy Regulation

Protection of the confidentiality of communications is an important part and equally a raison d'être, for the ePrivacy regulatory framework. The reason behind the protection of electronic communications data is that the content of electronic communications may reveal highly sensitive information about the natural persons involved in the communication (personal experiences, emotions, sexual or political preferences, etc), the disclosure of which has clear privacy implications.[32] Moreover, metadata derived from electronic communications, may also reveal very sensitive and personal information, as expressly recognised by the CJEU.[33]

The explicit protection of both content and metadata is of enormous importance nowadays. Back in the time confidentiality of content data could be seen as being more relevant due to its higher potential to reveal information about end users' behaviour, thoughts or inclination to certain ideas. However, current technologies enable easier and cheaper collection of vast amounts of metadata from which patterns and behaviours can be also been observed. Think for instance, about the possibility of inferring the religious beliefs of a person if one can gain access to his phone location data, revealing that he or she goes to a specific church every week. The examples are countless. In addition, while content data will, almost always, be in unstructured format and, therefore, more difficult to analyse, metadata can be gathered in structured formats and analysed in (near)real time. Together with this, it is

important to note the ever-increasing torrents of data coming from the Internet of Things and the connected society. This widens the ability to analyse end-user's data in an attempt to monetise it, with the subsequent violation of privacy. The result is that individual pieces of data that may have been innocuous years ago are can now expose private information, much of which can also qualify as personal data. These reasons justify the need for a clearer definition of metadata and its protection.

In this section we will analyse the original provisions of the draft ePrivacy Regulation, as suggested by the Commission and compare them to the Parliament's recommendations and amendments. Also, to understand the context that led to the ePrivacy Regulation being drafted in a specific way by the Commission, each subsection details the existing situation under the ePD, as well as the main conclusions of the REFIT evaluation carried out by the European Commission[34] to assess the modifications required. Overall, the ePrivacy Regulation has chosen a general approach consisting of broad prohibitions, narrow exceptions and the targeted application of the concept of consent, which the WP29 has explicitly welcomed.[35]

A. Metadata in the Draft ePrivacy Regulation: Is Merging Location and Traffic Data a Good Idea?

The ePD provides for Member States to ensure confidentiality of communications and of related traffic data in public communication networks and services. Therefore, listening, tapping, storing or engaging in other kinds of interception or surveillance of communications and the related traffic data without the consent of the citizen concerned was prohibited (except when legally authorised). This provision covers both the content of the communication (eg the voice in a phone call) and the related traffic data (eg the time of the call). That data can be used with the consent of the user, or if anonymised.

In this regard, 'traffic data' is defined in Article 2(b) ePD as 'any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof' (eg the time of the call, as mentioned, or the phone number). Under Article 6 ePD, traffic data can only be used if anonymised, for billing purposes or with the consent of the user for marketing or value-added services.

In the same way, the ePD defines 'location data' in Article 2(c) as 'any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service'. Location data other than traffic data can be used under the ePD when anonymised, or with the consent of the user when it was intended to be used for value added services (Article 9 ePD). An example of a value-added service using location data is a GPS on our mobile phones.

The REFIT evaluation found that these rules are not replicated in other legal instruments, such as the GDPR, therefore, being necessary under an eprivacy regulatory framework. However, under the ePD, these rules are not fully effective in protecting the confidentiality of communications. Some of the reasons are, for instance, the exclusion of OTT services[36] or the outdated wording (which did not include automatic intrusions without human

intervention). For instance, in an internet environment, the same data may constitute content for one provider while being traffic data for other. However, the definitions as set out in the ePD do not reflect this situation. High protection standards of all electronic communications data are equally important, as nowadays the processing of data about the communication, such as the URL of websites accessed, may be as revealing as the content of the communication itself.[37] Further, while the GDPR allows for several bases for the processing of personal data (such as consent, performance of a contract or legitimate interests) the ePD only allows for consent and restricts the processing to the provision of value-added services. Therefore, the ePD aims at a more restrictive approach than the GDPR.[38]

In light of all this, the REFIT evaluation concludes that confidentiality of communications should be protected under the ePrivacy rules, as they enhance people's rights. Specifically, the added value of these rules lies in the need to have a high level of protection and harmonised standards, an objective that cannot be achieved with national laws. Further, it was found that the concepts of confidentiality of electronic communications, traffic and location data needed to remain unified.[39]

In response to the above, the ePrivacy Regulation as originally drafted by the Commission aims to protect both the content of communications and the related metadata. In this context, the Commission's draft drops the concept of traffic data and location data and uses 'metadata' instead. Under the Commission's draft ePrivacy Regulation, the concept of metadata contraposes that of content.[40] In particular, the ePrivacy Regulation contains a more specific definition of 'electronic communications metadata' as:

> 'data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the terminal equipment processed in the context of providing electronic communications services, and the date, time, duration and the type of communication'.[41]

This new definition covers what the ePD defines as traffic data and location data. The reason for this merge lies in the increasing generation of data and the computing capacity to store and analyse it. As a result of these technological advancements, even when some electronic communications data were deleted, the analysis of traffic and location data coming from multiple sources could show emerging patterns which could subsequently lead to the creation of individual and group profiles, increasing the potential privacy impact. This is also especially important due to the covert and unexpected ways that could lead to massive collection and analysis of data. Merging rules on traffic data and location data (ie creating metadata provisions) would therefore offer a higher degree of protection and set clearer rules for all parties.[42]

However, the definition of 'electronic communications content' has been worded by the Commission in its proposal as:

> 'the content transmitted, distributed or exchanged by means of electronic communications services, such as text, voice, videos, images, and sound. *Where metadata of other electronic communications services or protocols are transmitted, distributed or exchanged by using the respective service, they shall be considered electronic communications content for the respective service*' (emphasis added).[43]

For instance, when taking a photograph, the picture itself would be content, whereas the

camera settings, the time and date, would be metadata. Also, when sending an email, the body of the e-mail, the subject and the attached documents would be the content, whereas the sender and the recipient of the e-mail would be metadata. More complex information can also qualify as metadata, such as that which can be parsed out of the IP traffic, such as website names, source and destination addresses, etc.[44] However, there is a fine-drawn detail in the distinction of content and metadata (see the emphasised sentence). In essence, the ePrivacy Regulation provides for differences so that the same data can be considered content or metadata depending on the service provider. To understand this, we will consider the e-mail example. What we said in the previous example is true for the e-mail provider. However, for the internet service provider, the body of the e-mail, subject, attached documents, sender and recipient will be the content of the IP packets routed by the provider.[45]

B. The Protection of Metadata under Articles 5 and 6 of the Draft ePrivacy Regulation

Taking the above into consideration, Article 5 of the ePrivacy Regulation has been configured by the Commission as a general rule, which provides the confidentiality of all electronic communications data. Since this is a fundamental right recognised by the Charter, any interference must be limited to what is strictly necessary and proportionate in a democratic society. Consequently, electronic communications data can only be used in certain exceptional situations, provided in Articles 6 and 7 of the ePrivacy Regulation.

Under Article 6.1 of the draft ePrivacy Regulation, electronic communications data, which encompasses both content and metadata, can only be used by providers of electronic communications networks in two situations: (i) to achieve the transmission of the communication; and (ii) to maintain or restore security of the network, or its availability, integrity or confidentiality, as well as detect technical errors in the transmission. In this latter case, the Parliament's amended text introduced the possibility of data being used by both the providers, or other third parties acting on their behalf. This could be the situation, for example, when a provider contracts with an external security company to ensure the communications are held securely and are free from technical error.

The Parliament amended the Commission's ePrivacy Regulation draft to explicitly set a strict threshold for the use of electronic communications data, by requiring that data be processed 'only if it is technically necessary', whereas the wording of the Commission limited the use of electronic communications data to what is 'necessary'. In addition to this provision, encompassing both content and metadata, the ePrivacy Regulation creates separate exceptions that allow for the use of electronic communications content and metadata.

Article 6.2 of the ePrivacy Regulation establishes that metadata can be used when necessary for certain purposes. Again, the Parliament amended the Commission's text to raise the bar from what is 'necessary' to what is 'only strictly necessary'. Processing electronic communications metadata is allowed in the following circumstances. Firstly, for billing purposes,[46] for instance, to ensure a person benefiting from the service has not

fraudulently sent the bill to another person, as well as for prevention of abusive use and subscription of electronic communications services.[47] In this case, only the necessary metadata may be kept until the end of the period during which a bill or an undue payment may be lawfully challenged or when technically necessary for security purposes described above.[48]

Secondly, metadata can be used when necessary to meet mandatory quality of service requirements[49] according to specific legislation. An example of this would be where the provider needs to adapt the quality of an image to the settings of your screen. Thirdly, other than in these necessary cases, metadata can only be used with the consent of the user, for the provision of specified purposes or specific services, when such services cannot be fulfilled with the data at stake (eg where the user is shown the cheapest petrol stations in the area by tracking his real time location). In this regard, Parliament's amendments to the text proposed by the Commission try to further limit the use of consent as an exception, by only allowing the consent of users (ie natural persons)[50] and not of all end-users (ie natural and legal persons)[51] and by adding the obligation to conduct a privacy impact assessment and prior notification to the supervisory authority when this processing shows a high risk for individuals, as stated in Articles 35 and 36 GDPR.[52] In these two later cases (namely, meeting quality of service requirements and providing specified purposes or services), metadata may be erased or made anonymous when it is no longer necessary.

In light of this, if the Parliament's amendments were accepted, a provider would be able to keep anonymised metadata for secondary uses that may not entail risk for users' rights and could help to develop new services in a big data scope. For instance, the Smart Steps project launched by Spanish telecom company Telefónica used aggregated anonymised metadata from their communications services to detect trends and group behaviour. This allowed the company to obtain precise information about how many tourists arrive in a city, where they come from and how they move around, which is of huge value for the tourism sector. This has, indeed, resulted in a new service by Telefónica, which delivers information to interested local businesses, who can then offer special discounts at certain times of the day for cultural, gastronomic or retail services.[53]

In a similar recent episode, the Swedish data protection authority has requested information from Google on the use of 'dark patterns' to obtain users' consent to access location data, being concerned that Google may be using 'deceptive design, misleading information and repeated pushing to manipulate users into allowing contact tracking of their movements'.[54]

As far as the content of communications is concerned, in the current draft ePrivacy Regulation, under the Parliament's amendments in the original Commission draft, this can only be processed with consent, due to its sensitive nature and the fact that no technical reason could justify such an interference with privacy.[55] As was the case with the processing of metadata, consent for the processing of content data is allowed for end-users in the Commission's proposal, but only by users under Parliament's more restrictive proposal.

In this case, however, for which purposes could consent be requested? Consent could be requested in two scenarios. First, user consent could be requested for the provision of specific

services requested by the user himself, provided the service cannot be fulfilled without the processing of such content 'by the provider', as added by the amended text of the Parliament. Under this provision, providers could not seek to obtain consent for the use of more content data than is necessary for the purposes of the services and these must be specific. In addition, the specification that data must be needed 'by the provider' further limits the scope of the Article, in that third parties cannot use the content of communications for their services. This will prevent, for instance, an e-mail provider from transferring your data to a third company who specialise in natural language processing algorithms and who could therefore be interested in accessing the text of your e-mails to enhance their service. This would also mean that Google would not be allowed to seek user consent to grant access to your Gmail e-mails by hundreds of third-party developers and even allow those third parties to share the data with other third parties, as it seemingly currently does, according to a letter that Google itself sent to US lawmakers.[56]

Second, consent to use the content of electronic communications data under the current ePrivacy Regulation draft could also be requested from all users for the provision of specified purposes, provided those purposes cannot be achieved using anonymous information and that the provider has consulted the supervisory authority according to Articles 36(2) and (3) of the GDPR.[57] This would cover those cases where services are not requested by the user himself, but rather may be offered by the provider. This happens when a social network presents users with a functionality under which it scans their pictures across the network to automatically tag them on it or to send alerts when someone uploads a picture where they appear. In this regard, the Parliament amendment establishes an exception under which the consent of all users will not be required, if the processing is done under a service explicitly requested by one of the users, with his consent and when it does not adversely affect the rights and interests of the other users. This would simplify the process of obtaining consent for domestic practices and creates a sort of household exemption.[58] By this means, the proposal shows a clear preference for consent as a lawful basis for the processing, while simultaneously trying to avoid user consent fatigue.

Lastly, regarding how long the data should be kept and when it must be erased, the Commission's proposal first indicated that providers should erase content data or make it anonymous when the transmission has been completed and the recipient has received the data, regardless of whether users could store it using a third-party service. The Parliament amended this provision to establish that content must be erased when it is no longer necessary for the service requested by the user. That is, it opted for a more protective approach by eliminating the possibility of providers keeping anonymised content data.[59] For example, when a user shares a picture through a messaging app, the app will delete the picture from its servers once it has been delivered to the recipient. However, both users can still decide to save it in a cloud provider, who will then be obliged to comply with the GDPR. This would mean, among other things, that the cloud service provider would need a lawful basis to process the data, would be obliged to respect the purpose limitation principle, to provide transparent information, attend users' rights or put in place appropriate security measures.

As a concluding remark on Article 5 of the ePrivacy Regulation as it stands today, without disregarding the specificities commented for each exception granted, they all share the need of being interpreted in a narrow way. For instance, some provisions allow processing of data 'for necessary purposes'. In this regard, necessity must be limited to what is 'technically necessary'[60] or 'strictly necessary'.[61] In addition, other provisions allow for the processing of data when users have given their consent. The situations where this is possible are restricted to a minimum, as requesting consent is limited to situations where the processing is necessary for specific purposes which otherwise cannot be achieved (eg, by not using the data or by using anonymous data).[62] Hence, under this approach, providers would not be allowed to ask customers to waive their privacy rights by consenting to invasive practices. These provisions show the clear vocation of the ePrivacy regime to narrow down the situations which interfere with the confidentiality of communications data. Also, by requiring consent for the processing of electronic communications data, the ePrivacy legislation opts for a more restrictive approach than the GDPR, which would potentially allow for a wider set of legal bases, such as the performance of a contract or legitimate interests,[63] as well as secondary uses of data that fall under a non-incompatible purpose.[64]

C. Confidentiality of Information Stored in Terminal Equipment: On 'Cookies' and 'Tracking Walls'

The ePD aims to protect the confidentiality of information in users' terminal equipment, such as computers or smartphones, by requiring the consent of the user before storing or accessing the information. This information includes cookies,[65] beacons, spyware, pictures and videos, content of e-mails, calendar, etc.

Article 5.3 of the ePD (one of the most polemic provisions in the Directive, often known as the 'cookie provision') allows cookies and other similar tracking technologies as long as the user has given informed consent. This led to so-called 'consent fatigue', derived from the increased use of cookie banners which cause users to face requests for consent that they neither read nor understand, while some cookies are installed without consent. In some aspects this consent rule is over-inclusive;[66] it covers practices that are non-privacy intrusive, such as first-party cookies or analytic cookies.[67] However, in other aspects it is under-inclusive, as it is unclear whether newer tracking technologies are covered by the provision. Nowadays, tracking cannot only be pursued through active means, by 'storing' or 'gaining access' to users' devices and obtaining information through cookies and similar technologies. It can also take place in a passive way,[68] through the use of identifiers 'emitted' by users' devices, such as WiFi tracking or device fingerprinting.[69] This latter form of tracking is not clearly included under the ePD.[70] There is a need to phrase the wording of the provision in a more technology-neutral way to cover future technologies, for instance, those related to the Internet of Things, so that the protection of communications is not dependent on the technique used, but rather on the potential impact on the user's rights. Finally, the chronological gap between the entry into effect of the GDPR and the ePrivacy Regulation has

left several interpretational issues open as DPAs tried to address each in its own manner.[71]

The REFIT evaluation found that the spirit of these provisions remains relevant and the protection against tracking technologies should be kept in the new law. The value of having these rules at EU level derives from the fact that every day more information is stored by users in their equipment and tracking techniques arising from the internet may often come from companies located in other countries. This means that, when the accessed information is personal data, any subsequent processing of that data, for instance, to create user profiles, will be subject to the obligations and rights envisaged by the GDPR. Also, the definition of consent sought in the GDPR is applicable for these provisions.

Taking the above into account, the draft ePrivacy Regulation prepared by the Commission calls for a simplification of the rules on tracking technologies stored in users' terminal equipment. The new rules aim to be more user-friendly and cover all tracking technologies. First and foremost, today the term 'terminal equipment' is a wide concept which includes not only computers or phones but also devices of the Internet of Things (eg a smart watch that captures your vital signs when you exercise, a TV that remembers your favourite series and times to watch them or a smart toilet that stores information on how often you use it or the sugar level in your urine).

In light of this, Article 8.1 of the ePrivacy Regulation states that: '[t]he use of processing and storage capabilities of terminal equipment and the collection of information from end users' terminal equipment, including about its software and hardware, other than by the user concerned shall be prohibited' and provides some exceptions.[72] This provision aims to protect information inside users' devices.[73] As such, it not only covers the installation of unwanted or unnecessary cookies in users' devices, but also the installation of malware, device fingerprinting or technologies that enable, for instance, an app to turn on a microphone or a camera to collect information.[74]

By way of exception, Article 8.1 of the ePrivacy Regulation maintains the consent rule.[75],[76] Other than the user consent, the collection of information from terminal equipment is also allowed when it is necessary for:

(a) carrying on the transmission;[77]
(b) providing an information society service requested by the user (eg a session cookie to add things to shopping cart or to log in your e-mail account);[78] and
(c) web audience measuring in relation to first party analytic cookies.[79]

In relation to this, while the Commission's draft only allowed for the measuring done by the provider himself, the amended text of the Parliament extended the permission to third parties acting on behalf of the provider or web analytics agencies acting in the public interest. Additionally, the Parliament added increasing guarantees for users, which thus requires data to be aggregated, the user being given the possibility to object and explicitly prohibits personal data being made accessible to any third party.[80] Also, the term 'web audience measuring' is not defined in the ePrivacy Regulation, so to make it clear that it could not be interpreted as enabling user profiling, the Parliament modified the wording of the Article to

allow ‘measuring the reach of an information society service requested by the user’.[81]

The Parliament added to the Commission’s original draft of the ePrivacy Regulation a fourth and fifth exception, following the advice of the LIBE report. As such, the collection of information from terminal equipment would be permitted when it is necessary:

(a) to ensure security updates of terminal equipment;[82] and
(b) in the context of employment relationships for the execution of an employee’s task, provided there are no other monitoring purposes.[83]

Here, again, the Parliament amended the initial wording of the Commission to move from mere necessity to ‘strict’ or ‘technically’ required necessity to provide for higher legal certainty and to align with the requirement of recital 49 of the GDPR which allows for some processing operations for security purposes when strictly necessary.[84]

Apart from these suggested amendments, the most important change the ePrivacy Regulation has suffered due to Parliament’s intervention is the inclusion of an explicit ban of the so-called ‘tracking walls’, following the recommendations of WP29[85] and the LIBE report.[86] Tracking walls present users with a ‘take-it-or-leave-it’ choice between privacy and access to a service, that is, when service providers deny users’ access to a service or functionality on the ground that have not provided consent for processing, storing and collecting information that is not necessary for the provision of that service or functionality.[87] The wording originally proposed by the Commission states that ‘no user shall be denied access to any information society service or functionality, regardless of whether the service is remunerated or not, on grounds that he or she has not given consent … to the processing of personal information … that is not necessary for the provision of a service or functionality’. This tracking is usually made through cookies and similar technologies to offer more targeted advertising to users, which is unquestionably more effective than other less personalised types of advertising, thus generating higher income rates.

Figure 10.2 Example of cookie wall. The online content provider Medium obliges users to accept cookies and other non-necessary data collection to read an article on their website



The prohibition of tracking walls has opened an intense debate around the ever-increasing business models based on the provision of services without any monetary exchange and thus

an exchange of valuable data that could achieve more efficient advertising, but which could also be used for other, unexpected, purposes. This debate also included services that offer an alternative to data-paid options, such as monetary payment for subscription in the service.[88]

Further, tracking walls provisions and the possible coerced consent therein also expand to the GDPR. Specifically, Article 6.4 of the GDPR on free consent as well as Article 7, which states that one of the factors to assess the validity of consent will be that the provision of a service is not made conditional to the provision of consent for the processing of personal data that is no necessary for such service.[89] Finally, the prohibition of tracking walls is also in line with recital 5, under which the ePrivacy Regulation should not lower the level of protection granted by the GDPR.

D. Confidentiality of Information Emitted by Users' Terminal Equipment

The ePD does not contain any provisions to protect confidentiality of information 'emitted' by users' terminal equipment. This situation changes under the draft ePrivacy Regulation suggested by the Commission, which protects confidentiality of communications regarding WiFi or Bluetooth signals sent by smartphones and other devices, which enable for location tracking.[90] This protection therefore covers machine-to-machine communications when the information is related to a user (which has an increasing relevance in the times of Internet of Things).[91] For instance, to create a communication via WiFi, devices constantly broadcast their MAC-address to detect access points. The information captured by these signals can be used in different ways, from stablishing the communication between devices to other more intrusive purposes such as the detection of location patterns or counting visitors.[92]

To accomplish that, Article 8.2 of the original Commission's draft establishes that 'the processing of information emitted by terminal equipment to enable it to connect to another device and/or to network equipment shall be prohibited', unless any of the exceptions apply. However, this provision has suffered what may be a significant modification in the Parliament's version. The first version, as phrased by the Commission, set two exceptions where this data could be processed: (i) where it was necessary for the purpose of establishing the connection; and (ii) where a clear and prominent notice is displayed to inform the user, in the same terms as under Article 13 GDPR, that personal data is being collected, together with information on the measures that the user can take to stop or minimise the collection and provided that appropriate security measures are taken in line with Article 32 GDPR.

Giving the sensitive and highly revealing nature of location data, it was noticeable that the provision seemed to suggest that user device location tracking was allowed without consent[93] and without requiring an opt-out right. This would have decreased the level of protection set in the GDPR where, in a similar situation, an opt-out right should be granted if no consent was needed. Thus, this would contradict the aim, expressed in the preamble of ePrivacy Regulation that it should not lower the level of protection enjoyed by natural persons under the GDPR.[94] In this regard, both the EDPS[95] and the WP 29[96] called for improvements in this provision.

Thus, the amended version suggested by the Parliament substitutes the clear and prominent notice to users by the requirement of informed consent. It also builds on the measures to mitigate the risks, such as purpose limitation, to mere statistical counting, limit tracking in time and space and to what is strictly necessary for the purpose, deletion or anonymisation of data after the purpose is fulfilled and object rights for users. This addition is important since it significantly raises the bar for providers to be able to process users' data. Merely requiring a notice would otherwise legitimise the collection of user information captured through, for instance, WiFi signals, which may reveal location and other people's private data in unnoticed ways and would incentivise the already high use of pervasive sensors.

V. The Issue of Consent and its Effect on Software Architecture and Settings

Consent is the central lawful ground under the ePrivacy framework, which allows for several processing activities if users have given consent. However, the REFIT evaluation of the ePD showed that some provisions created an unnecessary burden on businesses and consumers. For example, the consent rule to protect the confidentiality of terminal equipment failed to reach its objective. There is broad acknowledgement that, nowadays, end users face requests to accept cookies and other tracking technologies which are neither read nor understood, leading to situations where users accept terms without realising the consequences. In this way it is possible that tracking takes place without lawful consent. The consent rule under the ePD is both over-inclusive, as it covers non-privacy intrusive practices and under-inclusive, as it does not clearly cover some tracking techniques (eg device fingerprinting) which may not entail access or storage in the device.

The Commission, in its ePrivacy Regulation proposal, aims to tackle these issues.[97] Article 9.1 of the ePrivacy Regulation establishes that the definition of consent shall be that of the GDPR. This follows the line of ePD, which also referred to data protection law for a definition of consent. Under the GDPR, consent is defined as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her' (Article 4.11 GDPR).

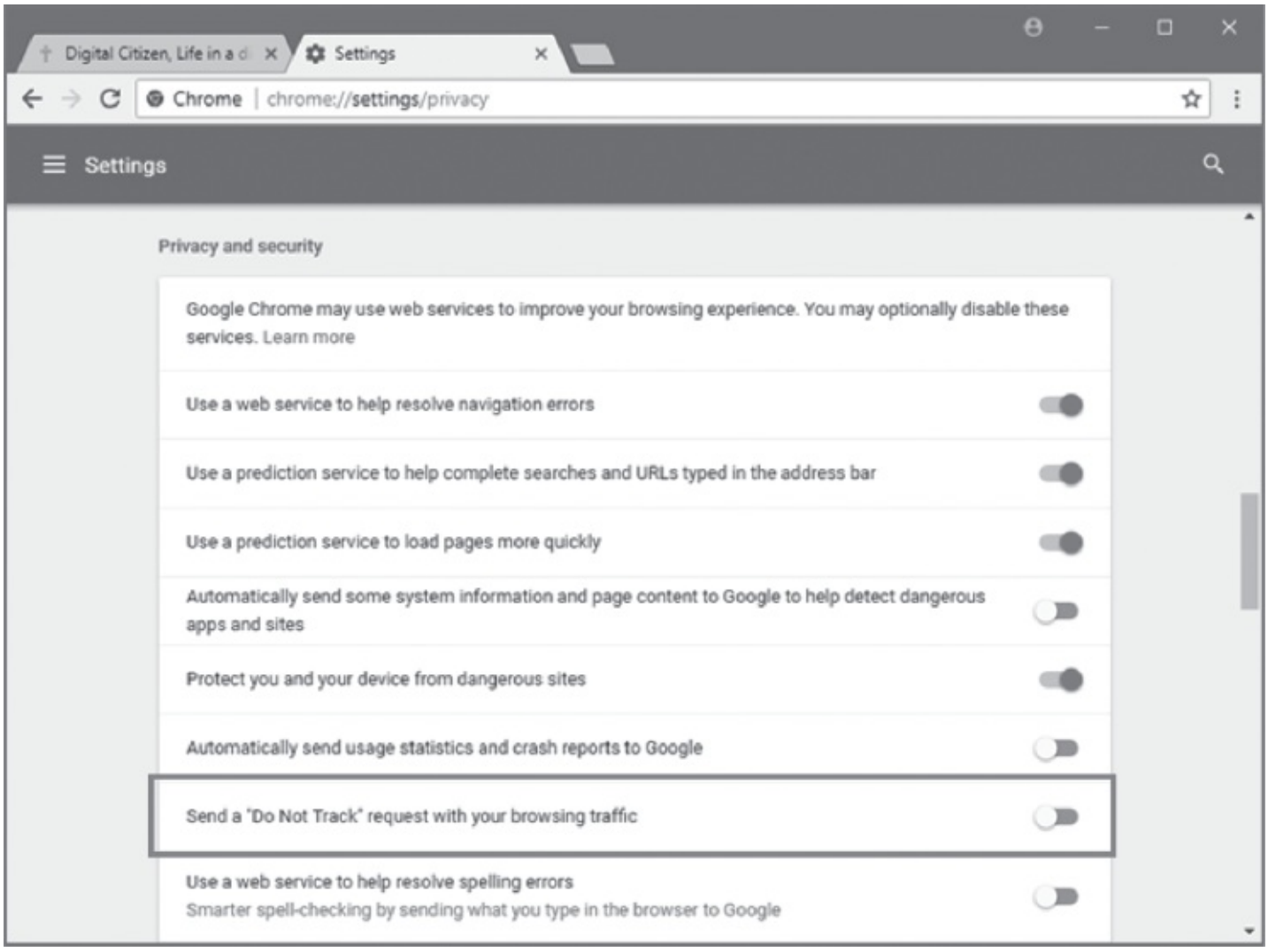
Yet, individuals often face consent requests that are not user friendly and some of them are even designed to be unclear. For that reason, Article 9.2 of the ePrivacy Regulation aims to provide more user-friendly ways to express consent. Specifically, Article 9(2) as drafted by the Commission, states that: 'Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Art. 8(1), consent *may* be expressed by using the appropriate technical *settings of a software application* enabling access to the internet' (emphasis added).

That is, if technically feasible, consent for cookies and other similar tracking technologies covered by Article 8.1(b) can be expressed through technical settings of your internet

browser or any other software application that provides access to the internet. These are the so-called ‘Do Not Track’ (DNT) standards. This is a mechanism that enables people to express their choice on cookies and other tracking technologies by setting their browser accordingly (or by using similar ways that apply to any other technology to centralise consent settings). In practice, DNT standards mean that users are able to tell their browser in one go what their cookies preferences are, rather than giving consent each time they visit a website. This would prevent users from being presented with endless cookie banners (or similar consent requests) every time they carry out a routine action such as opening a website. Instead, once a user has turned on the DNT setting, the browser sends a signal to websites, analytics companies, ad networks, plug-in providers and other web services encountered while browsing and requests that the web application refrain from tracking that person.[98]

However, under the ePD wording, some websites can still lawfully decide to track you, as they are not compelled to respect those settings. Even worse, some websites could choose to act on DNT signals as if they meant ‘do not send ads’ rather than ‘do not collect and process data about me and this device’.[99] The Commission therefore claims that centralising consent in software together with expanding the exception for cookie consent (ie not requiring consent for necessary or innocuous cookies) would significantly reduce the amount of notices users face, avoiding the current consent fatigue and leading to cost saving for many businesses who could work with no cookie banners.[100]

Figure 10.3 How to enable Do Not Track (DNT) in Chrome, Firefox, Edge, Opera and Internet Explorer[101]



The LIBE report, however, highlighted that the Commission's wording had the important drawback of making DNT standards optional and advised making them obligatory. It also recommended that DNT standards should apply to all tracking technologies to cover other contexts such as the Internet of Things. Subsequent to that advice, the proposed text of the Parliament reads:

> Article 9.2: 'Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Art. 8(1), consent may be expressed or withdrawn by using *technical specifications for electronic communications services or information society services* which allow for specific consent for specific purposes and with regard to specific service providers actively selected by the user in each case, pursuant to paragraph 1. When such technical specifications are used by the user's terminal equipment or the software running on it, they may signal the user's choice based on previous active selections by him or her. *These signals shall be binding on, and enforceable against, any other party*.' (emphasis added).

In this way the Parliament reinforces the provisions on DNT standards in several ways. Firstly, making them binding rather than optional. Secondly, by asking that the wording be more neutral from a technological perspective, as it does not refer to software application anymore but rather to the broader expression of 'technical specifications'. Thirdly, granular consent is now provided by allowing 'for specific consent for specific purposes and with regard to specific service providers'. Finally, the settings can be used not only to give consent but also to withdraw it.

Still, it is noticeable that both the Commission and the Parliament direct the DNT standards only to Article 8.1(b), thus granting protection only to information stored in terminal equipment (eg cookies and similar trackers). This would leave activities covered by Article 8.2 of the ePrivacy Regulation, that is, information emitted by terminal equipment (such as WiFi and similar signals) outside the protection of DNT standards. This would be true even after the Parliament rephrased Article 8.2 to require informed consent instead of giving just a clear and prominent notice for cases other than when it is necessary for establishing the connection. Following these changes and in line with the protection granted under Article 9, we argue that this provision should be amended to include Article 8.2 to provide the ePrivacy Regulation with internal coherence.[102]

Finally, Article 9.3 of the ePrivacy Regulation states that end users will be given a right to withdraw consent. The Commission's text restricted the scope of this right to the consent given in the processing of content from electronic communications (Article 6.3(a) and (b) ePrivacy Regulation) and its related metadata (Article 6.2(c) ePrivacy Regulation) and provided for users being reminded of their right of withdrawal every six months.

In this regard, the LIBE report advised that the provision be amended to include the possibility of withdrawing consent to use cookies and similar tracking technologies and that the reminder also applied to browser settings. Lastly, the report also added the necessity for banning cookie walls. This integral protection is seen as a way to better guard consumers against the intrusive nature of online behavioural advertising and the current extended profiling activities.

The Parliament indeed followed this recommendation to expand the scope of Article 9.3 and established that the right to withdraw consent will also cover the processing of information stored in terminal equipment, such as cookies (Article 8.1(b)) and the processing of information emitted by terminal equipment (such as WiFi and Bluetooth) (Article 8.2). The Parliament also suggests that cookie walls be banned, although this provision was inserted in Article 8 (as has been already seen above) rather than in Article 9. As regards the reminders, the Parliament eliminated this obligation for providers. Lastly, it also added that, any processing based on consent must not adversely affect the rights and freedoms of individuals whose personal data are related to or transmitted by the communication, in particular their right to privacy and the protection of personal data.

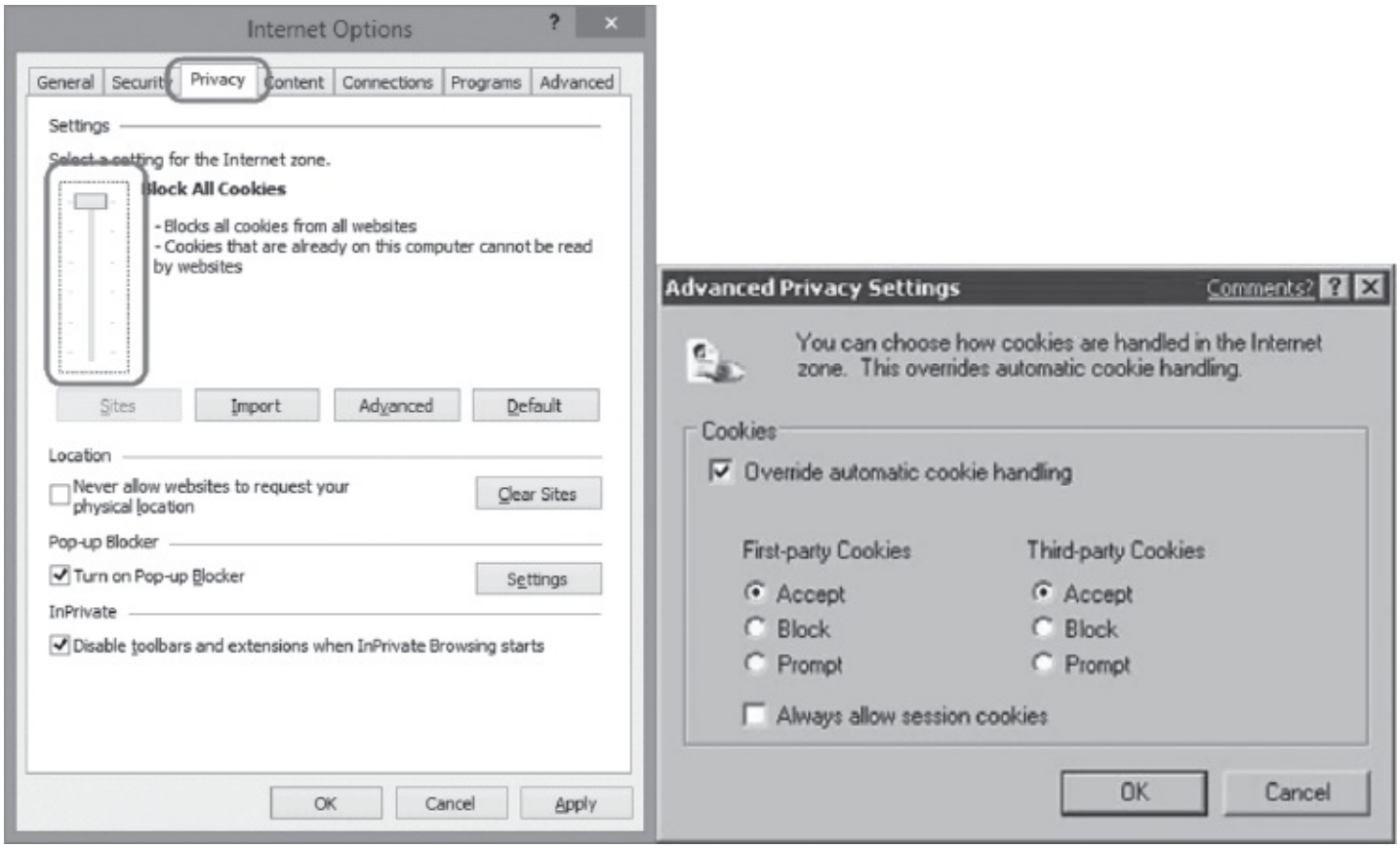
Article 10 of the ePrivacy Regulation then deals with the information and options for privacy settings to be provided. The Commission's proposal established the obligation of providers of software permitting electronic communications to 'offer the option to prevent third parties from storing information on the terminal equipment of an end user or processing information already stored on that equipment'. This provision is directed at providers of software such as internet browsers or app developers. This would entail changes for providers of browsers to develop these options to require a clear affirmative action from the end-user to signify agreement. In addition, software providers should offer the option to prevent third-party cookies, informing the user and requiring making an election about the preferred privacy settings before finalising the installation. By means of this, providers should give users several options to choose from and configure their settings to accept or reject being tracked by third parties. This is done by giving options such as:[103]

☐ Always accept cookies.
☐ Never accept cookies.
☐ Reject third-party cookies.
☐ Only accept first-party cookies.

Consequently, if the Commission's proposal is adopted, more users would become aware of existing tracking techniques and different options to protect themselves from their behaviour being tracked. The problem of this wording as shaped by the Commission is that, nowadays, the default settings for cookies are configured in most current browsers to accept all cookies. This means, only providing options to change the pre-set 'accept all cookies' option infringes the GDPR principles of data protection by design and by default (see Article 25 GDPR), as, if these principles were followed, the pre-selected option should be the most privacy protective one (ie 'reject all cookies').

In view of these shortcomings in the Commission's original wording the Parliament suggested that this provision be amended as follows. First, providers of software permitting electronic communications must pre-configure their systems to have, by default, the most protective options. No options would be given (as no consent would be required) for information that is collected from end-users' terminal equipment when it is strictly necessary for carrying out the transmission or for providing an information society service requested by the end-user (eg to adapt the screen size to the device, or to remember items in a shopping basket). Second, the user would be given granular options to choose from and to consent distinct category of purposes. These options would be presented upon installation of the software but would also be available after it. Third, it is provided that, even if the user has indicated his preferences on the general settings, he should be allowed to make exceptions and give specific consent (eg allowing the storing of cookies from a specific website although your preferences are set in a more protective way for other websites). Finally, information should be easily accessible and allow users to give informed consent.[104]

Figure 10.4 Example of browser cookie settings



In essence, the ePrivacy framework relies on consent to legitimise the use of data that are otherwise not necessary. This follows from the traditional European data protection rules, heavily based on consent as a means for individuals to exercise their autonomy and show self-determination.

Consent, however, has shown shortcomings in online environments. Take as an example the previously mentioned ‘consent fatigue’. Some authors have even argued against keeping consent as a key tool for protecting individuals. In this regard, one would immediately think of Helen Nissebaum and her statement ‘stop thinking about consent: it isn’t possible and it isn’t right’.[105] Lillian Edwards has also shared a similar opinion by stating that ‘real consent may in fact be the ultimate luxury good of the elite: well-educated, time-rich and with access to various options’.[106] Consent places the responsibility on the individual to understand that personal information is being processed by third parties. Similarly, it also provides a means of probe for the controller that the decision made by individuals when providing their consent was informed and free.

However, leaving consent aside as a way to reflect one’s preferences may create a playing field where controllers process data by default, on the assurance that few users would exercise their rights or by providing insufficient information about obscure practices. In the preliminary stages of the drafting process of the ePrivacy Regulation, the EDPS explicitly argued that consent as a basis for processing data provides a higher level of protection than other grounds observed in the GDPR:

> ‘[b]y requiring consent for the processing of traffic and location data, the current ePrivacy Directive offers a higher level of protection than the GDPR. The GDPR, at least potentially, allows other legal grounds, such as legitimate interests or performance of a contract. (…) In order to better protect the confidentiality of electronic communications, the EDPS

recommends that the ePrivacy Directive maintains and strengthens the current consent requirement (…)'.[107]

No matter what, in the end it seems that, at least for the moment, consent may be determined as the basis to enable uses for electronic communications data that are not necessary. The EDPB already showed that other options had not by any means been forgotten, but were just not considered viable, when it stated that '[u]ser consent should be obtained … before processing electronic communications data …. There should be no exceptions to process this data based on the "legitimate interest" of the data controller, or on the general purpose of the performance of a contract'.[108] These tensions between the arguments for and against consent gave rise to principle of data protection by default, enshrined in Article 25 of the GDPR and reflected in Article 10 of the ePrivacy Regulation and which are expected to be solve or, at least, reduce the strain.

VI. Conclusion

In recent years, the European Union has been immersed in the task of modernising key norms to boost the Digital Single Market. 2016 was the kick-off date for the future ePrivacy Regulation, when the first assessments for a modification of the ePrivacy Directive were made. At the beginning of 2017, the European Commission presented a proposal for an ePrivacy Regulation with the aim for it to be in force on 25 May 2018, simultaneously with the GDPR. However, this date has suffered several postponements and, at the time of writing (Summer 2019), after the June 2019 elections and the appointment of a new Commission there is no foreseeable end.

The purpose of this chapter has been to explain the raison d'être and wording of several of the Commission's originally drafted provisions in juxtaposition with the Parliament's views. While the intervention of the Council would have offered a more complete picture, at the time of writing, its official position was not yet available. In this way, we believe that research will be facilitated, once the final ePrivacy Regulation provisions emerge.

Our choice of provisions was based on two factors: First, our perception of what is important, or at least more important than others, in the draft of the ePrivacy Regulation; Second, what has already attracted the attention of parties relevant to the law-making process (DPAs, the EDPS, academics, the industry, NGOs, etc). While the ePrivacy Regulation promises to be an important text of many layers, given its aim and importance to the electronic communications field, certain aspects seem to prevail from others. Having said that, we believe that a critical analysis of all the ePrivacy Regulation provisions under the same light (Commission's draft vs the Parliament's amendments) would have been equally important and useful in the field.

Our examination of the above provisions has demonstrated that the Commission has succeeded in updating the ePrivacy regulatory framework onto current circumstances taking into account accumulated know how and the technological state of the art, such as extended digitisation, the Internet of Things or big data. It remains to be seen whether provisions

drafted in 2017 retain their relevance once the final ePrivacy Regulation is released. The ePrivacy framework is specific and connected to one of the most dynamic fields of technology. As such, it needs constant updating to remain relevant, as evidenced by its frequent updates in comparison to general data protection law. Whether the Commission has achieved its purpose of specificity and granularity remains debatable.

For its part, the Parliament has intervened in a useful and relevant manner, strengthening the protection of individual rights and providing clarification wherever needed. In this way it confirms its role as an important player in the EU law-making process. The evolution of the text from the Commission's version to the Parliament's one has shown an increased tightening of providers' obligations to protect user's rights. Although the final wording is not yet known and significant changes may occur, we consider it important that the ePrivacy Regulation maintains its current vocation for durability and technology-neutral approach, so that advances in the future years will not undermine the protection granted to users.

References

'AP Exclusive: Google Tracks Your Movements, Like It or Not', *New York Times*, 13 August 2018. Available at: www.nytimes.com/aponline/2018/08/13/us/ap-apfn-us-google-location-tracking-abridged.html.

Article 29 Data Protection Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), WP 247, 4 April 2017.

——, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), WP 240, 19 July 2016.

——, Working Document 02/2013 providing guidance on obtaining consent for cookies, WP 208, 2 October 2013.

——, Opinion 4/2012 on cookie consent exemption, WP 194, 7 July 2012.

Beritano, S 'Stop Thinking about Consent: It Isn't Possible and It Isn't Right' Interview with Helen Nissebaum for *Harvard Business Review, 2018.* Available at: https://hbr.org/2018/09/stop-thinking-about-consent-it-isnt-possible-and-it-isnt-right.

Big Brother Watch. Briefing Note: *Why Communications Data (Metadata) Matter*, 2014.

Body of European Regulators for Electronic Communications, *Report on OTT services*, January 2016.

Case C-582/14 *Patrick Breyer v Germany*, ECLI:EU:C:2016:779.

Case C-673/17 *Planet 49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände*.

Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Secretary of State for the Home Department*, ECLI:EU:C:2016:970.

Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others*, ECLI:EU:C:2014:238.

Centre for Information Policy Leadership, *Comments on the Proposal for an ePrivacy Regulation*, 11 September 2017.

——, *EPR vis-à-vis GDPR, A Comparative Analysis of the ePrivacy Regulation and the General Data Protection Regulation*, 2018.

Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, 6 May 2015.

Council of the European Union, Outcome of the 3623rd Council meeting, Transport, Telecommunications and Energy, Luxembourg, 7 and 8 June 2018. Available at: www.consilium.europa.eu/media/35597/st09810-en18.pdf.

Danhoé, R-G, *European ePrivacy Regulation: What non-European Companies Need to Know*, 31 May 2018.

Datainspektionen, Request for Reply and Further Clarification, 18 January 2019. Available at: www.datainspektionen.se/globalassets/dokument/ovrigt/google---request-for-reply-and-further-clarification---skrivelse-till-tillsynsobjekt.pdf.

Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) [2018] OJ L 321/36.

Edwards, L 'Data Protection and ePrivacy: From Spam and Cookies to Big Data, Machine Learning and Profiling' in L Edwards (ed), *Law, Policy and the Internet* (Hart, 2018).

European Commission, Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC SWD(2017) accompanying the document Proposal for a Regulation of the European Parliament and the Council on the protection of privacy and

confidentiality in relation to electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10 January 2017.
European Data Protection Board (EDPB), Statement on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications, 25 May 2018.
European Data Protection Supervisor (EDPS), Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation), of 24 April 2017.
——, Preliminary Opinion 5/2016 on the review of the ePrivacy Directive (2002/58/EC) of 22 July 2016.
European Parliament, Report on the Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 20 October 2017.
European Parliamentary Research Service, Briefing on the EU legislation in process: Reform of the ePrivacy Directive, of September 2017.
'Google admits giving hundreds of firms access to your Gmail inbox' *The Independent*, 21 September 2018. Available at: www.independent.co.uk/life-style/gadgets-and-tech/news/google-gmail-data-sharing-email-inbox-privacy-scandal-a8548941.html.
'Google is being sued over 'privacy-invading' location data collection' *The Inquirer*, 21 August 2018. Available at: www.theinquirer.net/inquirer/news/3061399/google-is-being-sued-over-privacy-invading-location-data-collection.
Papakonstantinou, V and P de Hert, 'The Amended EU Law on ePrivacy and Electronic Communications after its 2011 Implementation; New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights' (2011) XXIX (1) *The John Marshall Journal of Computer & Information Law* 101–147.
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free Government of such data and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1.
Stalla-Bourdillon, S, E Papadaki and T Chown, 'Metadata, Traffic Data, Communications Data, Service Use Information … What is the Difference? Does the Difference Matter? An Interdisciplinary View from the UK' in S Gutwirth and R Leenes, *Data Protection on the Move*, Springer 2015.
Telefónica, Smart Steps Project. Available at: www.wholesale.telefonica.com/es/services/digital/big-data/smart-steps/.
Zuiderveen Borgesius, F, J van Hoboken, R Fahy, K Irion and M Rozendaal, 'An Assessment of the Commission's Proposal on Privacy and Electronic Communications' Study for the LIBE Committee of the European Parliament (LIBE report), 2017.
——, S Kruikemeier, SC Boerman and N Helberger, 'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation' (2017) 3(3) *European Data Protection Law Review* 353–368.
Zwenne, GJ, Q Kroes and J van Eymeren, 'EPR vis-à-vis GDPR: A Comparative Analysis of the ePrivacy Regulation and the General Data Protection Regulation'. Study prepared for Centre for Information Policy Leadership, 19 July 2018.

---

[1] CEU San Pablo University (Madrid) and Instituut voor Informatierecht (IViR), Universiteit van Amsterdam.

[2] Professor at Vrije Universiteit Brussels (LSTS) and University of Tilburg (TILT).

[3] Professor at Vrije Universiteit Brussels (LSTS).

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, pp 1–88 (the GDPR).

[5] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'A Digital Single Market Strategy for Europe', 6 May 2015.

[6] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31.7.2002, amended two times by Directive 2006/24/EC of the European Parliament and the of the Council of 15 March 2006 and Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (the ePrivacy Directive).

[7] European Commission, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC

(Regulation on Privacy and Electronic Communications), 10 January 2017.

[8] See ePrivacy Regulation, recital 5.

[9] Ibid, recital 6.

[10] Ibid, recital 14.

[11] European Data Protection Board (EDPB), Statement 3/2019 on an ePrivacy Regulation, 13 March 2019.

[12] Explanatory Memorandum of the Proposal, p 2. See also the EDPB's relevant views in Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, 17 March 2019.

[13] This was true in the Commission's draft of the ePrivacy Regulation. However, the Parliament's text expanded on the security obligations. Therefore, it remains to be seen what the approach will be in the final text.

[14] Charter of Fundamental Rights of the European Union [2000] OJ L C 364/01.

[15] Explanatory Memorandum of the Proposal, p 5.

[16] Centre for Information Policy Leadership, 'EPR vis-à-vis GDPR, A Comparative Analysis of the ePrivacy Regulation and the General Data Protection Regulation, 2018', p 10.

[17] Explanatory Memorandum of the Proposal, p 4.

[18] European Parliamentary Research Service, 'Briefing on the EU Legislation in Process: Reform of the ePrivacy Directive, of September 2017' p 4.

[19] V Papakonstantinou and P De Hert, 'The Amended EU Law on ePrivacy and Electronic Communications after its 2011 Implementation; New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights' (2011) XXIX(1) *The John Marshall Journal of Computer & Information Law* 101–147.

[20] LIBE report, p 25. Available at: www.europarl.europa.eu/RegData/etudes/STUD/2017/583152/IPOL_STU(2017)583152_EN.pdf.

[21] Although Art 5 on confidentiality of electronic communications data also mentioned stored data.

[22] Article 29 Data Protection Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), WP 247, 4 April 2017, p 26.

[23] However, the Council version for the PeRP makes explicit that protection is only granted to data in transit.

[24] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), amended by Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) [2018] OJ L 321/36.

[25] For a deeper understanding of OTT services see Body of European Regulators for Electronic Communications, Report on OTT services, January 2016.

[26] The inclusion of machine-to-machine services is of special importance in the context of the Internet of Things. Indeed, the communications between machines generate both content and metadata which needs to be protected.

[27] In the Commission's proposal, only recital 12 mentioned that ePrivacy Regulation would be directed at machine-to-machine communications, but this fact was not included in any Article. This concern had been reflected by Article 29 Data Protection Working Party, Opinion 01/2017 (n 22) p 47.

[28] Ibid.

[29] Art 4(2) ePrivacy Regulation.

[30] Art 3 ePD.

[31] Art 3(2) ePrivacy Regulation.

[32] Recital 2 of the Proposal.

[33] Explanatory Memorandum of the Proposal, p 4. See Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others*, ECLI:EU:C:2014:238; Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Secretary of State for the Home Department*, ECLI:EU:C:2016:970.

[34] The REFIT evaluation provides the results of the study conducted by the Regulatory Fitness and Performance

Programme to assess the health and state of current rules and to identify improvement areas. The results of this study were presented by the European Commission together with the Proposal for a new ePrivacy Regulation on 10 January 2017. See European Commission, Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC SWD(2017) accompanying the document Proposal for a Regulation of the European Parliament and the Council on the protection of privacy and confidentiality in relation to electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10 January 2017.

[35] Article 29 Data Protection Working Party, Opinion 01/2017 (n 22).

[36] Being true that the processing of personal data through OTT services is covered by the GDPR, confidentiality of communications needs to be guaranteed by the new ePrivacy Regulation. This is necessary to protect users and granting an even playing field for all providers regardless of the technology used, especially in the age of Internet of Things.

[37] European Data Protection Supervisor, Preliminary EDPS Opinion 5/2016 on the review of the ePrivacy Directive (2002/58/EC) of 22 July 2016, p 13.

[38] REFIT evaluation study (n 34) p 38.

[39] In a similar way, the WP29 also recommended updating the provisions regarding traffic and location data, given the acknowledgement data may reveal very sensitive information and it is not only collected by traditional telecom providers, but also by new market players such as app developers. See Article 29 Data Protection Working Party, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), WP 240, 19 July 2016, p 13.

[40] The EDPS had called for adoption of the concept of metadata in European Data Protection Supervisor (n 37) p 13.

[41] Art 4.3(d) ePrivacy Regulation, as drafted by the Parliament Proposal.

[42] Article 29 Data Protection Working Party, Opinion 03/2016 (n 39) p 14.

[43] Art 4.3(b) ePrivacy Regulation, as drafted by the Parliament Proposal.

[44] S Stalla-Bourdillon, E Papadaki and T Chown, 'Metadata, Traffic Data, Communications Data, Service Use Information … What is the Difference? Does the Difference Matter? An Interdisciplinary View From the UK' in S Gutwirth and R Leenes, *Data Protection on the Move* (Springer 2015). Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2625181.

[45] See also recital 14(a) as drafted by the Parliament Proposal.

[46] Art 6.2(b) ePrivacy Regulation, as drafted by the Parliament Proposal.

[47] The WP29 called for a clarification of Art 6.2(b) ePrivacy Regulation for which certain spam and botnet detection could be interpreted as strictly necessary for the prevention of abusive use of electronic communications services. See Article 29 Working Party, Opinion 01/2017 (n 22) p 13. This recommendation has nonetheless not been included in subsequent versions of the ePrivacy Regulation.

[48] ePrivacy Regulation, Art 7.3 as drafted by the Parliament Proposal. In this regard, whereas the Commission's proposal made reference to 'relevant' metadata, the Parliament's amends only allows to keep and store metadata that is 'strictly necessary' for billing-related legal procedures.

[49] Ibid, Art 6.2(a).

[50] Ibid, Art 4.3(a)(f).

[51] Ibid, Art 4.3(a)(e).

[52] Ibid, new Art 6.2(a) as drafted by the Parliament Proposal.

[53] Telefónica, Smart Steps Project. Available at: www.wholesale.telefonica.com/es/services/digital/big-data/smart-steps/.

[54] Note, however, that, as location data related to an individual may constitute personal data, the Swedish authority is examining Google's activities under the eyes of the GDPR. See full request of information: Datainspektionen, Request for Reply and Further Clarification, 18 January 2019. Available at: www.datainspektionen.se/globalassets/dokument/ovrigt/google-request-for-reply-and-further-clarification-skrivelse-till-tillsynsobjekt.pdf.

[55] Art 6.3 ePrivacy Regulation, as drafted by the Parliament Proposal.

[56] Google admits giving hundreds of firms access to Gmail inboxes, *The Independent*, 21 September 2018. Available at: www.independent.co.uk/life-style/gadgets-and-tech/news/google-gmail-data-sharing-email-inbox-privacy-scandal-

a8548941.html.

[57] In this regard, the Parliament establishes an exception under which consent of all users will not be required if the processing is done under a service explicitly requested by one of the users, and when it does not adversely affect the rights and interests of the other users.

[58] The WP29 had called for a domestic exception in the processing of electronic communications data (both content and metadata) for purely personal purposes, such as the use of text-to-speech services. This would mean that, for the use of electronic communications data for any other purpose, such as behavioural advertising, consent from all users should be requested. See Article 29 Working Party, Opinion 01/2017 (n 22) p 3. The Parliament followed this recommendation only partially, in that consent from all users was *not* introduced as a requirement for the use of metadata, but only content. On the other hand, for the use of content data, household exemption was introduced.

[59] ePrivacy Regulation, Art 7.1 as drafted by the Parliament Proposal.

[60] Ibid, Art 6.1.

[61] Ibid, Art 6.2(a) and (b).

[62] Ibid, Arts 6.2(c) and 6.3.

[63] Art 6.1 GDPR.

[64] The Council proposal for an ePrivacy Regulation allows for 'further compatible processing of electronic communications metadata', in other words, compatible secondary uses of metadata, in line with the GDPR, based on pseudonymous data and provided that profiling of users is not done, and that the data protection authority is consulted.

[65] Recital 30 of the GDPR explicitly recognises the possibility to associate cookie identifiers with personal data by saying: 'Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.'

[66] Article 29 Data Protection Working Party, Opinion 4/2012 on cookie consent exemption, WP 194, 7 July 2012.

[67] *First-party cookies* are the ones served by the website being visited and can only be read by it. For instance, if we visit a bookstore's website, it may place a cookie in our computer that is only readable by that same website. *Third-party cookies* are issued by a different website than the one being visited. Privacy issues may arise here as users may not have reasonable expectations of this processing. This is the case, for example, when Google installs cookies on your computer while you navigate through other websites or when Facebook tracks you through its 'like' buttons.

Further, cookies can be used for several purposes. For instance, *session cookies* expire after you end the web session. These do not normally have privacy issues and can be used, for instance, by e-commerce sites to remember the items you put in your shopping cart or to save the language preferences chosen by a user. *Analytical cookies* can be used to notice when a new visitor access the website, analyse the flows and track the historical activity of a user in the website (eg its response to ad campaigns). *Persistent cookies* are those set with an expiration date and will remain on your computer until that moment, even if you exit the website or close your browser. For example, almost all the Google Analytics cookies are persistent. In another level we find *zombie cookies*, also known as super cookies, which are automatically reinstalled after the user has deleted them. These have strong privacy implications as they circumvent people's choices when they delete those cookies.

[68] Article 29 Data Protection Working Party, Opinion 03/2016 (n 39) p 11.

[69] Device fingerprinting allows a device to be recognised without the need of cookies by other information transmitted by the device, such as the settings (language, screen resolution, timeframe, etc). These are relatively unique and therefore enabled for tracking. It is a way to track users without storing an identifier in their terminal equipment or devices.

[70] Nonetheless, the lack of clarity under the ePD as regards these tracking technologies, have resulted in some companies already being fined. For instance, a case involving unlawful device fingerprinting practices is that of the Spanish telco provider Telefónica. In 2016, the company was fined by the National Data Protection Authority (AEPD) after it was found to have used fingerprinting technology. Telefónica alleged the practice was necessary to provide the users' premium requested services. However, in the end it confessed it had been using browser fingerprinting technology with all kind of users from 2012 until 2015. Telefónica should have informed users about the use of this technology, therefore it had infringed the Spanish e-commerce Act (which transposes ePD into national legislation) and was fined €20,000.

[71] In July 2019, both the UK's ICO and France's CNIL published guidelines on the use of cookies (for a comparative

table see G Voisin and R Boardman, ICO and CNIL Revised Cookie Guidelines, IAPP Resource Center. Available at: https://iapp.org/media/pdf/resource_center/CNIL_ICO_chart.pdf.

[72] Art 8.1 ePrivacy Regulation, as drafted by the Parliament Proposal.

[73] This would leave out the scope of this Article, for instance, the content stored in the cloud.

[74] LIBE report, p 79.

[75] Art 8.1(b) ePrivacy Regulation. For deeper remarks on consent, see below.

[76] Notably, legitimate interest is not one of the exceptions. Although this has been a point of contention for some observers, such as the Centre for Information Policy Leadership, Comments on the Proposal for an ePrivacy Regulation, 11 September 2017. Available at: www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_proposal_for_an_eprivacy_regulation. However, other stakeholders have recommended legitimate interests not to be included among the exceptions, as the LIBE report.

[77] Art 8.1(a) ePrivacy Regulation.

[78] Ibid, Art 8.1(c).

[79] Ibid, Art 8.1(d).

[80] In any case, it seems that this exception only includes first-party analytics cookies, therefore leaving out third-party tracking even if for the purpose of generating anonymised and aggregated statistics. As a consequence, providers would still need to request consent for tracking done by third-party providers such as Google analytics.

[81] Article 29 Working Party, Opinion 01/2017 (n 22) p 18.

[82] Art 8.1(d)(a) ePrivacy Regulation.

[83] Art 8.1(d)(b) ePrivacy Regulation.

[84] Article 29 Working Party, Opinion 01/2017 (n 22) p 20.

[85] Ibid, p 15.

[86] LIBE report, p 92.

[87] For a deeper analysis of tracking walls and the alternatives to a total ban of them see Frederik Zuiderveen Borgesius et al 'Tracking Walls, Take-It-or-Leave-It Choices, the GDPR, and the ePrivacy Regulation' (2017) 3(3) *European Data Protection Law* Review 353–368.

[88] The Council proposal lies in an opposite path to that of the Parliament and specifically allows tracking walls in recital 20 for websites where the content is provided without a monetary payment, provided that the visitor is presented with an alternative to tracking, such as a subscription service.

[89] See Arts 6.4 and 7 GDPR.

[90] LIBE report, p 86.

[91] European Parliament, Explanatory Statement on the Proposal for a new Regulation on Privacy and electronic communications. Available at: www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0324+0+DOC+XML+V0//EN&language=en#title2.

[92] WP29 (WP 240), p 11.

[93] European Parliamentary Research Service, Briefing on the EU legislation in process: Reform of the ePrivacy Directive, of September 2017, p 7. Available at: www.europarl.europa.eu/RegData/etudes/BRIE/2017/608661/EPRS_BRI(2017)608661_EN.pdf.

[94] LIBE report, p 84.

[95] EDPS Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation), of 24 April 2017, p 20.

[96] Article 29 Working Party, Opinion 01/2017 (n 22) 11.

[97] Explanatory Memorandum of the Proposal, p 5.

[98] Future for Privacy Forum. See https://allaboutdnt.com/.

[99] L Edwards, 'Data Protection and ePrivacy: From Spam and Cookies to Big Data, Machine Learning and Profiling' in

L Edwards (ed) *Law, Policy and the Internet* (Hart, 2018) p 19.

100 Explanatory Memorandum of the Proposal, p 6.

101 See www.digitalcitizen.life/enable-do-not-track-dnt-chrome-firefox-edge-opera-internet-explorer.

102 In relation to this, the authors of the LIBE report sent a communication to MEPs highlighting the need of amending Art 9.2 of the ePrivacy Regulation in the sense discussed to grant the same level of protection to information emitted by terminal equipment.

103 See recital 23.

104 The Council text, however, proposes to delete Art. 10 on privacy settings, which would cause significantly smaller number of users to be aware of the existence of more protective privacy settings.

105 S Beritano, 'Stop Thinking About Consent: It Isn't Possible and It Isn't Right'. Interview with Helen Nissebaum for *Harvard Business Review* (2018).

106 Edwards (n 102) p 50.

107 EDPS, Opinion 5/2016 (n 37) p 17.

108 European Data Protection Board (EDPB), Statement on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications, 25 May 2018, p 3.

11

CPDP

Closing Remarks

1 February 2019

GIOVANNI BUTTARELLI

Congratulations to Paul, Rosamunde, Dara and the whole team on another fantastic conference.

It is safe to say that the market for privacy and technology events in Brussels is saturated.

But CPDP continues to defy the laws of physics, reaching this year the maximum capacity of ONE THOUSAND, TWO HUNDRED AND FIFTY registrations.

This is a great achievement – you almost compete with the number of registrations for the 2018 International Conference of Data Protection and Privacy Commissioners![*]

You are entitled to feel very proud.

For those wanting to escape the polar vortex over much of middle America and the Eurasian landmass, there can be no better refuge than CPDP.

The first day of the conference coincided with an unusual milestone – spotted by clever man on Twitter.

The THIRTIETH of January 2019 was precisely TWELVE THOUSAND, SEVENTY HUNDRED AND NINETEEN DAYS after the ‘cold, bright day in April’ at the beginning of George Orwell’s 1984.

And that is the precisely the same amount of time between the publication of the novel in 1949 and the date it was set.

So, the real 1984 is now more distant from us in the past than the dystopian 1984 was for Orwell in the future.

The appalling vision of 1984 may have mobilised many people in this room to fight to safeguard civil liberties in the face of technological change.

But the digital reality in 2019 is very different from the science fiction of the first half of the twentieth century.

We have just had the privilege of listening to Professor Zuboff both open and close this event.

Shoshana is now finally getting universal recognition as a profound, eloquent and erudite prophet of our time – a reputation she has long deserved.

Her overall diagnosis of 2019 is not Orwell's techno-totalitarianism. Although there are some parts of the world which indeed do labour under a similarly oppressive regime.

Instead, Shoshana points to the constant mining of people, their thoughts and relationships in order to predict and shape their future behaviour.

This mined data is analysed and combined to become knowledge.

Knowledge becomes the power to decide what is true and not true.

And this power is now concentrated in a few hands like never before.

As a result, we don't have machines learning to be more intelligent than people as imagined by sci-fi novels and films.

But we do have people who are increasingly expected to think and operate like machines.

This digital future was not inevitable. And continuing on that trajectory is not inevitable either – even if many policymakers and investors assume that it is.

This is the delusion that lies behind, for example, the contention that updated EU rules on the confidentiality of communications – ePrivacy – must be opposed because they stand in the way of Artificial Intelligence.

In fact, this digital future has taken less than two decades to establish itself.

And it can just as easily unravel and be replaced by a model which is more sustainable, more just, more democratic.

CPDP this year, in choosing the theme of democracy, reflects our realisation that our datafied, digitised economy and society does not just affect individuals.

The dominant business model – the mythology around connecting everyone and everything – the fetishisation of big data and AI – this new orthodoxy of how to manage society, is now losing its shine.

People are waking up to the risk that rampant and unaccountable data practices pose to social cohesion and basic values like democracy.

We are realising that privacy is important not just to each of us as individuals. Privacy is a social good.

Respect for private space is necessary for freedom of expression.

Which means that privacy is essential for democracy.

And that is why in 10 days we will host, on the ELEVENTH of February, a conference on the multiple elections taking place this year in Europe and on what DPAs and others need to do

to expose and tackle manipulation in the digital space.

Because, dear friends, 30 years since the fall of the Berlin Wall, our political discourse has moved into Walled Gardens.

These Walled Gardens are not really the ‘public sphere’, but rather unaccountable private spaces, where we are monitored and served information according to the logic of an opaque algorithm.

Democracy, after all, is more than just voting.

It is the freedom to participate in discussions.

It is the freedom to receive information from a plurality of sources.

The right to be informed and to inform.

Everyone is entitled to express her- or himself without their every move, thought and transaction being captured and marshalled to perfect a hidden profile.

If you still go and buy a newspaper in a shop, only the newsagent can observe and infer your political tendencies.

Now, thanks to programmatic advertising, this sensitive information is pumped out to hundreds of obscure agents in the ‘LUMAscape’.

They know what you read and don’t read.

Data protection authorities have been thinking about this for a long time. Back in 2005 the international conference adopted a resolution on political propaganda and personal data processing.

Now DPAs are raising their game.

As various panels this week have made clear: data protection is vital to securing trust in elections.

And data security is essential for elections to deliver a winner – but also to convince the loser of the fairness of the outcome.

In the words of Bruce Schneier, we cannot place democracy at the mercy of the vulnerabilities of computers – which, in the case of elections, are by nature hackable, unreliable or not private – or all three.

The risks of failure in democratic processes are too high. Which is why, for instance, the Dutch government in 2017 decided to return to counting all ballots by hand.

…

Let us, however, try to move beyond the language of risks and dystopian nightmares.

It’s been a terrific week and we should end with a call for positive action.

On this day, 1 February EIGHTEEN SIXTY FIVE, President Abraham Lincoln signed the

Thirteenth Amendment to the United States Constitution.

This amendment declared unconstitutional all slavery and involuntary servitude.

Subsequent case law interpreted the Amendment as prohibiting ‘control by which the personal service of one man is disposed of or coerced for another's benefit’ (*Bailey v Alabama*).

The principle is echoed in Article 5 of the Charter of Fundamental Rights.

And, in recent years, the EU has taken steps to prohibit ‘the recruitment, transportation, transfer, harbouring or receipt of persons … by means of … forms of coercion … of fraud, of deception, of the abuse of power or of a position of vulnerability … for the purpose of exploitation’.

Those words are taken from the 2011 anti-human trafficking directive.

The horrors of slavery are a reminder of the fragility of freedom. In parts of the world, digitisation has been a tool for reducing people to data points serving the interests of powerful players.

The great Frederick Douglass was a man who escaped from his slave-masters and became one of the most brilliant visionaries in US history.

In 1862 he delivered a lecture, called the ‘Age of Pictures’, about the impact of photography on society.

Douglass said, ‘in every human there are vast depths, resting in unbroken silence, never yet fathomed. We feel that … there is something more, that the curtain has not yet been lifted … behind the seen lies the immeasurable unseen’.

Let us not doubt the capacity for people to lift that curtain – to see what really lies behind vague slogans like ‘Innovation’, ‘Artificial Intelligence’, ‘Smart this’ and ‘Smart that’, to look into the black boxes of algorithms, to understand the extent of positive possibilities which technology can offer in a democracy.

Then we can start a more informed dialogue about how to shape technology and its application in ways which benefit the whole of society.

Thank you for your participation this week.

I wish you all a safe – and warm – journey home.

---

* Hosted by the EDPS.

INDEX

A

access to information
see also access to personal data
right of here, here

access to personal data
access control here–here
accuracy of data, verification here, here
African Union *see* African Union Convention on Cybersecurity and Data Protection
authentication here–here
authorisation here, here
Cameroon here–here, here–here
developing countries here
EU data protection law here–here
examination scripts here, here, here, here–here
forbidden, latent risks of here, here
meaning of personal data here, here, here
online here
public registers here
right of here, here, here, here, here, here
teacher-student abuse *see* teacher-student abuse

accessibility of information
GDPR here–here, here, here

accountability
AI systems here–here
algorithms here, here, here
automated here
data controller here, here, here
data protection as tool of here
lifelogging devices here–here
privacy by design here–here
public sector here, here, here, here–here
risk, GDPR concept of here, here, here–here, here–here
teacher-student abuse here
transparency, for here

***AccuWeather/Reveal Mobile* case**
access to personal data forbidden here, here
CAPVerDE modelling here–here, here, here–here
case description here–here
consent here–here
controllership here–here
DPIA application here–here
legal analysis here–here
legitimate interests here
privacy here–here

advertising
children's lack of awareness here–here, here
data processing for advertising purposes here
Online Behavioral Advertising (OBA) here

African Information Society Initiative here

African Union

‘Brussels effect’ here
data protection convention *see* African Union Convention on Cybersecurity and Data Protection
establishment here
European law, influence here, here–here, here
legal status here
privacy here
African Union Convention on Cybersecurity and Data Protection
access to personal data here–here, here, here–here
aims here, here
cybersecurity here
data controllers here, here
Data Protection Authority (DPA) here
definition of personal data here, here
electronic commerce here
enforcement here, here–here
establishment here
examination scripts here–here, here
fundamental rights and public freedoms here
legal status here–here
Oliver Tambo Declaration here
personal data protection here, here, here, here–here
ratification here–here
rectification, right of here
aggregation, data here
Agrawal, Rakesh et al here–here
algorithms
accountability here, here, here
data quality and here–here
ranking and scoring here–here
Allen, Anita here
anonymisation
ePrivacy Regulation draft here, here, here
privacy by design here–here
apps
Apple/iOS as gatekeeper here, here–here
embedded third parties here–here
Artificial Intelligence (AI) models
accountability of system here–here
accuracy here
bias in here–here
data interrogation here–here
data quality here–here
decision-making systems here–here
development pipeline here–here
fairness here
feedback loop here
information, communication here
proposed standardisation here
ranking and scoring here
auditing
lifelogging devices here
authentication here–here
authorisation here, here

B

backdoor attacks here
Batchelor, Rachel et al here
Bauer, Christoph et al here
BayesDB here, here, here
beacons
ePrivacy Regulation draft here
Bertino, Elisa here
Bhatia, Rekha and Singh, Manpreet here–here
bias
AI systems trained on biased data here–here
data interrogation practice here–here
data quality assessment here, here
Dataset Nutrition Label here–here
facial recognition systems here
feedback loop here
gender, in language translations here
mitigation here–here
natural language processing here, here
over-indexing here
proxy identification here–here
biometric authentication here
Bobek AG here–here
Brill, Julie here
Brkan, Maja here, here
***Buivids* case** here
bureaucracy
data protection and here

C
Camera di Commercio v Manni here
Cameroon
see also African Union Convention on Cybersecurity and Data Protection
absence of university code of ethics here–here
access to personal data here–here, here–here
AU Data Protection Convention here
bijurial system here
Decree 93/035 here
disciplinary sanctions on university staff here
European law, influence here, here–here
national criminal law here, here–here
regulation of teacher-student abuse here–here, here–here
teacher-student abuse here, here, here, here–here, here–here
capacity
consent of data subject here
CAPVerDE privacy verifier here, here, here–here, here, here–here
Cavoukian, Ann here
Charter of Fundamental Rights (CFR)
access to personal data here, here, here, here, here, here–here
Article 7 here, here, here, here, here, here, here, here, here, here, here, here, here
Article 8 here, here, here, here, here–here, here, here–here, here, here, here, here
Article 24 here
Article 47 here
Article 52 here, here, here
best interests of child principle here–here
children's rights here–here

compliance, control by independent authority here, here, here, here, here
consent to data processing here, here
data processing here
ePrivacy Regulation draft and here
essence of rights here–here
evolving capacities of child here–here
freedom of expression here
GDPR compatibility here, here
generally here, here, here, here
interpretation and application here
legal status here, here
legitimate basis for data processing here, here
negative conception of data protection here–here, here
personal data protection here–here, here–here, here–here, here–here
positive conception of data protection here–here, here–here
privacy, right to here, here, here, here, here–here
proportionality standards here, here–here
structure here–here
children
data protection information addressed to here
digital environment *see* children, rights in digital environment
internet as paramount space for children's rights here–here, here
right to be heard here, here
children, rights in digital environment
academia's responsibility here, here–here, here
accessibility of information here, here
advertising, data processing for here–here, here
age requirement for data processing consent here, here, here, here–here, here
age verification here–here, here
balancing oversight and privacy here, here–here, here
best interests of the child principle here–here
business, responsibility of here–here
Charter of Fundamental Rights here–here, here
child-friendly information here, here–here, here, here
children's lack of awareness here–here
codes of conduct, preparation here, here–here, here
consultation with children here
data collection by websites here
data portability here, here
data protection by design and by default here, here, here
data protection impact assessment here, here
digital and media literacy here–here, here
disabled children here
discrimination here–here
dual-use services here
economic exploitation, protection from here
education, right to here, here
educational actors' role here, here–here, here
empowering children online here, here, here–here
erasure, right to here–here
EU Strategy for a Better Internet for Children here
European legal system here
evolving capacities of child here–here, here
exercise by child here
GDPR, generally here, here, here, here–here, here

GDPR Article 8 here–here, here–here
generally here
geo-location data here
health data here
impact assessment here–here
informational self-determination, right to here
internet influencers here
language of information here, here–here, here
legal obligations here–here
level of children's internet use here–here
long-lasting impact of activity here
marketing, data processing for here–here, here
meaning of child here, here
mediating internet access here
multidisciplinary approach here, here
offer directly address the child here
optimal development, right to here, here, here, here
parental consent here–here
parental/family role here, here, here, here–here, here
positive impact of digital technology here–here, here–here, here
predictive technology and here, here
preventive or counselling services, child offered here–here, here, here
privacy here, here, here, here–here, here–here, here, here, here
profiling, provisions as to here, here
protection and participation, balancing here, here
regulation, generally here
research institutes' responsibility here, here–here, here
right to be forgotten here–here
rights enshrined for everyone here
risk/safety paradigm here, here, here, here, here–here, here
sexual exploitation, protection from here
social network sites here–here
specific rights of children here
stakeholders, generally here, here, here–here
supervisory authorities, role here, here, here–here, here, here
toys with internet connection here
transparency of information here–here, here, here
unbalanced data and information here
UNCRC here, here–here
Clinch, Sarah et al here
cloud storage
ePrivacy Regulation draft here–here, here
lifelogging devices here, here
zombie cloud data here
compliance
control here, here, here, here, here
data controller here, here–here, here–here, here
facilitating here, here–here
risk, GDPR concept of here, here, here–here
confidentiality
ePrivacy Regulation draft here, here, here, here–here
lifelogging devices here–here
privacy by design here–here
consent of data subject
AccuWeather/Reveal Mobile case here–here

age requirement here, here, here, here–here, here
CFR provisions here, here
consent fatigue here, here
cookies and tracking technologies here–here, here–here
definition here
e-Privacy Regulation draft here–here, here–here, here–here
GDPR here, here
generally here, here, here–here
implicit here
informed consent here, here
lifelogging devices and here–here, here, here
mental capacity here
Online Behavioral Advertising here
pre-ticked boxes here
privacy by design here–here
silence or inactivity here
third parties, non-consensual logging of here, here–here
traceability techniques here–here
unambiguous indication of here
withdrawal here, here
cookies
ePrivacy Regulation draft here, here–here, here–here
Corbet, Rob here, here
Council of Europe (CoE)
Convention 108 here, here, here, here
personal data protection here–here
right to privacy here, here
Crabtree, Andy et al here

D
DaPIS icon set
see also iconography
abstract concepts here
balancing stakeholder priorities here
combination with text here, here
companion icons here, here
comprehension tests here–here
creation here–here, here–here
design methodology here–here
evaluation methodology here–here, here–here
future research here–here
icons used here–here
lessons from existing icon sets here–here, here
nature of icons, generally here–here
number of icons here
ontology-based nature here
research questions motivating here
semiotics and iconography here
simplicity or preciseness of representation here
specificity of icons here–here
usability in multiple contexts here, here
use and function here–here, here
data analysis
learning methods here–here
data cleaning here

data controller
accountability here, here, here
AccuWeather/Reveal Mobile case here–here
African Union Convention on Cybersecurity and Data Protection here, here
compliance and here, here–here, here
DPIA *see* data protection impact assessment
EU data protection law here
GDPR definition here
interpretation of concept here–here, here
joint controllership here, here, here–here
legal bases of processing acts here, here–here
legitimate interests of here
obligation to perform DPIA here, here, here
responsibility here, here–here, here–here, here, here
role and scope of concept under GDPR here, here, here, here–here
university as here
data distribution
limiting here
data interrogation
see also Dataset Nutrition Label
accuracy and fairness here–here
data minimisation
privacy by design here, here–here
data nutrition project here
data pipeline
bias in here–here
feedback loop here
data portability
children's rights here, here
GDPR provisions here, here
data processing
age requirement for consent here, here, here, here–here, here
automatic processing of personal data here
CFR provisions here
children's rights *see* children, rights in digital environment
codes of conduct, preparation here, here–here, here
CoE Convention 108 here
control *see* data controller
data protection and here, here, here
ECHR here–here
ePrivacy Regulation draft *see* ePrivacy Regulation draft
EU data protection law here–here, here, here
GDPR *see* General Data Protection Regulation
geo-location data here, here–here
legitimate basis, must be on here
legitimate purpose here, here
lifelogging devices *see* lifelogging devices
non-electronic here
power and information asymmetries here, here, here, here, here
predictive technology here, here
privacy *see* privacy; privacy by design; privacy terms
public awareness, promotion here–here
purpose, data subject must understand here
purpose limitation here–here
right to information privacy and here

transparency here
data protection
see also personal data; personal data protection, fundamental right to
accountability and here
African Union Convention *see* African Union Convention on Cybersecurity and Data Protection
aim of EU law here
anonymisation here–here
bureaucracy and here
certification schemes here
CFR provisions here–here
child, information addressed to here
children's rights *see* children, rights in digital environment
CoE Convention 108 here, here, here
CoE principles here
DaPIS icon set here–here
data pseudonymisation here, here, here
defence by attack strategy here
definition here
DIPA *see* data protection impact assessment
educating data subjects about here
embedded into design here–here
EU data protection law here–here, here, here, here–here
existing data protection icon sets here–here, here
GDPR provisions here–here, here, here
iconography here–here
informational self-determination here
international instruments here–here
Legal Design here
legal information design *see* legal information design; privacy terms
lifelogging devices *see* lifelogging devices
Lisbon Treaty here–here, here, here
national legislatures here–here
non-readership of privacy terms here–here, here–here, here–here
OECD Guidelines here–here, here
personal data *see* personal data protection, fundamental right to
privacy *see* privacy; privacy by design; privacy terms
privacy distinguished here, here, here, here–here, here–here
private life, right to here, here, here
proceduralism here–here
public awareness, promotion here–here
public registers here, here
secondary legislation here, here, here, here, here, here, here
TFEU provisions here, here, here
tool of transparency, as here–here, here, here, here, here
transborder data flows here–here
transparency of information *see* transparency
Data Protection Authorities (DPAs) here, here, here, here
Data Protection Directive (DPD)
personal data protection here–here, here, here, here, here, here, here, here, here, here, here, here, here, here
repeal here, here
data protection impact assessment (DPIA)
AccuWeather/Reveal Mobile case here–here
CAPVerDE privacy verifier here, here, here–here, here, here–here
CNIL process here, here, here
consent to data processing here–here, here–here

data controllers' obligation to perform here, here, here
description of system architecture here
GDPR Article 35 here–here
general rationale here, here
generally here, here, here, here, here
importance here
joint controllers, where here–here
legal bases of processing acts here–here, here–here
legitimate interests of controller here
logic here–here
pia tool here
potential measures against risk, assessment here, here, here, here–here
probability of risk realisation, calculation here
proving suitability of measures to DPA here, here
quantifying risks detected here
risk assessment, generally here–here
side channels here
structured approach to here, here
technical tools aiding here, here, here–here, here, here–here
ULD process here, here, here
verifying absence of violations here
Data Protection Management Systems (DPMS) here
Data Statements for NLP here
data storage
cloud storage here, here, here, here–here, here
ePrivacy Regulation draft here–here, here
lifelogging devices here–here, here
limitation here–here
terminal equipment, stored in here–here
data subject
consent *see* consent of data subject
meaning here
data validation techniques here–here
dataset
analysis before and during model development here, here
comparison here
exploratory phase here
inconsistencies and exclusions here–here, here
information, communication here
nutrition label *see* Dataset Nutrition Label
selection here–here
standardised datasheets here
supervised learning, in here
Dataset Nutrition Label
anomalous relationships here–here
backends here, here, here
Bayesian analysis here
benefits here–here, here–here
choice of module here
comparison of multiple datasets here, here–here
dataset inconsistencies and exclusions here, here
dataset interrogation here–here
dataset selection here
distribution information here
diversity of modular framework here, here

flexibility here, here, here, here, here, here, here
form and contents generally here, here, here
future directions here–here
generation here
ground truth correlations here, here–here, here, here
histograms here
interactivity here, here, here, here
.json format here
label maker here
label viewer here
limitations here–here
linear correlations here
metadata here, here, here, here, here–here
mitigations here–here
modules here, here, here, here
norms, driving change in here
pair plots here, here, here, here–here
privacy and here
probabilistic model here, here, here–here, here, here
prototype development here, here–here, here, here
prototype results here–here
provenance module here, here, here, here–here, here
as proxy for dataset itself here–here
proxy identification here–here
public-facing version here
purpose here–here, here–here, here–here
qualitative and quantitative modules, mixing here
sensitive or proprietary data here
standard format for metadata communication here, here, here
static modules here
statistics here, here, here, here
subjectivity here, here
tabular data here
technical expertise required here, here, here, here
variables here, here, here, here–here
visual appearance here
web-based application here–here
datasheet
standardisation here
De Hert, Paul et al here, here
De Hert, Paul and Gutwirth, Serge here
decision-making systems
AI systems here–here
dataset selection here–here
Diakopoulos, Nicholas and Friedler, Sorelle here
Digital Object Identifier here
***Digital Rights Ireland* case** here
Directive on Privacy and Electronic Communications here
discrimination
discriminatory surveillance here
UNCRC non-discrimination principle here–here
diversity
assessing here

E

economic exploitation
UNCRC here
***EDate* case** here
edge computing here–here
Electronic Communications Code here
email
ePrivacy Regulation draft here
email provider
ePrivacy Regulation draft here
embedding
legal measures here, here, here, here–here
lifelogging devices here, here, here, here–here
privacy by design here–here
third parties here–here
encrypted content
lifelogging devices here, here, here, here
metadata here
ePrivacy Directive
European Union here, here, here, here
ePrivacy Regulation draft
aim here, here, here
anonymisation here, here, here
Article 2 here–here
Article 3 here–here
Article 5 here–here, here
Article 6 here–here
Article 8 here–here, here, here
Article 9 here
Article 10 here
beacons here
broadcasting services here–here
CFR and here
confidentiality of communications here, here, here, here–here, here–here
consent fatigue here, here
consent issue here–here, here–here, here–here
content of communication here–here, here
cookies here, here–here, here–here
data erasure here
dating apps here
Do Not Track (DNT) standards here–here
electronic communications data here–here
electronic communications service here–here
email providers here
emails here
GDPR and here, here, here–here, here, here
generally here, here
home, protection of here
Internet of Things here, here, here, here, here, here
interpersonal communications services here–here
legal persons here, here
lex specialis, as here, here, here
machine to machine services here–here, here
material scope here–here
metadata here, here–here
natural persons here, here

Over-the-Top providers here, here, here, here
private life, right to here
processing outside EU territory here
provider established outside EU here
publicly accessible private communications networks here–here
REFIT evaluation here, here, here, here, here
secondary uses, anonymised metadata for here
social network sites here, here
spyware here
stored data here–here, here, here–here
structure and contents here
terminal equipment, information emitted by here–here
terminal equipment, information stored in here, here–here
territorial scope here, here, here–here
text messaging here
tracking technologies here, here–here, here–here, here–here
traffic data here–here
unsolicited marketing here
value-added services here
videogames here
voice-over IP here
equality
impact of digital technology here–here, here, here
erasure of data
ePrivacy Regulation draft here
right to, GDPR provisions here–here
ethics
natural language processing here
parental control to internet access here
EU Kids Online here
European Convention on Human Rights (ECHR)
Article 8 here–here, here–here, here, here, here, here–here, here–here, here
data processing here–here
horizontal effect here–here
personal data protection here, here–here, here–here, here
positive obligations doctrine here
privacy, right to here, here, here, here–here, here, here, here
proportionality standards here–here, here–here, here
European Court of Human Rights (ECtHR)
jurisprudence here, here, here, here, here, here
European Network of Information Security Agency (ENISA) here, here
European Union
access to personal data here–here
Agenda for the Rights of the Child here, here–here
'Brussels effect' here
case law here–here
CFR *see* Charter of Fundamental Rights
children's rights here, here–here
CJEU jurisprudence here, here, here, here–here, here
concept of personal data here–here
data controllers here
data processing here–here, here, here
data protection here–here, here, here, here–here, here–here, here–here, here–here
data protection, development here, here, here, here–here, here, here, here–here
Data Protection Directive here–here, here, here, here, here, here, here, here, here, here, here, here, here, here, here

Data Retention Directive here
digital services *see* e-Privacy Regulation draft
Digital Single Market Strategy here, here, here–here
Directive on Privacy and Electronic Communications here, here
educating data subjects here
Electronic Communications Code here
ePrivacy Directive here, here, here, here
ePrivacy Regulation draft *see* ePrivacy Regulation draft
essence of rights here–here
examination scripts, verification and rectification here–here, here, here–here
GDPR *see* General Data Protection Regulation
influence of EU law in AU countries here, here–here, here
information duties here–here, here
information rights, generally here–here
internal market here, here
Lisbon Treaty here–here, here, here
monistic system here–here
Open Data and Public Sector Information Directive here
personal data protection *see* personal data protection, fundamental right to
privacy *see* ePrivacy Regulation draft *see* ePrivacy Regulation draft
processing outside EU territory here
provider established outside here
public registers here
rectification of personal data here–here
rights protection, data protection law here–here
riscification of data protection legislation here
Strategy for a Better Internet for Children here
TFEU here, here, here
UNCRC here–here
examination scripts
access to here, here, here–here, here, here–here
African Union Data Protection Convention here–here, here
control of grading here
EU personal data law here–here, here, here–here
failing students for personal reasons here
fairness, principle of here, here
personal data, as here–here
rectification here, here, here–here, here
sexual abuse for grades here–here
'sorting' here–here
teacher-student abuse, tackling here, here, here–here
verification here, here, here–here, here

F
facial recognition systems
bias here
fairness
assessing here
data processing, CFR provisions here, here
examination marking here, here
lifelogging devices here–here
privacy by design here–here
***Fashion ID* case** here, here–here
fog (edge) computing here–here, here
freedom

privacy as here, here
freedom of expression
CFR here
UNCRC here
freedom of speech
children's rights here
fundamental rights
absolute (exclusive) stance here–here
African Union Convention on Cybersecurity and Data Protection here
competing rights here
digital era, in here
essence of rights here–here, here
interference with here–here
overriding rights here–here
personal data protection *see* personal data protection, fundamental right to
proportionality here–here
relative (integrative) stance here–here
Fuster, Gloria González and Gutwirth, Serge here

G
gender bias in language translations here, here
General Data Protection Regulation (GDPR)
accessibility of information here–here, here, here, here–here
accountability here, here
age requirement for data processing consent here, here, here, here–here, here
age verification here–here, here
aim here, here
Article 1 here–here, here
Article 2 here, here
Article 4 here, here, here
Article 5 here, here, here, here
Article 6 here–here, here, here–here, here
Article 7 here, here, here
Article 8 here–here, here–here
Article 12 here–here, here
Article 12.7 here, here
Article 13 here, here
Article 14 here
Article 15 here
Article 16 here
Article 17 here–here
Article 20 here
Article 22 here
Article 24 here–here, here, here, here
Article 25 here, here–here, here–here
Article 30 here–here
Article 34 here
Article 35 here, here, here–here, here, here, here–here
Article 36 here
Article 40 here, here, here
Article 41 here
Article 57 here, here
CFR compatibility here, here
children's rights here, here, here, here–here, here
codes of conduct, preparation here, here–here, here

compliance, enabling here
consent, withdrawal here
consent of data subject here, here
DaPIS icon set here–here
data controller, role and scope of concept here, here, here, here–here, here
data portability here, here
data processing here, here, here–here
data protection here–here, here, here
data protection by design and by default here, here, here, here
DPAs here, here, here, here
DPIA *see* data protection impact assessment
e-Privacy Regulation and here, here, here–here, here, here
generally here–here, here, here, here, here, here
iconography here–here
intelligibility of information here–here, here–here, here, here
interpreting personal data here
legal information design recommendations here, here
legal obligations, forming and triggering here
lex generalis, as here, here, here
machine-readable legal information here, here–here
mandated disclosure here–here, here–here
material scope here, here–here, here
non-readership of privacy terms here–here, here–here, here–here
offer directly address the child here
personal data, definition here, here, here–here
personal data, role and scope of concept here, here–here, here, here–here
preventive or counselling services, child offered here–here, here, here
privacy here–here
privacy by design here
privacy terms here–here
profiling, provisions as to here, here
proportionality standards here–here
public awareness, promotion here, here–here
public registers here, here, here–here, here
rectification of personal data here–here
right to be forgotten here–here
risk, concept of *see* risk, GDPR concept of
supervisory authorities' tasks here, here–here, here, here
transparency, principle of here–here, here–here, here
triggering legal obligations here
UNCRC compatibility here
user-centric nature here, here
geo-blocking here, here
geo-location data
children here
dark patterns here
ePrivacy Regulation draft here–here, here–here
lifelogging devices here, here–here
Git here
Gjermundrød, Harald et al here
***Google Spain* case** here, here, here, here
ground truth
Dataset Nutrition Label correlations here, here–here, here, here
problematic data here

H
health data
children here
Hijmans, Hielke here
Hintze, Mike here
Hippocratic Database (HDB) here–here
histograms
Dataset Nutrition Label here
***Huber* case** here–here
Hustinx, Peter here

I
iconography
abstract concepts here
attention hierarchy here
balancing stakeholder priorities here
child, information addressed to here
combination with text here, here
companion icons here, here
complexity here, here
comprehension tests here–here
content classification here
creation here–here, here–here
DaPIS *see* DaPIS icon set
data protection here–here
ecological validity here
evaluation here–here
familiarity and here, here
future research here–here
GDPR here–here
icon discriminability here
information overload here, here
legal here–here
nature of icons here–here
PrimeLife project here, here
resemblance icons here
risky or unlawful practices, flagging here–here, here
screen size here, here
semiotics and here
simplicity or preciseness of representation here
standardisation here–here
usability in multiple contexts here
information asymmetries
generally here
public sector here, here, here
informational self-determination
data protection here
right to here
UNCRC here
InMobi settlement here, here
integrity
lifelogging devices here–here
internet
children's rights *see* children, rights in digital environment; Internet of Things
ePrivacy Regulation *see* ePrivacy Regulation draft

geo-location data here
health data here
indefinite persistence of the content here
influencers here
as paramount space for children's rights here–here, here
parental control tools here
positive impact here–here, here
predictive technology here, here
Internet of Things
see also lifelogging devices
ePrivacy Regulation draft here, here, here, here, here, here
information flow here
terminal equipment here

J
Jacquemard, Tim et al here
***Jehovan* case** here

K
k-anonymity here
Kagal, Lalana here–here
Kaggle here
Kokott, Juliane and Sobotta, Christoph here
Kokott AG here

L
l-diversity here
labelling
dataset nutrition label *see* Dataset Nutrition Label
use, generally here–here
language
child-friendly here, here–here, here, here
legal information, transparency here, here–here, here–here
translations, gender bias here
Le Métayer, Daniel here
legal certainty
public registers promoting here, here
Legal Design here
legal information design
abstract concepts here
balancing stakeholder priorities here
companion icons here, here
comprehension tests here–here
concept mining here
content classification here
DaPIS *see* DaPIS icon set
ecological validity here
existing data protection icon sets here–here, here
future research here–here
GDPR iconography here–here
icon complexity here, here
icon discriminability here
icon familiarity here, here
information overload here, here
language issues here, here–here, here–here
Legal Design here, here

machine-readable here, here–here
meaning of machine-readable here
meta-textual information here
nature of icons here–here
non-verbal here, here
ontology-based here, here–here
oversimplification here
PrimeLife project here, here
PrOnto here
risky or unlawful practices, flagging here–here, here
semantic web technologies here–here
semiotics and iconography here
specificity of icons for here–here
standardisation here, here–here
user-centric here, here, here
visualisations here, here
WP29 recommendations here, here
lifelogging devices
see also Internet of Things
access control here–here
accountability issue here–here
accuracy issue here–here
anonymisation here–here
auditing here
cloud storage here, here
confidentiality here–here
consent of data subject here–here, here, here
data cleaning here
data distribution, limiting here
data flow traceability here, here
data minimisation here, here–here
data sharing across platform here
data validation techniques here–here
disabling in shared spaces here
embedded legal measures here, here, here, here–here
encryption techniques here, here, here, here
fabricated data here
fairness here–here
fog (edge) computing here–here, here
geo-location data here, here–here
integrity here–here
machine-readable privacy policies here
memory augmentation here–here
potential for privacy breaches here, here, here, here–here
potential uses of data sets here, here–here
privacy-by-context approach here
privacy by design here–here
processing power here
profiling by here–here
pseudonymisation here, here, here
purpose limitation here–here
Purpose-based Access Control Systems here
QR codes here
risks posed by here–here
screen size here

security and authentication systems here–here
sticky policies here
stop recording functionality here–here
storage facilities, generally here–here
storage limitation here–here
strengthening data protection rights here–here
surveillance risk here, here–here
terminal equipment here
third parties, non-consensual logging of here, here–here
transparency here, here, here, here, here
violation detection and identification here
volume of data involved here–here
Lioudakis, Georgios V et al here
Lisbon Treaty
personal data protection here–here, here, here
location data *see* **geo-location data**
Lynskey, Orla here

M
machine learning
competition platforms here, here
Dataset Nutrition Label here, here
machine to machine services
ePrivacy Regulation draft here–here, here
machine-readable legal information
concept mining here
GDPR here, here–here
lifelogging devices here
meaning here
Makker, Sona R here
Makulilo, Alex B here–here
Marjory Stoneman Douglas High School shooting here
market regulation
public registers here
marketing, unsolicited
ePrivacy Regulation draft here
marketing purposes
data processing for here–here, here
public register data used for here
Mayer-Schönberger, Viktor here
metadata
Dataset Nutrition Label here, here
e-Privacy Regulation draft here, here–here
Metoui, Nadia and Bezzi, Michele here
model development
dataset analysis here
Dataset Nutrition Label here
preprocessing phase here
probabilistic modelling backends here, here
MyData here

N
natural language processing (NLP)
bias here
Data Statements for NLP here

ethics here
gender bias here
natural person, identified or identifiable
personal data protection here–here, here, here, here, here, here
Nikolaou v Commission here
notice-and-scan approach here
notice-and-take-down approach here
Nutrition Facts label here–here, here

O
Oliveira, Stanley RM and Za, Osmar R here
Oliver Tambo Declaration here
onlife experience
verification of personal data here
Open Data and Public Sector Information Directive here
open government
public registers here–here, here–here, here
Open Government Partnership here
Organisation for Economic Co-operation and Development (OECD)
personal data protection here–here, here
***Österreichischer Rundfunk* case** here
Over-the-Top providers
ePrivacy Regulation draft here, here, here, here, here

P
pair plots
Dataset Nutrition Label here, here, here, here–here
Perez, Alfredo J et al here–here
personal data
access to *see* access to personal data; personal data protection, fundamental right to
'any information' here
AU Data Protection Convention definition here, here
concept here–here
EU data protection law here–here
evaluation here
examination scripts as here–here
format here
GDPR definition here, here, here–here
interpreting here
meaning here, here, here, here, here–here, here
medium in which contained here
non-electronic means, processed by here
public registers *see* public registers
rectification *see* rectification of personal data
'relating to' here–here, here
role and scope of concept under GDPR here, here–here, here, here–here
undue restriction on scope of here
verification here, here
personal data protection, fundamental right to
absolute (exclusive) stance here–here
CFR *see* Charter of Fundamental Rights
children *see* children, rights in digital environment
CJEU jurisprudence here, here, here, here, here, here
compliance, control here, here, here, here, here
consent of person concerned here, here

constitutionalisation here–here, here, here, here–here, here
constitutive elements here–here
data processing and here, here, here
Data Protection Directive here–here, here, here, here, here, here, here, here, here, here, here
doctrinal debate surrounding here–here
ECHR here, here–here, here–here, here
ECtHR jurisprudence here, here, here, here, here, here
emergence as EU fundamental right here, here, here, here–here, here, here–here, here
essence of right here, here–here, here, here
examination scripts, rectification here–here, here
fairness principle here, here, here, here
GDPR provisions here–here
generally here–here, here, here–here
identified or identifiable natural person here–here, here, here, here, here
information duties here–here
information sharing and here, here
infringement here, here
interference with here–here
interpretation of EU right to here, here–here
legitimate basis principle here, here, here
mandated disclosure here–here, here–here
norms, development here–here
overriding rights here–here
permissive conception of here
personal data protection and privacy distinguished here, here, here, here–here, here–here
power and information asymmetries here, here, here, here, here
privacy and here, here, here, here, here–here, here–here, here–here
privacy distinguished here, here, here, here–here, here
privacy terms *see* privacy terms
procedural right, as here, here
proportionality here–here
purpose specification principle here, here, here, here, here
rationale here–here, here–here
relative (integrative) stance here–here
right to be forgotten here–here
'right to a rule' here, here–here, here
rights and freedoms safeguarded by here
secondary legislation here, here, here
sui generis development here, here, here, here, here, here
technological development, ties to here, here, here, here–here, here, here, here, here
transparency here–here
personality right
right to informational self-determination here
Peter Nowak v Data Protection Commissioner here, here, here, here, here–here, here, here, here, here
Pew Research Center here, here
Platform for Privacy Preferences (P3P) standard here–here
Porcedda, Maria Grazia here–here
PrimeLife project here, here
privacy
AccuWeather/Reveal Mobile case here–here
African Union here
automatic processing of personal data here
by design *see* privacy by design
CAPVerDE privacy verifier here, here, here–here, here, here–here
Charter of Fundamental Rights here, here, here, here, here, here–here, here–here

children's lack of awareness here–here
children's rights in digital environment here, here, here, here–here, here–here, here, here
'computers and privacy' issue here–here, here, here
Council of Europe here, here
data privacy here–here
data processing here–here
data protection, generally here, here, here–here, here, here–here, here–here, here–here
data protection by design and by default here, here, here, here
Data Protection Directive here, here, here
data protection distinguished here, here, here, here–here, here–here, here
Dataset Nutrition Label here
differential here
Directive on Privacy and electronic communications here
ECHR here, here, here, here–here, here, here, here
educating data subjects about here
embedded into design here–here
ePrivacy Directive here, here, here, here
ePrivacy Regulation draft *see* ePrivacy Regulation draft
as freedom here, here
GDPR here–here, here–here
informational self-determination here, here
international data protection here–here
international recognition of right to here–here
joint controllership, where here–here
lifelogging technologies here–here
machine-readable privacy policies here
national legislatures here–here
Platform for Privacy Preferences (P3P) standard here–here
privacy-by-context approach here
privacy by design here–here
proxies (brokers) here
public registers, proportionality issue here, here, here, here–here, here, here, here
software languages, restriction here
sticky policies here
substantive right, as here, here
terms *see* privacy terms
tool of opacity, as here–here, here, here
training models, investigation of datasets used here–here
uncritical acceptance of surveillance here
privacy by design
accountability here–here
anonymisation here–here
concept, generally here–here
confidentiality here–here
consent of data subject here–here
data cleaning here
data distribution, limiting here
data flow traceability here, here
data minimisation here, here–here
data validation techniques here–here
disabling devices in shared spaces here
encryption techniques here, here, here, here
fairness here–here
fog (edge) computing here–here, here
foundational principles here

GDPR here
guidelines here–here
Hippocratic Databases (HDBs) here–here
integrity here–here
lifelogging devices here–here
multiple parties are involved here
privacy proxies (brokers) here
privacy-preserving data mining (PPDM) here
pseudonymisation here, here, here
public registers here
purpose limitation here–here
Purpose-based Access Control Systems here
storage limitation here–here
transparency here, here–here
Privacy Impact Assessment (PIA)
public registers here
Privacy Nutrition Label here–here
privacy terms
accessibility of information here–here
attention hierarchy here
child, information addressed to here
DaPIS *see* DaPIS icon set
design issues here, here–here, here
display here
educating data subjects about here
existing data protection icon sets here–here, here
GDPR here–here
iconography, transparency achieved through here–here
information overload here, here
intelligibility here–here, here–here, here
language issues here, here–here, here–here
length here–here
machine-readable legal information here–here
mandated disclosure here–here, here–here
non-readership of here–here, here–here, here–here
timing of disclosure here–here
transparency of information here–here
privacy-preserving data mining (PPDM) here
private life, right to
personal data protection and here, here, here
probabilistic computing
BayesDB here
Dataset Nutrition Label here, here, here–here, here, here
proceduralism
data protection here–here
definition here
profiling
GDPR provisions here, here
lifelogging devices here–here
proportionality and rights protection
assessment here, here
CFR here, here–here
ECHR here–here, here–here, here
effective means to achieve purpose here–here, here, here–here, here–here, here
GDPR here, here–here

necessary, data processing must be here–here, here–here, here
personal data protection here–here
privacy interests, balancing here, here, here, here–here, here, here–here, here, here, here
proportionality test here
public registers here, here, here, here–here
ProPublica dataset 'Dollars for Docs' here
pseudonymisation
privacy by design here, here, here
public registers
accessibility here, here, here–here, here, here, here
accountability in public sector here, here, here, here–here
categories here–here
compliance, assessment here, here, here, here
data protection law here, here
definition here
design stage here, here
digitisation here–here
direct marketing and here
DPIA not required here
economic and social transparency here, here–here
effective means to achieve purpose here–here, here, here–here, here–here, here
effectiveness, assessment here, here, here–here, here, here, here
EU law here, here
financial information, registers of here, here–here
GDPR here, here, here–here, here
growing number here, here–here, here
lawful grounds for data processing here, here–here
legal certainty, promotion here, here
legal representation, registers of here, here–here
legislative record, contents here
legitimate purpose here–here, here, here, here–here, here–here, here
market regulation here
necessary, data processing must be here–here, here–here, here
objectives here, here, here–here, here
open government here–here, here–here, here
personal data in here–here
potential for privacy harms here, here–here, here–here
predating data protection legislation here, here, here, here–here
Privacy Impact Assessments (PIAs) here
privacy law here, here, here
professional qualifications, registers of here, here–here
proportionality, balancing interests here, here, here, here–here, here, here–here, here, here, here
transparency here, here, here, here, here, here–here
Purpose-based Access Control Systems here

Q
QR codes
lifelogging devices here

R
Rahman, Mahmudur et al here
Ramirez, Edith here
Ranking Facts here–here
Rao, Umesh Hodeghatta and Nayak, Umesha here
rectification of personal data

African Union Convention on Cybersecurity and Data Protection here
CFR here–here
EU data protection law here–here
examination scripts here, here
GDPR here–here
right of here, here, here, here
REFIT evaluation
ePrivacy Regulation draft here, here, here, here, here
right to be forgotten
GDPR provisions here–here
risk, GDPR concept of
accountability, enabling here, here, here–here, here–here
compliance, facilitating here, here–here
criterion for forming legal obligations here
criterion for triggering legal obligations here
definition of risk here
DIPA *see* data protection impact assessment
generally here–here
interpretation here
joint controllership and here–here
latent risks of forbidden data access here
legal interpretation here–here
likelihood of risk here, here, here, here, here
potential measures against risk, assessment here
rights and freedoms of natural persons here, here, here, here, here–here
role of risk here–here, here–here, here–here
scope here, here–here, here–here
severity of risk here, here, here, here, here

S
Satakunnan Markkinapörssi Oy & Satamedia Oy v Finland here
Schartum, Dag Wiese here
***Schrems* case** here
Schwartz, Ari here, here
screen size
iconography and here, here
lifelogging devices here
self-determination
informational here
privacy and here, here
semantic web technologies
machine-readable legal information here–here
semiotics and iconography here
sexual abuse
teacher-student *see* teacher-student abuse
sexual exploitation
UNCRC here
Shahzad, Muhammad and Singh, Munindar P here
'sharenting' here
social network sites
children using here–here
ePrivacy Regulation draft here, here
indefinite persistence of the content here
influencers here
predictive technology here, here

‘sorting’
examination scripts here–here
spyware
ePrivacy Regulation draft here
SQL injection attacks here
stability
assessing here
Stack Overflow here
statistics
Dataset Nutrition Label here, here, here, here
sticky policies here
storage limitation
privacy by design here–here
subjectivity
Dataset Nutrition Label here, here
surveillance
discriminatory here
lifelogging devices, risks posed by here, here–here
state here
third parties, non-consensual logging of here, here–here
uncritical acceptance of here

T
t-closeness here
tabular data exchange
.csv format here
Dataset Nutrition Label here
teacher-student abuse
accountability here
African Union here, here, here, here–here
Cameroon here, here, here, here–here, here–here
criminal law here, here–here
deterrence here–here
examination scripts *see* examination scripts
failing students for personal reasons here
lecture note handouts, payment for here–here
power imbalance here, here, here, here, here
regulation here–here
reporting here, here, here
sexual abuse for grades here–here
‘sorting’ here–here
student victimisation here
transparency here
teaching environment
see also teacher-student abuse
data analysis here–here
dataset selection here–here
technological developments
personal data protection and here, here, here, here–here, here, here, here
terminal equipment here
text messaging
ePrivacy Regulation draft here
traceability, data here, here
tracking data
dark patterns here

Do Not Track (DNT) standards here
ePrivacy Regulation draft here, here–here, here–here
lifelogging devices, by here, here, here–here
traffic sniffing here
training models
investigation of datasets used here–here
trained on biased data here–here
transborder data flows
international data protection here
transparency
accountability for here
assessing here
children, rights in digital environment here–here, here, here
concept mining here
DaPIS *see* DaPIS icon set
data protection as tool of here–here, here, here, here, here
DPIAs here
educating data subjects and here
GDPR here–here, here–here, here
iconography *see* DaPIS icon set; iconography
language issues here, here–here, here–here
legal information design *see* legal information design
lifelogging devices here, here, here, here, here
machine-readable legal information here, here–here
mandated disclosure here–here, here–here
nature of icons here–here
open government here–here, here–here
Platform for Privacy Preferences (P3P) standard here–here
principle of, in data processing here
privacy by design here, here, here–here
privacy terms here–here
public registers here, here, here, here, here, here–here
semantic here
standardisation of legal information design here, here–here
teacher-student abuse, tackling here
visualisations, achieving through here–here
WP29 recommendations here, here
Treaty on the Functioning of the European Union (TFEU)
Article 16 here, here
Article 114 here
data protection here, here, here

U
UN Convention on the Rights of the Child (UNCRC)
best interests of the child principle here–here
definition of child here
economic exploitation, protection from here
education here, here
evolving capacities of child here–here
freedom of expression, thought and association here
GDPR compatibility here
generally here, here–here
informational self-determination here
non-discrimination principle here–here
optimal development here, here, here, here

privacy here
right to be heard here
sexual exploitation, protection from here
United Nations Economic Commission for Africa (UNECA) here
universities
as data controllers here
examination scripts *see* examination scripts
power imbalance here, here, here, here, here
teacher-student abuse *see* teacher-student abuse

V
voice-over IP
ePrivacy Regulation draft here
***Volker und Markus Schecke and Eifert* case** here, here

W
Wachter, Sandra and Mittelstadt, BD here
***Wirtdchaftsakademie* case** here, here, here, here, here
Wolf, Christopher and Polonetsky, Jules here
World Wide Web Consortium (W3C) here
WP29
legal information design recommendations here, here

Y
Young Canadians in a Wired World here–here

Z
Zoneziwoh, Wondieh M here

HART PUBLISHING

Bloomsbury Publishing Plc

Kemp House, Chawley Park, Cumnor Hill, Oxford, OX2 9PH, UK

1385 Broadway, New York, NY 10018, USA

HART PUBLISHING, the Hart/Stag logo, BLOOMSBURY and the Diana logo are trademarks of Bloomsbury Publishing Plc

First published in Great Britain 2020

Copyright © The editors and contributors severally 2020

The editors and contributors have asserted their right under the Copyright, Designs and Patents Act 1988 to be identified as Authors of this work.

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage or retrieval system, without prior permission in writing from the publishers.

While every care has been taken to ensure the accuracy of this work, no responsibility for loss or damage occasioned to any person acting or refraining from action as a result of any statement in it can be accepted by the authors, editors or publishers.

All UK Government legislation and other public sector information used in the work is Crown Copyright ©. All House of Lords and House of Commons information used in the work is Parliamentary Copyright ©. This information is reused under the terms of the Open Government Licence v3.0 (http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3) except where otherwise stated.

All Eur-lex material used in the work is © European Union, http://eur-lex.europa.eu/, 1998–2020.

A catalogue record for this book is available from the British Library.

Library of Congress Cataloging-in-Publication data

Names: Annual International Conference on Computers, Privacy, and Data Protection (12th : 2019 : Brussels, Belgium) | Hallinan, Dara, editor. | Leenes, Ronald, editor. | Gutwirth, Serge, editor. | Hert, Paul De, editor.

Title: Data protection and privacy : data protection and democracy / [edited by] Dara Hallinan, Ronald Leenes, Serge Gutwirth, Paul De Hert.

Description: Chicago : Hart Publishing, an imprint of Bloomsbury Publishing, 2020. | Series: Computers, privacy and data protection; volume 12 | Includes bibliographical references and index.

Identifiers: LCCN 2019044167 (print) | LCCN 2019044168 (ebook) | ISBN 9781509932740 (hardback) | ISBN 9781509932764 (Epub)

Subjects: LCSH: Data protection—Law and legislation—Congresses. | Privacy, Right of—Congresses.

Classification: LCC K3264.C65 A75 2019 (print) | LCC K3264.C65 (ebook) | DDC 342.08/58—dc23

LC record available at https://lccn.loc.gov/2019044167

LC ebook record available at https://lccn.loc.gov/2019044168

ISBN: HB: 978-1-50993-274-0
ePDF: 978-1-50993-275-7
ePub: 978-1-50993-276-4

Typeset by Compuscript Ltd, Shannon

To find out more about our authors and books visit www.hartpublishing.co.uk.
Here you will find extracts, author information, details of forthcoming events
and the option to sign up for our newsletters.