ACTA ELECTRONICA UNIVERSITATIS LAPPONIENSIS 307

Aleksander Wiatrowski

Abuses of Dominant ICT Companies in the Area of Data Protection

LAPIN YLIOPISTO
UNIVERSITY OF LAPLAND

Acta electronica Universitatis Lapponiensis 307

ALEKSANDER WIATROWSKI

Abuses of Dominant ICT Companies in the Area of Data Protection

Academic dissertation
to be publicly defended with the permission
of the Faculty of Law at the University of Lapland
in Lecture Hall 19 on 21 May 2021 at 12 noon.

LAPIN YLIOPISTO
UNIVERSITY OF LAPLAND

Rovaniemi 2021

University of Lapland
Faculty of Law, Institute for Law and Informatics

Supervised by
Professor Emeritus Ahti Saarenpää, University of Lapland

Reviewed by
Doctor of Laws Jari Råman, Office of the Data Protection Ombudsman
Professor Emeritus Wolfgang Mincke, Attorney-at-Law for NEEF LEGAL

Opponent
Doctor of Laws Jari Råman, Office of the Data Protection Ombudsman

Layout: Taittotalo PrintOne

Cover: Communications and External Relations, University of Lapland

Acta electronica Universitatis Lapponiensis 307

ISBN 978-952-337-259-7
ISSN 1796-6310
Permanent link to the dissertation: http://urn.fi/URN:ISBN:978-952-337-259-7

To my parents.

Acknowledgements

When I started my PhD studies in 2011, coming for the second time to Finland from Poland, I had no idea it will be such a long process. I also would have never imagined that I will have patience and strength for it. But more importantly, I am grateful for those around me who endured me and my prolonged work. Writing a dissertation is not only long but, in a way, lonely process. Yet, I was lucky enough to be surrounded by people helping and supporting me. Even in times, I found myself doubting that I can continue and eventually finish.

First, I would like to thank my original supervisor, professor Rauno Korhonen. I met him as an Erasmus student attending Introduction to Legal Informatics lecture. Never before have I heard about this subject. Yet, as soon as I graduated in Poland, I came with the idea to continue in this area of law. He accepted me from the very beginning and was helping me for years, showing all the patience in the world. Professor Korhonen introduced me to his mentor and one of the most influential personas in Nordic Legal Informatics, to Professor Ahti Saarenpää. I gained another fantastic supervisor. His knowledge and experience had an invaluable impact on my work and myself. Because of him, I could get to know the circle of Finnish and international academics.

Among these academics, I must mention Professor Eric Schweighofer who had always been supporting by asking essential questions and offering many crucial comments. Professor Wolfgang Mincke gave me his philosophical perspective, always reminding me that law is much more than a collection of regulations. Listening to Dr Tuomas Pöysti, both to his lectures and any comments I had a chance to get, has priceless value to my work. I want to thank Dr Reijo Aarnio for every time he shared his inside knowledge about data protection and his work at the office of Data Protection Ombudsman. I cannot miss this chance to thank Professor Manuel Masseno. The Facebook groups he created for shearing legal knowledge provided me with a vast number of sources for this dissertation.

Secondly, I would like to express my gratitude to the Faculty of Law at the University of Lapland. I was given an excellent opportunity to study here and to participate in numerous international conferences. The support from the Faculty also included sending me as a visiting researcher to the University of Bologna in 2012 and the Stockholm University in 2013.

Thirdly, I want to thank all that supported my work financially: Centre for International Mobility, Finnish Cultural Foundation, Olga ja Kaarle Oskari Laitisen

säätiö, Foundation for Economic Education and Rector of University of Lapland Mauri Ylä-Kotola.

Finally, I want to express my deepest gratitude to my parents, Aleksander and Urszula. They supported me in every possible way. Without them, I could not start nor finish this dissertation. Thank you!

Aleksander Wiatrowski
Rovaniemi, 31 March 2021

Table of Contents

When we've got these people who have practically limitless powers within a society, if they get a pass without so much as a slap on the wrist, what example does that set for the next group of officials that come into power? To push the lines a little bit further, a little bit further, a little bit further, and we'll realize that we're no longer citizens - we're subjects. Sometimes the scandal is not what law was broken, but what the law allows.

Edward Snowden

1. INTRODUCTION

Today we live in the Information Society, however, a new concept is about to replace it: the Network Society. In the discussion triggered by the situation that very well might be called "mass surveillance crisis", we are in the need of asking, what society thinks about it and does society want to do anything about it.

Now, more than ever before, we know we are being spied upon and that dominant ICT companies are playing a significant role in it that matter. How can our society trapped in the network react to this? Is the legal framework properly prepared and how can it respond? The General Data Protection Regulation, adopted on 27 April 2016, gave us new solutions, but it took many years before this next generation of data protection rules emerged.[1] One positive element, soon to come[2], is a proposal for ePrivacy Regulation.[3]

Our knowledge about mass surveillance is better than ever and questions about the position of society and the state of our privacy have to be raised once again. Thanks to especially Edward Snowden we know, the scope and complexity of mass

1 Blume B., An Evolving New European Framework for Data Protection, [in:] D. Svantesson, S. Greenstein (eds.), Nordic Yearbook of Law and Informatics 2010-2012. Internationalisation of Law in the Digital Information Society, Copenhagen 2013, p. 25

2 The ePrivacy Regulation will replace the current ePrivacy Directive. Although it has been delayed, it should be adopted sometime in early 2019. However, the delays to ePrivacy have resulted in new problems to consider. The EU Parliament elections in May 2019 are one such problem. Were the elections to result in a significant change in the make-up of Parliament, new MEP's may well demand to re-open the ePrivacy file. The new Parliament would not be bound to follow the decision of the old Parliament. Were this to be the case it would significantly delay the process.

3 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), COM/2017/010 final - 2017/03 (COD), http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2017:0010:FIN

surveillance[4]: governments spying on citizens[5], US and British governments using data collected by dominant ICT companies[6], such as Microsoft, Apple, Google or Facebook.[7]

With a little exaggeration, we can call the 21st century the age of networks.[8] Jan van Dijk states that networks are becoming the nervous system of our society, with having expected influence on our social life, *higher than the construction of roads had in the past*. The Network Society, together with the concept of Information Society, became a way to define modern society as a society of a *high level of information exchange and use of information and communication technologies*.[9]

The Network Society is a modern type of society with an infrastructure of social and media networks that characterizes its mode of organization at every level: individual, group/organizational and societal. Increasingly, these networks link every unit or part of this society (individuals, group and organizations). In western societies, the individual linked by networks is becoming the basic unit of the Network Society. In eastern societies, this might still be the group (family, community, work team) linked by networks. It could be said that the Network Society is built onto the foundations of the Information Society and focuses on networks and their organizational forms.

The Network Society may be a completely new idea, or a higher level of describing and interpreting the changes in modern society, as Ahti Saarenpää explains. In his opinion we should forget about the Information Society – *The age of the information society is over*.[10] The time has come to tell the world that we are now living in the Network Society - *The network society has been a big step forwards from what in fact was a very static information society.*[11] The reason to abandon the Information Society in favour of the Network Society is not the end of information, but the increasing role of networks. Society is now more than ever reliant on infrastructure rather than on information.

---

4 Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services/q-and-a

5 New leaks say NSA can see all your online activities, 31 July 2013, http://net-security.org/secworld.php?id=15328

6 Brunstein J, The Computer's Lines on Prism, June 07 2013, http://www.businessweek.com/articles/2013-06-07/the-companies-lines-on-prism

7 Cate F., Dempsey J., Rubinstein I., Systematic government access to private-sector data, [in:] International Data Privacy Law, volume 2, numer 4, 2012, p. 195-199

8 Van Dijk J., The Network Society, Sage Publications 2012, 3rd Edition, p. 2

9 Ibid., p. 23.

10 Saarenpää A., Legal welfare and legal planning in the network society, [in:] Barzallo J. Luiz, Valdes J. Tellez, Olmedo P. Reyes, Fernandez Y. Amoroso (ed.), XVI Congreso Iberoamericano de Derecho e Informatica, p. 57

11 Network Society as a Paradigm for Legal and Societal Thinking (NETSO), http://www.ulapland.fi/InEnglish/Units/Faculty-of-Law/Institutes/Institute-for-Law-and-Informatics/NETSO-Project

The emergence of explicit data protection laws is in fact relatively recent - all starts in the early 1970s. There are over 120 countries which have enacted data protection laws[12], a number of solutions were presented on the international scene.[13] Today we are witnessing the emergence of the third generation of data protection acts thanks to General Data Protection Regulation. The primary aim of data protection laws is safeguarding of individuals persons right to privacy. Different cultures have a different understanding of that term. Many cultural and even historical elements make enacting sufficient data protection laws almost impossible.

1.1. The meaning of the topic

In my Dissertation, I am focusing, among other issues, on dominant companies. I am not interested in actions of smaller, less significant, in an economic and legal point of view, entities.

Why dominance is so important? Companies selected for analysis, by the fact they are dominant, have a significant and major impact on legal and factual actions in the area of protecting and securing data as well as privacy.

Microsoft, Facebook, Google, etc., are so huge and influential that they are already known for abusing their position in numerous cases. Their economic, global position allows them to easily pay all the fines. So far it seems that tools countries and organizations all over the world have, are not enough to stop dominant companies from their illegal actions.

I would like to explain why dominant companies are in a very comfortable position, and why focusing on them is so important in understanding threats to privacy and data protection and data security, especially with the mass surveillance in the background.

The whole concept of dominance comes directly from the competition law dictionary. I focus on dominant companies because the bigger power on the market has a subject the bigger abuser it can be. Competition law interests me because it is one of the oldest branches of law dealing with powerful, often international subjects. Therefore, provisions are more complete, lawyers more experienced; there are more cases to learn from.

As my area of interest is at first Data Protection I don't use competition law definitions literally. Competition law is known for lacking precise definitions or

12 Banisar D., National Comprehensive Data Protection/Privacy Laws and Bills 2019 (August 1, 2019), https://ssrn.com/abstract=1951416

13 Data privacy law: the top global developments in 2018 and what 2019 may bring, February 25, 2019, https://www.dlapiper.com/en/finland/insights/publications/2019/02/data-privacy-law-2018-2019/

definitions at all.[14] Even common legal understanding of the term "dominance" or "dominant", coming from competition law, may not be sufficient. There are several criteria which I will present, to explain how different companies are, I have chosen for my topic, from those which are usually called "dominant" or even "superdominant". There is a place for the new term - "global dominance" or "absolute dominance".

Also, it is not only about "dealing" with companies or with the problems caused by them. It is not only about creating aggressive legislation to have tools to fight with them. Cooperation is equally important and may be the only way to convince those companies to "behave". Facebook and Google among all the abuses presented some worth mentioning ideas.

The dominance is an underrated factor in dealing with abuses in all legal areas, not only security or data protection. It deserves to proper explanation to underline the issue. I want to explain that in the topic of my dissertation "Abuses of ICT Dominant Companies in the Area of Data Protection", part "Dominant Companies" may be more important than "Abuses". Of course, together, it highlights the whole idea, but when the fact of the existence of abuses is well known, the influence and importance of dominance are less considered.

1.2. Source Material and Method

Source Material

The source material in this dissertation refers to legal acts and policy documents of the European Union and Council of Europe. In narrower scope, it also involves United States – to the extend that allow to detect and describe abuses of dominant ICT companies in the EU. EU secondary legislation – Directives and Regulations are an important part of the research. Other than that the dissertation relies on the jurisprudence of the European Court of Human Rights, the European Court of Justice and in a broader extend on US Supreme Court. Additionally, the work includes official comments, public speeches, agreements between the EU and US, international legislation and in some cases national legislation.

Although legal sources are the most important basis for this work, there is another source in the form of articles and monographs. That includes materials such as textbooks and scholar articles with value for this research – both in material and online form.[15] These materials vary from legal theory to ICT law and to other disciplines, such as competition law.

The work discusses the present situation, the abuses that are taking place right at this time, or in the very near past. With all that is happening, legally and factually

14 Example: Monopoly de jure, monopoly de facto, even dominance.

15 Especially important sources: https://www.academia.edu/ and https://www.researchgate.net

speaking, printed sources or traditional sources are limited, not sufficient. In some cases, it is because of the illegal or classified nature of actions that are described or used as examples for the purpose of this work. In order to deal with this situation, the lack of transparency, secrecy, actions of dominant companies and governmental agencies, the research relies heavily upon media reports, declassified texts and official reports and statements from public officials. All these sources are analysed with caution taking into consideration their non-legal nature. It includes also reliance on materials gathered using computer science and later translation into a legal context.

Method

Ronald Dworkin thinks that there is almost always a right answer to a legal question, while Kaarle Makkonen is of the opposite opinion.[16] Makkonen has pointed out that creation of legal norms is an act of will. When one does not know for sure whether this will has covered the case under consideration, one cannot find the right answer to legal questions the case poses.[17] In my research, I try to find the right answers, possibly legal answers, to problems derived from technology. Some of my questions are strictly legal, some operate around the efficacy of existing legal solutions. What connects them is the pursuit to find the right answers. According to Peczenik the right answer to moral or legal questions is the acceptable answer, but the notion of acceptability is person related.[18]

To elaborate further, Aulis Aarnio thinks that different groups of people may have different standards of acceptability.[19] Where Aarnio has in mind generally judges or lawyers, I am looking for the right answers from the perspective of the European Union audience – scholars and practicing lawyers. Here in the EU, the Western world, the law can be considered naturally to be an institutional power order. The law as an institutional instrument[20] of power ended in the centre of attention.[21] Therefore, to my legal questions, I would prefer to find legal answers. I use the words "would" and "prefer", because in the course of research I found some technological solutions. This is not wrong in itself; however, I find non-legal solutions to be less convincing. On the other hand, technological or non-legal solutions might be necessary in present times.

In my work, I use mostly analytical method. The argument behind choosing a general analytical review of the sources and the literature is justified by the rapid

16 Peczenik A., Is There Always a Right Answer to Legal Question? [in:] U. Kangas, Essays in Legal Theory in Honor of Kaarle Makkonen, Vammala 1983, p. 241

17 Makkonen K., Zur Problematik der juridischen Entscheidung, Turku 1965, p. 215.

18 Peczenik A., Is There Always a Right Answer to Legal Question?, p. 257.

19 Aarnio A., On Legal Reasoning, Turku 1977, p. 94.

20 Aarnio A., Essays on the Doctrinal Study of Law, Springer 2011, p. 48-49

21 Aarnio A., Reason and Authority. A Treatise on the Dynamic Paradigm of Legal Dogmatics, Cambridge 1991, p. 19.

ICT changes and internationalisation posing legal challenges to global legal systems. One of the biggest goals is to forecast the future ICT regulations.[22] New solutions should take into consideration technological changes. Therefore, especially legal solutions should on one hand side be able to recognize rapid changes and on the other become as technologically neutral as possible.

A big part of this work depends on traditional legal sources, a textual analysis of the positive law and the look for theoretical answers. However, "theoretical" may also refer to the ideal construct or utopia distant from reality.[23] Because of that, I argue that there is a need and place, after all, to seek practical answers, such as technological solutions to the problems stressed in this dissertation.

In this dissertation, there is also a place for traditional positivist analysis of the law. It is from the necessity to ascertain if the existing law has the potential to deal with modern issues caused by dominant ICT companies.

From there I use normative analysis. It is the activity of evaluating, and making arguments pertaining to questions of right and wrong. Therefore, it is the soundness of normative premises – whether such premises can be justifiably held or not. Normative statements usually use factual evidence as support, but they are not by themselves factual. Instead, they incorporate the opinions and underlying morals and standards of those people making the statements.[24]

Finally, the topic of this dissertation imposes a specific issue. The analysis of chosen dominant ICT companies is not and cannot be complete. Especially from legal, and in some areas, no-legal, factual points of view. Knowing the abuses that will be described in this work, it is clear that certain amount of actions conducted by these companies are not transparent. In some situations, they are secret, illegal and covered by governmental agencies. What is shown to the world is only one small part of their activities. Not only has that required deep analysis, but special caution. On the one hand side, we have official statements, official privacy policies, on the other facts which eventually led to the knowledge of the vast abuses – abuses in the area of data protection.

1.3. Research questions and the purpose

Can actions of data protection institutions be effective? What about remedies? When Microsoft was "finally defeated" by the European Commission and The Court of First Instance, commentators pointed out that in fact, Microsoft was the one that

22 Wahlgren P, The Quest for Law, Stockholm 1999, p. 25.

23 Aarnio A., Legal Point of View. Six Essays on Legal Philosophy, Helsinki 1978, p. 50.

24 Daniels N., Reflective Equilibrium, The Stanford Encyclopedia of Philosophy (Spring 2011 Edition), Zalta E. N. (ed.), http://plato.stanford.edu/archives/spr2011/entries/reflectiveequilibrium/

won. Microsoft had to pay record fines, but at the same time, it did not change the balance of power on any market. This example gives a question if actions of US and EU data security and data protection institutions can and could be effective.

How any of this can be effective with mass surveillance? When governments are committing the same abuses as dominant companies, executing law becomes even more difficult. One positive aspect is that now as we know that mass surveillance exists in so extreme form, we can try to deal with it.

How dangerous is cooperation between dominant companies? I believe this is one of the most important and at the same time unsaid issue. Not only dominant companies have almost unlimited access to their users' data, but also, they share this information. This is happening, because of the profitability of such actions. Dominant companies, in this case, Facebook but also smaller MySpace, for profit, are willing to violate their own security policy. Several social-networking sites have been sending data to advertising companies that could be used to find consumers' names and other personal details, despite promises they do not share such information without consent. To some extend it is similar when it comes to cooperation between dominant companies and surveillance programs/agencies.

Can these abuses be dangerous? There are more and more people connected to the Internet, IT technology is more than ever useful and widely used as a technology, which is irreplaceable. Other than that, marriages between dominant companies are uniting data from several sources.

What is privacy and do we still own it? How can we fight it back?

The significant problem of cooperation between mass surveillance programs and dominant companies leads to one more question: In what light it puts future General Data Protection Regulation? Law tries to protect our data and privacy. Mass surveillance programs use dominant companies experience in data mining making these tries futile.

The main objective of this work is to answer questions connected to abuses in the area of data protection, both from companies and governments. It requires observing dominant companies and worldwide efforts to prevent these abuses, either by using existing or by creating new legal solutions. There is one recent positive that may be an answer to some European Union problems concerning data protection - General Data Protection Regulation. I find this very promising, but on the other hand, it focuses on the private sector, leaving vulnerability to the privacy abuses from states – mass surveillance. It leads to the question of assessing the role of governments in abuses in the area of data protection. Cooperation between surveillance programs and dominant companies creates a situation where abuses are encouraged. It is no longer a matter of private, commercial sector actions but more of natural behaviour.

1.4. Terminology

This Dissertation is using at least three terms in rather not a standard fashion. Therefore, in the following, they require to be explained in detail. These terms include "Abuse", "Dominance" and "Personal Data". There are two reasons standing behind them.

First of all, the terms "Abuse" and "Dominance" come and are most commonly related to Competition Law. However, in the case of this Dissertation, I barely refer to this branch of law and therefore these terms may cause some confusion, if unexplained.

Secondly, "Personal Data" requires explanation, as I would like to point out that this term is extremely broad and open considering that I focus on challenges, issues and problems of new technologies. As written later, I do not want to reinvent it, only focus on ways of understanding it that may help with the topic.

1.4.1. Abuse

Everything that is contrary to good order established by usage. Departure from reasonable use; immoderate or improper use.[25] This might be a very generic definition, however one that describes shortly and generally the issue behind the topic of the dissertation.

It is not prohibited under Article 102 TFEU to have a dominant position, but the dominant undertaking has a special responsibility toward the competitive process.[26] Even if I am not referring in this thesis to the Competition Law, this is worth mentioning for reason. It means that a dominant company is not allowed to abuse its position by adopting conduct that may be considered abusive. Where in competition rules it relates to the position on the market, in my dissertation it is about all misbehaviours in handling personal data.

Article 102 lists some of practices that are abusive, but this list is nonexhaustive. In general, abusive conduct, in competition law, can be divided into exploitative conduct – imposing unfair prices or trading conditions, and exclusionary conducts – contractual tying or refusal to deal.[27]

These types of abusive conducts do not fit my topic. For the purpose of this dissertation, mainly the definition proposed by the International Organization for

25 West's Encyclopedia of American Law, edition 2. (2008). Retrieved September 21 2018 from https://legal-dictionary.thefreedictionary.com/abuse

26 Case 322/81, "Nederlandsche Banden Industrie Michelin (Michelin I) v Commission" [1983] ECR 3461, para 57.

27 van Loon S., The Power of Google: First Mover Advantage or Abuse of a Dominant Position?, p. 15 [in:] Lopez-Tarruella, A. (ed.) Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models, Springer 2012

Standardization (ISO) will be used. It refers to computer abuse and states[28] that it is *wilful or negligent unauthorized activity that affects or involves the computer security of a data processing system*. The definition of what is abusive, or at least what is illegal, should depend on the objective of the law.[29]

In cases explicitly mentioned definition of abuse taken from competition law may be used.

1.4.2. Dominance

During my short academic experience as a doctoral student, I noticed an interesting phenomenon. Whenever I mention the topic of my dissertation, Abuses of Dominant Companies in the Area of Data Protection, the reaction is always the same – "You are writing about Google, Facebook etc." It is on the one hand helpful, as helps me jump right into the core of the discussion. On the other hand, it means only one thing. Lawyers have one understanding of the term "dominance". It is the competition law "dominance".

Why do I think it is an issue? Mostly because it somehow simplifies the complexity of the problem in the area of data protection and privacy, and at the same time it complicates what should be kept simple.

Naturally, whenever we use the terms "dominance" or "dominant position" we should, and we do think about competition law. That means with the topic "Abuses of Dominant ICT Companies in the Area of Data Protection" the first thing that comes to mind is the connection between Competition Law and Legal Informatics or IT Law.

It is a right guess, and it is at the same time a wrong one. "Dominance" definitions taken from competition law are not even complete or if we want to look for them in legislation, there are none.

What is the "dominance" taken under discussion in almost every publication concerning antitrust law or competition law? Without defining this term, or without quoting relevant provisions it is pointless to discuss. Of course, it may seem that at this point everything has been already said and defined. Yet, there are still plenty of problems and issues. Even though I am not exactly interested in competition law, this way of understanding "dominance" is what I need to include in this paper.

The prohibition on abuse from article 102 TFEU[30] only applies to the conduct of companies with a dominant position – assessment of dominance is an essential

28 The International Organization for Standardization/the International Electrotechnical Commission standard 2382-8: 1998(en), Information technology — Vocabulary, https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en:term:2126318.

29 OECD Policy Roundtables. Abuse of Dominance and Monopolisation, 1996, http://www.oecd.org/competition/abuse/2379408.pdf

30 Treaty on the Functioning of the European Union.

requirement for its application. The first problem is that the article or the whole Treaty on the Functioning of the European Union does not explain what "dominance" is. Single company dominance, the one I am mostly interested in, was defined early by the European Court of Justice (ECJ) in *United Brands*[31] and *Hoffmann-La Roche*[32] cases as "a position of economic strength enjoyed by an undertaking which enables it to prevent effective competition being maintained on the relevant market by affording it the power to behave to an appreciable extent independently of its competitors, customers and ultimately of its consumers."[33] Even this definition, widely accepted and used, raises serious uncertainties: the concepts of economic strength or independence have no economic meaning, it ignores the fact that in most markets, no company is truly independent and there is no indication of which degree of economic strength or independence must be achieved.

Additionally, in competition law, it is required to look for a relevant market. It can be a product market or a geographical market and it is important to assess the time of dominance. In the case of super dominant companies, it is also a part of the discussion, yet in my opinion competition law simplifies the problem.

Competition law is, even if with some understatements, focusing on an economic point of view. Where and when the company is dominant, what is the market share, is the company independent, has the consumer alternative and so on.

The dominance I am interested in is different. Of course, the company must be dominant presently. It must be a global and multinational position. Obviously, the company must have a strong market position in relation to data processing.

From time to time the term "super dominance" or "super dominant position" has appeared in case law. It was popularized in *Microsoft* case and referred to Microsoft's share of more than 90% on the operating systems' market. Before that, it was presented for the first time in the *Tetra Pak*[34] case and confirmed later in the *Compagnie Maritime Belge* case in the opinion of Advocate General Fennelly. He described it as a "position of such overwhelming dominance verging on monopoly" that it would give rise to "particular onerous special obligations".[35]

The term "super dominance" may seem to very accurately and rightly describe the position and situation of the companies I have chosen for my Dissertation and this paper. Unfortunately, in fact it is only a clever way of saying that a company has a massive advantage in the particular market. What is more, this concept has not yet

31 Case 27/76, United Brands Co i United Brands Continental BV [1979], (para. 00207).

32 Case 85/76, Hoffmann-La Roche La Roche & CoAG [1979], (para. 00461).

33 Monti G., EC Competition Law, p. 127.

34 Case C-333/94 P, Tetra Pak, [1996] ECR I-05951 – word superdomiance is not used, but the Commission recognizes exceptional 90% share of the markets of aseptic machines and cartons intended for the packaging of liquid foods in the European Economic Community.

35 Opinion of Advocate General Fennelly in Compagnie Maritime Belge and others v. Commission, [2000] ECR I-1365 (para. 137).

been specifically referred to by the Commission or the European Courts – with one exception of *Microsoft* case.[36]

I like this term very much, but unfortunately, because of its nature it is not useful to me. I am not seeking for a definition focused on market position *per se*.

Yet, I am mentioning it. The first reason is because I want to emphasise how, for competition law, dominance has become a way of describing economic position. The second reason is because I hoped to find a term, to name the situation in the area of data protection and data security. It is not super dominance, but the appearance of such terms in case law shows that sometimes there is a need to create unusual, I would even say flashy names.

I support the idea that when it comes to global dominant companies, or companies considered to be super dominant it is very rare that they abuse the position they own. It could be said that they became victims of their success. Google and Microsoft are the brightest examples. In the case of Google, this is a rather widely accepted opinion[37]. Microsoft is more known for being just an abuser. I prefer to include Microsoft as a victim, as a kind of "elephant in a porcelain shop" – the company already that big and influential that it sometimes acts against competition law rules without having an intention of doing so. The European Commission and The General Court would not agree with me[38], but this is my opinion which was a base already for my Master Thesis "The Prohibition of Abuse of a Dominant Position in the Light of the *Microsoft* Case".

On the other hand, what needs to be underlined, when it comes to abuses in the area of data protection and privacy, is that it does not matter why the company is dominant or whether it is a victim or an abuser. The situation is different. Abusing the dominant position, in competition law understanding, is about the market power and has an economic basis. The difference between US Antitrust Law and EU Competition Law shows us that it is not obvious what the reaction should be. Should we try to eliminate monopolies, but at the same time allow smaller companies to defend themselves and focus on protecting consumers (US Antitrust Law)[39], or should we protect consumers indirectly by protecting smaller companies (EU Competition Law)[40]? I don't think it is far from the truth to say that with widely

36 Van Bael, Bellis (eds.), Competition Law Of The European Community, The Hague 2005, page 119, E. Szyszczak, Controlling Dominance in European Markets, [in:] Fordham International Law Journal, Volume33, Issue 6, 2011, page 1757.

37 van Loon S., Chapter 2. The Power of Google: First Mover Advantage or Abuse of a Dominant Position, [in:] Lopez-Tarruella A. (ed.), Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models, The Hague 2012, p. 10.

38 COMMISSION DECISION of 24 May 2004 relating to a proceeding pursuant to Article 82 of the EC Treaty and Article 54 of the EEA Agreement against Microsoft Corporation (Case COMP/C-3/37.792 — Microsoft), 2007/53/EC

39 Majcher J., Dostęp do urządzeń kluczowych w świetle orzecznictwa antymonopolowego, Warszawa 2005, p. 34.

40 Jones A., Sufrin B., EC Competition Law Third Edition, New York 2019, p. 571.

understood data protection it is easier. It is about privacy and data that needs to be protected and it does not matter if the company is abusing its position on purpose, accidentally or as a victim of its extremely strong market position.

The problem of an insufficient definition of dominance, for the purpose of my Dissertation, can be partially solved by naming requirements for companies' dominance in the area of data protection and privacy. These requirements must be based on competition law as I do not want to isolate my work and ideas from the existing legal solutions and concepts.

In my Dissertation, I would like to use companies' dominant position in very specific ways. The exact market share is not what I am interested in. Facebook is an example of a very influential and powerful entity that does not have exact market shares, yet I do not think there are any doubts whatsoever that it has dominant position. Especially considering that there are ways to establish a monopoly of Facebook on the Social Media market.[41]

Having that in mind I would like to propose the following requirements for deciding whether the company holds a dominant position or not, without starting an investigation under competition law:

- the company must have a global and multinational presence,
- strong overall market position,
- strong economic position,
- possible legal influence;

Of course, the companies to meet my requirements and be useful in course of my work, must deal on the daily basis with a large amount of data, possibly collected about their profile.

As can be easily recognized these requirements have origins in competition law. This way it simplifies their application and understanding.

What does it mean that the company must be global and multinational? The role of this requirement is to exclude all the entities, which are dominant on the market of just one country or even just one continent. Therefore, there is no place for Yandex[42], which is the biggest search engine on the Russian market, or Baidu[43], having the same position on the Chinese market.

Global and multinational, these give me only companies having their presence and interests all over the world, reaching everyone, whether willingly or not. Some companies may have headquarters in one, specific place, but in fact act like several smaller and often independent entities. For example, Facebook is after all everywhere, but this is an American company established under US law having headquarter in

41 http://thenextweb.com/socialmedia/2012/06/10/facebook-is-eating-the-world-except-for-china-and-russia-world-map-of-social-networks/

42 http://www.yandex.com/

43 http://www.baidu.com/

the United States. At the same time having the European headquarter in Ireland, in European Union.[44]

The custom in competition law decides when the company holds a dominant position and on what market etc. As I have written already, Facebook, for example, has a very specific situation in which assessing by numbers its position is rather difficult. Microsoft is, according to the competition law, definitely not a dominant company in the search engine market. Google on the other hand holds a strong position in all markets they are involved.

"Strong Overall Market Position" requires something different. For a company to be considered as dominant for my purposes, in the area of data protection and privacy, it must hold a position that allows it to collect and process large amounts of data. Microsoft may not be the owner of the most popular search engine (Bing) but together with all the Windows operating systems (including PC and mobile solutions), Skype, Internet Explorer, Xbox Live and Windows Live, it has access to one of the biggest databases in the world. Almost the same applies to Google. Facebook gained access to one of the biggest databases in a different way, but the result is the same.

Microsoft, Google, Facebook - similar and different at the same time, found their ways to collect an incredibly large amount of data. How many more companies in the world can say that they have access to information about people from every corner of the world?

A strong economic position in this case, means that the selected companies can pay any given financial fines put on them without actually feeling this.

Microsoft is a great example. Losing the *Microsoft* case cost the company together around 1.2 billion euro.[45] It was the highest fine ever paid in the history of the European Union at this time.[46]

But was it a big loss for Microsoft? Microsoft is the first company to be subject to such a high penalty. This is a record, but keep in mind that, for example, Microsoft's revenue in 2005 was 39.78 billion and net profit 12.25 billion. The fine of 1.2 billion is the sum of all fines that Microsoft had to pay during the 10 years of the process against the European Commission. It is not hard to imagine that in this perspective 1.2 billion euro no longer looks that big.[47]

---

44 Facebook's new headquarters is located at 1 Hacker Way, http://www.zdnet.com/article/facebooks-new-headquarters-is-located-at-1-hacker-way/

45 Microsoft underwent a series of investigations and settlements, racking up a total of more $3 billion in European fines over the course of a decade, including a penalty in 2013 for failing to adhere to an earlier settlement.

46 Today's record belongs to Google: €4.34 billion - http://europa.eu/rapid/press-release_IP-18-4581_en.htm

47 Poeter D., EU Slams Microsoft With Record $1.35 Billion Fine, http://www.crn.com/news/applications-os/206900563/eu-slams-microsoft-with-record-1-35-billion-fine.htm, Słojewska A., Bruksela nie kończy walki z Microsoftem, "Rzeczpospolita", 13.07.2006.

A strong economic position means that a company does not have to fear any possible fine that can be given under existing laws. That the fine may just become the cost of running the company. Of course, I assume that there is a number, a fine high enough to scare even one of these companies. The European Parliament, for instance, has called for a breakup of Google.[48] A breakup will almost certainly not happen, but for Google, its inability to reach a settlement with the European Commission despite years of trying means the company could still potentially face a fine of nearly $6 billion, or 10 percent of global annual sales, and restrictions on its freedom to do business in Europe if it is eventually found to have broken EU competition laws.[49]

During the KnowRight 2012 conference in Helsinki, the Finnish Data Ombudsman Rejio Aarnio spoke about 25 years of Data Protection in Finland and asked the question, "Are we ready?" He listed a number of solutions which are planned to be implemented into European Union law. Most of these solutions already exist in Finnish law. Regardless of that, even Finland is having troubles dealing with Facebook.[50]

Actions of companies I am interested in, may result in law becoming outdated or at least insufficient long before it is even enactment. It may be the biggest issue with new data protection regulation or with data protection laws in countries which are only now working on legislation in this area (e.g. China, Russia and India).

There is also a possible way of influencing the law. Every time Google or Facebook works on a revised version of, for example, their Privacy Policies they may present innovative ideas and solutions.[51]

Competition law does not define the term "dominance" in legislation. Dominance, in a rather unclear fashion, was explained in EU case law, leaving a lot to discuss. Being not really defined, dominance on the other hand is in competition law quite specific and leaves usually no doubt which company is dominant and on what market. Yet, it causes some uncertainties in some cases. Specifically, when I want to talk about dominant companies in the area of data protection and privacy. Saying only that selected companies hold given numbers on some markets, or that they are not dominant only in very few places in the world is not enough.

When it comes to processing data and dealing with privacy issues, there are several companies which are different compared to others. They are everywhere, but at the

48 The Misbegotten 'Right to Be Forgotten', http://www.usnews.com/debate-club/should-there-be-a-right-to-be-forgotten-on-the-internet/the-misbegotten-right-to-be-forgotten

49 E.U. Parliament Passes Measure to Break Up Google in Symbolic Vote, http://www.nytimes.com/2014/11/28/business/international/google-european-union.html?_r=0

50 Maurieni C., Facebook is Deception (Volume One), 2012, http://books.google.fi/books?id=s6TxlJ1v5y4C&printsec=frontcover&dq=Facebook+is+Deception+(Volume+One)&hl=pl&sa=X&ei=7GMKUZDyGInitQaez4DYAQ&ved=0CCwQ6AEwAA

51 Rodrigues R., Privacy on Social Networks: Norms, Markets, and Natural Monopoly, [in:] Levmore S., Nussbaum M. C. (eds.), The Offensive Internet, Cambridge, Massachusetts, London 2010, p. 241-250.

same time nowhere. They hold a strong position on many markets, together having the possibility to create enormous data bases. They conduct or are able to conduct abuses in connection with the data they process. Existing law is insufficient to stop them. Finally, unlike in competition law, there is as of yet no way of cooperating with the abuser.

It is all fine, but why in fact do I believe we need a different dominance? Marking a company as a monopolist, dominant or super dominant means that the company has special responsibilities. Mainly because the special position may cause more harm. It is more or less the victim of the size or position. Using competition law requirements to asses if a company is in a dominant position is not enough. Microsoft does not have a monopoly on any market that alone could cause danger to privacy or data protection. Facebook is not even a monopolist, at least officially, although it is treated as such by europe-v-facebook.org.[52] Finally, Google is an exception, but this exception shows how strong, on the single product market the company has to be, to be seen and recognized as a threat.

Seeing a company as a subject on multiple markets, not always connected with each other, by any means, may help in recognizing the problem earlier. If in competition law a recognized monopolist is treated as a potential abuser, in the area of data protection and privacy we should look for companies being able to collect data without any limitation thanks to the position they hold on several markets. Competition law is focused on the economy, my point of view is focused on privacy and data protection. In both cases, we cannot stop the companies from being dominant, but we can start asking questions about the necessity of their actions. And if we recognize them early enough as potential abusers, we may have more chances to avoid a situation similar to the one with Facebook, Google and Microsoft.

1.4.3. Personal Data

The understanding of personal data term in this work comes directly from the definitions used by the EU and Council of Europe. The Council of Europe Convention 108[53] and OECD Guidelines[54] refer to personal data as *any information relating to an identified or identifiable individual.* The General Data Protection Regulation states[55] that *'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.*

52 Open Social Networks, http://www.europe-v-facebook.org/EN/Objectives/objectives.html

53 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, CETS No. 108.

54 Article 1 (b) OECD Guidelines.

55 Article 4 (1) General Data Protection Regulation.

For the purpose of this work following proposition for personal data is made. It is any kind of information (a single piece of information or a set of information) that can personally identify an individual or single them out as an individual. Common examples are somebody's name, address, national identification number, date of birth or photograph. Other examples, less obvious, include vehicle registration plate number, credit card details, fingerprints, IP address or a health record. What is important to remember is that personal data is not just information that can be used to identify an individual directly. It is enough to single out a person from among other people using a combination of pieces of information or other identifiers. As an example, can be given online advertising companies practices. They don't know the name of the person, but they use tracking techniques and assign a unique identifier in order to monitor that person's online behaviour. It is building a profile that allows showing offers that could be relevant to this person. This way of identifying that leads to building a profile which is considered to be personal data.[56] Later in the dissertation, some extreme examples of personal data will be presented.

Data is an incredibly valuable resource for both the public and private sectors and is becoming increasingly so thanks to big-data technologies' ability to process large amounts of data quickly and cheaply.[57] The benefits to society of collecting and processing large amounts of personal information are numerous, including advances in public health, education, safety and welfare. But the generation of such vast amounts of personal information poses real risks, such as the revelation of information about individuals that they wish to keep private because it is harmful or embarrassing; the facilitation of discrimination and profiling not in the interest of the individual; identity theft; and extortion.[58]

1.4.4. Data/information

A philosophical difference must be drawn between data, which refers to the symbols processed in data processing, and information, which is contextually interpreted data, i.e. symbols to which certain meanings are attached. Data is raw, unorganized facts that need to be processed. Data can be something simple and seemingly random and useless until it is organized. When data is processed, organized, structured or presented in a given context so as to make it useful, it is called information.[59]

---

56 And introduction to Data Protection, The EDRi papers, issue 06, https://edri.org/wp-content/uploads/2013/10/paper06_web_20130128.pdf, page 4

57 According to "TechRadar: Big Data," a Forrester Research report released in Q1 2016, some of the latest big-data technology includes predictive analytics software and hardware. www.forrester.com/report/TechRadar+Big+Data+Q1+2016/-/E-RES121460

58 De Mooy M., Rethinking Privacy Self-Management and Data Sovereignty in the Age of Big Data. Considerations for Future Policy Regimes in the United States and the European Union, 2017, https://cdt.org/files/2017/04/Rethinking-Privacy_2017_final.pdf, p. 24.

59 https://www.diffen.com/difference/Data_vs_Information.

According to ISO information is *knowledge concerning objects, such as facts, events, things, processes, or ideas, including concepts, that within a certain context has a particular meaning* and data *is a reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing*.[60]

In this dissertation, with the exception of explicitly mentioned instances, the terms *data* and *information* are used interchangeably. In most cases, there is no need to make a distinction.

1.4.5. Privacy

Writing about privacy is always a challenge. At this point of the discussion, probably everything was already taken under consideration and said. The contributions can be found in philosophy, political science, political and legal theory, media and information studies, as well as in computer science and engineering.[61] Yet, there is no correct answer to the question, what is privacy. Ahti Saarenpää in his article *Openness, Access, Interoperability and Surveillance: Transparency in the New Digital Network Society* states that there is no point in having a precise legal definition of privacy.[62] The reason may be that defining privacy depends on a large number of factors: social, legal, technical and historical, finally, each culture has its own view of what privacy is.[63] Over time, we collected ideas and experiences from the past and present, and now we can tell long stories about how privacy could be understood. Indeed, I believe that there is no right answer to the question: *What is privacy?* For the purpose of my dissertation, I choose to aim in answering a different question: *How could privacy be understood?* Understood in general, by me and by Internet users, with special recognition of social media users.

It is worth starting with the fact that privacy is a Fundamental Human Right.[64] It is recognized as such by the 1967 International Covenant on Human Rights and by Article 12 of the 1948 Universal Declaration of Human Rights:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

60 The International Organization for Standardization/the International Electrotechnical Commission standard 2381-1: 1993 (en), Information technology — Vocabulary — Part 1: Fundamental terms, https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-1:ed-3:v1:en.

61 H. Nissenbaum, Privacy in Context. Technology, Policy, and the Integrity of Social Life, Stanford 2010, p. 67.

62 A. Saarenpää, Openness, Access, Interoperability and Surveillance: Transparency in the New Digital Network Society [in:] E. Schweighofer, F. Kummer, W. Hötzendorfer (ed.), Transparency, Proceedings of the 17th International Legal Informatics Symposium IRIS 2014, Salzburg 2014, p. 241.

63 P. Leith, Privacy as Slogan, [in:] A. Saarenpää (ed.), Legal privacy, Zaragoza 2008, p. 99.

64 W. Diffie, S. Landau, Privacy on the Line. The Politics of Wiretapping and Encryption. Updated and Expanded Edition, MIT 2007, p. 142.

The most often quoted idea on privacy seems to be the one presented by Samuel D. Warren and Louis D. Brandeis in their famous *The Right to Privacy*[65] - the right to be left alone. Following this, according to one of Oxford English Dictionary definitions privacy can be described as:

> The state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; seclusion; freedom from interference or intrusion.[66]

Interestingly, from the mass surveillance point of view, Oxford English Dictionary, among together six proposed definitions, gives us also this one:

> Absence or avoidance of publicity or display; secrecy, concealment, discretion; protection from public knowledge or availability.

It is also underlined that this definition is now rarely used, or as a part of the one quoted above. I decided to point out this one as one part of the description of privacy in possible accordance with social media and mass surveillance.

Continuing the thought that privacy can be understood in many ways, Ahti Saarenpää reminds us that privacy even as a concept can be understood differently in international literature.[67] On the one hand side we have simpler definitions, mostly focusing on one aspect of the issue. Again, probably the famous *the right to be let alone* is a good example. On the other hand, Lee Bygrave decided to distinguish four general ways to understand privacy, by collecting several ideas. He states that *the privacy concept is pregnant with definitional variation. Analysis of the literature on privacy reveals four major ways of defining the concept.*[68]

- Privacy viewed essentially in terms of non-interference (Right to be left alone)
- Privacy in terms of degree of access to a person (Limited accessibility)
- Privacy in terms of information control (When, what and how information is communicated to others)
- Privacy related to aspects of persons' lives that are intimate and/or sensitive (As a result not every disclosure of information is a loss of privacy)

Knowing all that and even more, because literature on concept of privacy is so expanded that calling it unlimited would not be an exaggeration, we still have one problem. What about respecting privacy? This is just one side of the coin. In

65 Warren S. D., Brandeis L. D., The Right to Privacy, Harvard Law Review, 4(5), 1890, p. 193-220.

66 http://www.oed.com/view/Entry/151596?redirectedFrom=privacy

67 Saarenpää A., Perspectives on Privacy, [in:] Saarenpää A. (ed.), Legal privacy, Zaragoza 2008, p. 23, Gerety T., Redefining Privacy, [in:] Harvard Civil Rights-Civil Liberties Law Review, vol 12, number 2, 1977, p. 233

68 Bygrave L., Data Protection Law: Approaching its Rationale, Logic and Limits, Kluwer Law International 2002, p. 128-129.

today's globalized society, Network Society, Internet users very often do not respect their own privacy. Social media pages are designed to encourage us to reveal us much information as possible. *Teenagers will freely give up personal information to join social networks on the Internet*.[69] The world of privacy became the place where teenagers reveal every detail about their lives online as well as a place where government agencies and marketers are collecting personal data about us. The ways to both reveal information and be the subject of the collection are numerous if not unlimited. Social media pages, applications and services by Facebook or Google, mass surveillance programs such as PRISM or Tempora.[70] If that is not enough, also should be mentioned driver licenses databases, online shopping profiles, credit card companies' databases, etc.

Susan Barns[71] suggests that in the age of digital media we probably do not have any privacy.[72]

1.5. Which Dominant ICT Companies

Facebook, Google and Microsoft. These are the companies I am choosing as the brightest examples. Examples of abuses, dominance, strong position on several markets and finally because they are extremely well-known names in the world. Simply, everyone knows them and something about their actions. I purposely do not include any Chinese or Russian companies as they often held the dominant position of respective national markets, but in my opinion, have no legal and business influence on European Union and the United States.

The first question is, are these companies really dominant, or can they be called super dominant? It is easy to make this kind of assumption, but equally easy is the realization that when it comes to legal definitions, nothing is that obvious.

Google and Microsoft have already been accused of abusing their dominant positions.[73] The European Commission stated that these companies are dominant in respective markets. Microsoft was even called super dominant on the market of operating systems.[74] Case closed; these companies are dominant.

---

69 Barnes S. B., A privacy paradox: Social networking in the United States, First Monday, Volume 11, Number 9 - 4 September 2006, http://firstmonday.org/ojs/index.php/fm/article/viewArticle/1394/1312%2523

70 More about PRISM and Tempora in part five: PRISM and what stands behind it.

71 Susan B. Barnes is a Professor in the Department of Communication at the Rochester Institute of Technology (RIT).

72 Barnes S. B., A privacy paradox...

73 Decision of European Commission from 24.03.2004 r. in T-201/04 case, Microsoft, point 18, Crane D. A., Search Neutrality and Referral Dominance, [in:] Journal of Competition Law & Economics, 8(3), p. 459, http://www.theregister.co.uk/2012/05/21/joaquin_almunia_google_statement/

74 SPEECH/07/539, 17.09.2007 r., R. Whish, Competition Law 6th Edition, New York 2009, p. 185.

Google is a company that is hard to assess or even compare to the rest of dominant companies. Definitely superdominant on the market of search engines and having huge share on the market of mobile operating systems owning Android and on the market of internet browsers thanks to Chrome, but at the same time almost free from some massive security issues. On the other hand, Google as the owner of an application called Google Adds is known for buying data from Facebook. Google is given a place here because of its huge database (Google search engine) and a number of connections (Android, Chrome, illegal business connections with Facebook).

Microsoft was called by Court of Justice of the European Union a superdominant company. Dominant position on various markets gives a wide and constant access to the personal data of hundreds of millions of users. Microsoft is mostly well known for its Windows operating systems and internet browser Internet Explorer, but also for being major shareholder or an owner of some other brands such as Bing and Yahoo! search engines, Skype, Windows Live Messenger and Hotmail. It is not a common knowledge that Microsoft holds 1.3% of Facebook shares. In 2011 Microsoft acquired Skype for 8.5 billion dollars. Skype became a global, most commonly used Internet communicator - in 2016 Skype number of users was estimated at 300 million.[75] Together that gives a wide and constant access to personal data of over 1 billion users.[76]

What with Facebook, my third example? So far Facebook has never been an object of a competition law investigation, nor has it been accused of abusing its position. In my opinion, according to competition law, Facebook is not a dominant company in any specific market. Why? Because the dominance of the company is investigated only if the company is accused of conducting abuses. Could I then just say "case closed, Facebook is not dominant on any market"? No. The fact is that Facebook is dominant in the market of social media. To what extent, this is not exactly established.

Facebook is a phenomenon - giving a series of examples, how many abuses can be conducted in the area of data security and data protection. Facebook is probably the first place on the Internet where people freely and without proper understanding give details about almost every single information of their life. Yes, there was MySpace before, but the scale was always much smaller, having a less significant impact on privacy and society.[77] Names, photos, addresses, e-mail addresses, phone

75 Skype in decline: Who broke it?, 2018, https://borncity.com/win/2018/05/13/skype-in-decline-who-broke-it/

76 According to Microsoft's own data from 2017 Windows 10 had 45% market share, meaning the actual installed base for all versions of Windows is 600 million/0.45 = 1.33 billion Windows users. - 2018, https://mspoweruser.com/microsofts-numbers-once-again-suggest-there-are-less-active-windows-users-than-we-think/

77 Newman D., The Difference Between Facebook and Myspace, 2014, https://www.fool.com/investing/general/2014/02/10/the-difference-between-facebook-and-myspace.aspx

numbers and possibly many others. We create a kind of profile of ourselves with high commercial value that can be used for directing specific ads and sold to Google or Yahoo!. With over 2.32 billion monthly active users Facebook might be the biggest private database in the world.[78] On top of that, Facebook is the biggest abuser and offender when it comes to securing and protecting collected data. Some examples include transmitting identifying information to dozens of advertising and Internet tracking companies. Facebook is not immune to so called socialbots, small programs impersonating the real profiles of Facebook users, normally operate at the same time, posting comments and sending invitations to different people. Socialbots stole[79] 46,500 thousand email addresses and 14,500 thousand home addresses.

The way and the moment competition law decide that a particular company is dominant, causes some problems and again forces me to avoid a typical legal understanding of the term "dominance". In my Dissertation, I need to refer to Facebook as to the dominant company without using any additional qualification, such as "in fact" or "as the numbers indicate".

1.6. Structural Overview

The dissertation consists of six chapters:

INTRODUCTION
Chapter 1 presents the meaning of the topic, specifically to clarify the focus on privacy and data protection rather than competition law, source material used in the work and the methodology, research questions and the purpose of the dissertation. It also discusses the central terms, their definitions used by the researcher and their concepts. For this dissertation and a better understanding of the discussion and the topic four terms are presented in detail: abuse, dominance, personal data, data/information and privacy.

THE LEGAL BACKGROUND
Chapter 2 establishes the historic and legal background necessary for the dissertation. Here, the researcher explains the importance and influence of legal informatics in the discussion, the history and development of legal science that led to the development of data protection and privacy laws. Especially in the relevance to new technologies.

78 The Top 20 Valuable Facebook Statistics – Updated April 2019, https://zephoria.com/top-15-valuable-facebook-statistics/

79 Socialbots used by researchers to 'steal' Facebook data, 2011, https://www.bbc.com/news/technology-15553192

Additionally, this chapter describes data protection legislation in European Union and in less detail in the United States. Understanding of privacy is compared between EU and US, which allows, together with the earlier description of data protection laws, to understand differences in approaches towards ICT companies on both sides of the Atlantic. Finally, some remarks about the direction of legal changes are made: specifically focusing on cases of Safe Harbour/Privacy Shield and the Google Case/Right to be Forgotten Judgement.

THE REALITY BACKGROUND

Chapter 3 firstly describes the reality in which ICT companies and their clients and users exist. This includes explaining the complicated nature of computer or virtual reality in which we live nowadays, as well as the changes in modern society. Researcher describes the network society that evolved from industrial society and proposes the new term society trapped in the network as an explanation for some phenomena, such as global popularity or even addiction to social media. And the repercussions coming from that.

This chapter brings up the topic of the Deep Web, including the Dark Web as places and tools explaining the relevance of the Internet, its impact on the network society and privacy. Both as a danger to it and the potential way of protection.

Further, the chapter describes mass surveillance, specifically global surveillance disclosures by Edward Snowden. This part aims to reveal the connections between national agencies and dominant ICT companies, the impact on privacy and data protection – both in positive and negative aspects.

Finally, chapter 3 demonstrates the radical influence of technology on society and legislation. In this part, the researcher focuses on presenting generally the rapid changes in ICT technologies, the importance of modern databases and blockchain technology. This is the latest example of the challenges to the law coming from technology.

DOMINANT ICT COMPANIES – THREE SUPERDOMINANT PLAYERS

Chapter 4 is entirely dedicated towards a detailed analysis of the three chosen companies: Facebook, Google and Microsoft. It describes their history and background, dominance on relevant markets and relevance of this dominance to the topic of the dissertation. Although, the main focus is on giving a broad spectrum of abuses' examples conducted by these companies. Given the topic of this dissertation, all the examples are in the connection of data protection and privacy matters.

The chapter brings up the role of dominant ICT companies – what impact these chosen by the researcher companies have on society, privacy and finally the legislation. The aim is to point out both negative and positive impact.

Finally, there is a short analysis of the cooperation and competition between dominant ICT companies, not only Facebook, Google and Microsoft, and the relevance of those to the topic.

The chapter ends with a short summary that focuses on the consequences of abuses committed by dominant ICT companies.

EFFORTS AGAINST ABUSES OF DOMINANT ICT COMPANIES

Chapter 5 aims to list all the efforts directed to deal with the situation described in the dissertation. It includes firstly legal efforts, with the focus on legislative and judicial proceedings – the role of EU Data Protection Reform (GDPR) and coming changes (ePrivacy Regulation), Safe Harbour Judgement and Max Schrems v Facebook, Google Case, and US dealings with ICT companies. Secondly, there is a place for independent ideas such as European Center for Digital Rights (NOYB) and Project R.O.S.E. (Return On Social Engagement). Thirdly, the role of the technology – Dark Web and blockchain technology. Finally, the chapter mentions the potential role of competition as a substitute for data protection laws.

CONCLUDING REMARKS

The final chapter, chapter 6, shows if the dissertation answered the research questions. It also summarises all main conclusions together.

2. THE LEGAL BACKGROUND

2.1. Introduction to the field and to the Legal Informatics

Legal informatics is no longer a young and an unknown discipline. However, still a word is in place to describe its main characteristics. Legal informatics is a branch of legal science. This means that problems are defined and dealt with according to criteria, which the legal community consider relevant and comprehensible. But legal informatics strives to go beyond traditional, text-oriented analyses of valid law (normative or 'dogmatic' legal science). Thus, legal informatics is interdisciplinary and strives to complement the traditional legal perspective with perspectives from the field of informatics.[80]

2.2. History and development

The development of legal informatics has been going on for more than 70 years. Already in the late 1970s the field had a history that could be divided into different periods: the period of forerunners until about 1960, the period of growth during the 1960s and the period of maturing during the 1970s.[81] The actual term "legal informatics" was introduced by Wilhelm Steinmüller in 1970s.[82] The forerunners were disparate attempts to discuss computer-related aspects of law such as Lee Loevinger's vision of legal thinking based on quantitative and formal reasoning in 1949 and Norbert Wiener's reflections on cybernetics and law in 1954.[83] During the 1960s the literature in the field grew and comprised both works on the emerging concept of 'computer law' and analyses of computer assisted legal decision-making and automated information retrieval.[84] This development continued during the 1970s and was accompanied by a number of attempts to understand the broader

80 Seipel P., IT Law in the Framework of Legal Informatics, Stockholm Institute for Scandinavian Law 1957-2010, p. 32-33, Saarenpää A., Legal Informatics – the View from the University of Lapland

81 Seipel, P., Computing Law. Perspectives on a New Legal Discipline, Liber, Stockholm 1977, p. 112-116.

82 Bing J., Let there be LITE: A brief history of legal information retrieval, [in:] Paliwala A., A History of Legal Informatics, Zaragoza 2010, p. 31

83 Loevinger, L., Jurimetrics the Next Step Forward. Minnesota Law Review, 33/1949. Wiener, Norbert, The Human Use of Human Beings. Cybernetics and Society, Eyre & Spottiswoode, London 1954.

84 Duggan, M. A., Law and the Computer. A KWIC Bibliography, Macmillan Information, New York 1973.

context and explain the notion of legal informatics.[85] Special research institutes oriented towards legal informatics began to appear by the end of the 1960s and the early 1970s.[86] Legal informatics provides a fertile ground for the continued development of IT law. In a word, legal informatics opens ways of adding to and enriching traditional ways of dealing with IT-related aspects of law. Moreover, the advance of legal informatics itself will benefit from letting the field encompass both regulatory aspects of the use of IT and IT applications in the field of law.

Small, but important part of legal informatics is data protection. Today we are witnessing the emergence of the third generation of data protection acts thanks to General Data Protection Regulation, where data protection is now a fundamental right.

The notion of data protection originates from the right to privacy and both are instrumental in preserving and promoting fundamental values and rights. Different cultures have different understanding of that privacy term, some even seem to do not it understand in a way that could allow creating law to protect "privacy". Many cultural and even historical elements make enacting sufficient data protection laws almost impossible.

Data Protection Directive[87] was adopted in 1995, when the Internet was still in its infancy. Today EU enjoys protection from updated and long waited General Data Protection Regulation.[88]

Today information on web surfing habits allows service providers to tailor products to customers' needs, placing for example ads which are relevant for people doing frequent searches for the best flight deals. But some private information can be very sensitive, such as credit card numbers or bank account deposit details. Other type of sensitive information may relate to people's health condition or sexual or political orientation. Location data or online identifiers, such as cookies, are also widely considered as personal data.

Meanwhile, EU citizens are becoming increasingly aware of the possibilities for misusing their personal information. According to a recent Eurobarometer poll[89], 51% of those surveyed say they have only partial control over their personal information online, and nearly a third (30%) feel that they have no control at all.

Data protection law restricts the processing of personal data and grants legal rights to individuals in how they are processed. It was developed in Europe in the 1970s and 1980s and has now spread to all regions of the world. However, only

85 Reisinger, Leo, Rechtsinformatik, de Gruyter, Berlin 1977.

86 The Swedish Law and Informatics Research Institute began its work in 1968, then named The Working Party for EDP and Law. In 2018 published anniversary book: Wahlgren P. (ed.), 50 Years of Law and IT, Scandinavian Studies in Law, Vol. 65, 2018

87 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

88 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

89 Special Eurobarometer 487a, The General Data Protection. Summary, June 2019

a small number of countries (Australia, Brazil, Japan, South Korea, Thailand and USA) are considered to have, what now can be called GDPR-like data privacy laws.[90]

The development of the right to privacy and, specifically, to data protection within the EU legal includes the case law of the ECJ. Since the EU established its high standard of data protection through the Directive, and continues it with GDPR, the ECJ has upheld such standard, and even further raised the status of this right. The Court has prioritized privacy over other rights and freedoms to the point that critics claim it has created a type of super-human right.[91] In cases relating to the Directive, the Court has used the principle of proportionality and established a strict necessity test in order to justify violations of privacy.[92] The principle of proportionality was established in 2003 with the Österreichischer Rundfunk case in which the Court found that Austrian measures to disclose information regarding public funds – a legitimate state interest – did not pass the proportionality test set down in the Directive, as they infringed on the privacy of the persons in question by potentially causing them harm arising from such publicity.[93] Important cases raising the standard of privacy protection include the 2008 Huber case,[94] 2008 Satamedia case,[95] and 2010 Schecke case.[96] In the Satamedia case, the ECJ clarifies that when balancing two fundamental rights, such as privacy and freedom of expression, the right to privacy requires that any derogations and exceptions be applied only as strictly necessary. The "strictly necessary" test was reiterated by the Court in the 2013 IPI case[97] and 2014 Digital Rights Ireland case.

The question of transfer of data to third countries was first brought to the ECJ in the 2003 Lindqvist case.[98] Another important case to transborder data flow is the 2014 Google Spain case and finally the Schrems case. Both widely described and discussed in this dissertation.[99]

90 Simmons D., 6 Countries with GDPR-like Data Privacy Laws, January 17, 2019, https://insights.comforte.com/6-countries-with-gdpr-like-data-privacy-laws

91 Lehofer H. P., EuGH: Google muss doch vergessen – das Supergrundrecht auf Datenschutz und die Bowdlerisierung des Internets, E -Comm, 13 May 2014, http://blog.lehofer.at/2014/05/eugh-google-muss-doch-vergessen-das.html

92 Tranberg, Ch. B., Proportionality and data protection inthe case law of the European Court of Justice, International Data Privacy Law 1, no. 4 (2011), 239-248.

93 Joined Cases C-465/00, C-138/01, and C-139/01 Österreichischer Rundfunk [2003] ECR I-6041, EU:C:2003:294.

94 Case C-524/06 Huber [2008] ECR I-9705, EU:C:2008:724

95 Case C-73/07 Satakunnan Markkinapörssi and Satamedia [2008] ECR I-9831,EU:C:2008:727

96 Joined Cases C-92 and C-93/09 Volker and Marcus Scheke Eifert [2010], ECR,EU:C:2010:662

97 Case C-473/12 IPI [2013], ECR, EU:C:2013:715

98 Case C-101/01 Bodil Lindqvist [2003] ECR I-12971, EU:C:2003:596

99 Case C-131/12 Google Spain SL v. Agencia Española de Protección de Datos [2014], ECR, EU:C:2014:317

2.3. Data Protection

The term "data protection legislation" is used according to the established terminology for legislation, which regulates the use of personal data, both in manual and computerized systems. The traditional term is "privacy", but the traditional implication of this "right to be let alone" became inappropriate for modern data protection legislation.[100]

The computerization of data use was initially seen, in both public and private sectors, to help handle information pertinent to a specific issue, such as a criminal investigation, the cause and symptoms of certain diseases, or the administration of client data. However, the clearer it became that enhanced technology not only allows the processing of a practically endless amount of personal data but also an extendable linkage of data banks, the more the focus has shifted to preventive policies that in a growing number of cases initiate an intensive "predictive surveillance."[101]

Wiener[102] and Frank[103], saluted "cybernetic machines" as guarantees of an unprecedented rationalization of social and political discourse. Their central statement was that never had it been possible to collect and process a virtually unlimited amount of information, and therefore the chances of truly objective decisions had never been so good. Consequently, the rapidly expanding use of "machines" was regarded as the passage to communication structures guided by a thorough and transparent analysis of all relevant information. In the future, decisions about individuals would no longer be based on speculations or influenced by a purely subjective approach.

Databanks, like the collection initiated by the Government of the German Federal State of Hesse in the middle of the 1960s,[104] embodied the hopes evoked by "cybernetic machines." The data collections were to allow efficient long-term policies, such as in finance and social security, and to secure better medical help, especially in emergencies. But while the databanks were at first generally accepted, doubts gradually arose, beginning in 1968, regarding the processing of personal data. The involvement of nearly all Hesse citizens, the storage of especially sensitive data, as those concerning health or income, and the databank's capacity to exploit information for different purposes triggered demands that the Government

100 Bing J., Information Law?, Journal of Media Law and Pratice, 1981, vol. 2, no. 3, p. 8

101 Lynch M., Predictive Surveillance: Precogs, CATCHEM, and DNA Databases, 18 RISK & REG. 8 (Economic & Soc. Res. Council, London, U.K.) (Winter 2009).

102 Wiener N., CYBERNETICS: OR CONTROL AND COMMUNICATION IN THE ANIMAL AND THE MACHINE (2d. ed. 1961).

103 Frank H. G. (ed.), KYBERNETISCHE MASCHINEN, 1964.

104 See HESSISCHE ZENTRALE FUR DATENVERARBEITUNG, GROSSER HESSENPLAN: ENTWICKLUNGSPROGRAMM FUR DEN AUSBAU DER DATENVERARBEITUNG IN HESSEN (1970).

investigate the risks of a permanent surveillance of citizens. Consequently, on October 10, 1970, the Hessian Parliament adopted the world's first Data Protection Act after a short but intensive debate.[105]

The adoption of data protection laws in other countries, begun with Sweden in 1973 and continuing with new data protection laws almost every year all over the world.[106] A common characteristic of nearly all these laws is their omnibus approach. In other words, they all contain rules applicable to every kind of processing of personal data. An approach like this openly contrasts with the prevalence of sectoral-oriented provisions[107] in the United States[108].

Data protection laws have always been marked by the uneasiness in dealing with constantly advancing technology. Legislators deliberately chose a distinctly abstract language to improve the chances to address unknown aspects and new developments of technology. Nevertheless, the more computers expanded, the clearer it became that the original rules had to be replaced by regulations that explicitly took specific uses into account. As a result, lawmakers-especially in Europe-have enacted a second context-oriented generation of data protection regulations. Clearly sectoral laws are, for instance, increasingly used to regulate particularly sensitive processing areas. Statutes, such as those related to social security, preventive medical examinations, various security agencies, handicapped persons, or electronic health cards, include provisions on access to personal data. Europe more and more resembles the United States.[109] Omnibus laws were since the earliest days of data protection, especially in Europe, considered to be the only means to secure both a broad and reliable way to regulate the use of personal data. By now, a mounting and interminable amount of provisions dominates, an experience equally typical for the European Community.[110]

Data protection is a type of privacy protection manifesting in special legal regulation. Considerations about a review of the present data protection law are increasingly overshadowed by what may be the most significant challenge that a regulation of privacy has ever faced. As demonstrated daily by the spread of the Internet, technology has once again transformed the conditions of data use. Radically reassessed marketing strategies

105 Hessisches Datenschutzgesetz [HDSG] [Hessian Data Protection Act], Hess GVB1. I 625 (1970). For its history, see Spiros Simitis, Zwanzig Jahre Datenschutz in Hessen - eine kritische Bilanz, in 19 TATIGKEITSBERICHT DES HESSISCHEN DATENSCHUTZBEAUFTRAGTEN 138 (1990).

106 Data privacy law: the top global developments in 2018 and what 2019 may bring, February 25, 2019, https://www.dlapiper.com/en/finland/insights/publications/2019/02/data-privacy-law-2018-2019/

107 Schwartz P. M., Preemption and Privacy, 118 YALE L.J. 902, 908 (2009).

108 Bellia P. L., Federalization in Information Privacy Law, 118 YALE L.J. 868 (2009). The one American exception to this sectoral approach is the 1974 Privacy Act, 5 U.S.C. § 552a (2000).

109 Schwartz P. M., Preemption and Privacy, p. 913, 931.

110 Simitis S., Privacy - An Endless Debate, California Law Review, Vol. 98, Issue 6, December 2010, p. 1999-2000

for consumer goods, countless chats criticizing products and services, widespread exchanges of experiences with physicians, detailed discussions about marital life, or a disclosure of every aspect of strictly personal habits, shifted data processing more and more to the Internet. In short, the Internet has redefined communication structures in a manner as radical as the introduction of computers.[111]

Data protection right ensures a person the right of disposal over all data in connection with his personality. This way it serves to sustain the protection of privacy in a world where the possibility of collecting, storing and conciliation of large pools of data is widely available. In this situation the significance of facts and data that were previously regarded irrelevant by legislation (regarded as not belonging to the scope of individual secrets) increases: earlier, due to the lack of highly developed data-processing technologies no threat was imposed by a situation in which these data became public and known to others, while today processing, conciliation and association of data or creating new data relying on the old ones might result in the infringement to the right of privacy. The underlying notion behind the codification of data protection law is the insufficiency of secrecy protection: within the new context protection should apply to all data: 'data protection should be differentiated from the interpretation of privacy as intimacy.'

The protection of personal data within the new circumstances can offer the protection of privacy. These statements are true; however, they say little about what privacy is and why it needs protection.[112] However, it is important to remember that EU's General Data Protection Regulation does not use any specific concept of privacy.

The concept of data protection is often treated as part of privacy protection, or quite as its contrary, opposing it, as a specifically European (legal) solution to a problem which contributed to the appearance of the "right for private life" in American constitutional law. In my view several – legal and extra-legal – tools, methods of privacy protection may be distinguished, and the notion itself may be applied to a far wider category of phenomena than data protection – data protection might be understood only within the framework of privacy protection as a legal tool of privacy protection, born within a given social and technical context. We should also not disregard the fact that the notion of privacy is used today in a much broader sense in American legal thinking – as I have referred to it above, as a result of the development it has gone through since the end of last century, by now it can be interpreted as the equivalent of general personality right.

This protection existed already before the appearance of data protection: privacy protection was provided by extra-legal, natural boundaries, or the extra-legal system of

111 Simitis S., Privacy - An Endless Debate, California Law Review, Vol. 98, Issue 6, December 2010, p. 2003

112 DATA PROTECTION LAW - AN INTRODUCTION by András Jóri – data protection.eu

social norms. Following the appearance of data protection these tools may be (and are) applied continually. Data protection as a specific legal protection appeared as a result of the weakening or disappearance of some natural boundaries that earlier ensured the protection of privacy. In recent years, however, parallel modes of privacy protection have regained their earlier significance –this phenomenon might be understood as the crisis of data protection. On the one hand, this crisis is prompting efforts to renew data protection as legal protection, on the other hand it widens data protection regulations, because the size of other (mostly technological) measures and tools serving privacy protection is increasing (on this issue see below the part on data security).

Data protection, thus, may be interpreted within privacy protection according to the following:

a. data protection in all cases means the legal protection of an individual's privacy, which
b. appeared in Europe as an answer to the dangers of electronic data processing which were becoming widespread via the electronic revolution, beginning with the 1970s, and
c. the content of the legal protection provided by it has changed significantly since its appearance several times and is still changing presently.

Data protection cannot be identified with the right of informational self-determination, since the early data protection laws did not ensure an individual any disposal over his personal data. Although the appearance of the right of informational autonomy is a significant milestone in the history of data protection, it is still wrong to claim that the development of data protection cannot go beyond the basic principles of the right of informational self-determination. There is a view according to which data protection based on the right of informational autonomy is undergoing a crisis, and that the latest generation of data protection regulations is based on the right of informational self-determination only nominally. Thus, data protection includes all regulations that, via the regulation of the treatment of an individual's personal data, aim at the protection of these data, irrespectively of whether this regulation ensures the right of informational self-determination of an individual or not. [113]

Answering the simplest question, what does "data protection" mean? leads to the list of answers:

- the right to control and decide how (autonomy)
- the right to know how
- the right to live your life without undue interference (confidentiality in all communications, regulated by law)
- the right to be evaluated on the basis of correct and relevant information

113 DATA PROTECTION LAW - AN INTRODUCTION (The notion of data protection) by András Jóri – data protection.eu

- the right to know what criteria automatic decision-making systems are based on
- the right to trust data security = secures other rights
- the right to receive assistance from independent authorities
- the right to be treated in accordance with all other basic rights (democracy)

We need all these rights so that:

- our human dignity is respected
- our autonomy is respected
- our honour is respected
- we will not be discriminated
- our equality as citizens is secured.

Before presenting legal framework dedicated to privacy and data protection, few words must be said about the big problem of legislation nowadays. This problem is recognized as overregulation. According to Wolfgang Kilian data protection is overregulated in the public field and leaves no longer a chance for self-determination of a data subject. Self-determination only matters in the private field.[114] He continues the critique of current state of data protection with following words:

- Data subjects are no longer able to maintain control on the use of their personal data effectively, for many reasons (e.g. data networks; Internet; hierarchies of users; commercial services).
- The current legal framework is based on the assumption that in the private field the informed consent of a data subject is structuring the collection, storage, use, and transmission of personal data. This is a fiction, since hidden primary and secondary uses of personal data are predominant. Personal data have become a marketable good.[115]

Before going into details, it is worth mentioning most general efforts. The worldwide interest to create better protection for privacy and personal information has bring efforts to harmonize national legislations in this field during the last 30 years. The progress has been tried to make via agreements and different kind of recommendations. One of the first was the OECD Data Protection Recommendation in 1980. (Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of the Personal Data, 23.8.1980). The second important document was the Council of Europe's Data Protection Convention in 1981. (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (108/1981). Most of the EU-countries have

114 Kilian W., Leibniz University Hannover, Germany, August 11, 2009, http://ec.europa.eu/justice/news/consulting_public/0003/contributions/citizens/kilian_wolfgang_en.pdf

115 Ibid.

ratified the last-mentioned convention and EU also accepted the convention as a society in 1999.

The European Convention on Human Rights has also to be kept in mind when we analyze the development of privacy and data protection regulation in Europe. The OECD Recommendation and European Convention are very similar when we analyze the contents of them. The member states have promised to enforce the European Convention principles concerning the data protection in their own national legislation. The Council of Europe has also produced many other recommendations in the field of privacy and data protection. Above mentioned conventions and recommendations were the background material when the law-drafting process of EU Personal Data Directive started in 1992.

We may have found ourselves nowadays in uncomfortable situation of overregulating data protection. This leads to slowing down regulatory efforts – the more regulations we create, the more problems appear.[116]

Privacy is mentioned in 1967 International Covenant on Human Rights and in Article 12 of the 1948 Universal Declaration of Human Rights, but in Europe it is also acknowledged by Article 8 of the European Convention of Human Rights. Additionally, on international level, we have Treaties of Rome and Strasbourg by European Council and the Treaty on Civil Rights and Political Rights by United Nations. On national level: constitutions and national privacy laws. Privacy was the core topic in United Nations Privacy Resolution on November 2013 Draft Resolution: *The right to privacy in the digital age*:[117]

One of the most important documents treating on privacy is OECD and European Commission 8 principles formulated in 1980. OECD has revised in 2013 its Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data.[118] Among them, I would like to point out four, which may be most significant in the protection of privacy discussion:

- *implementing privacy management programs* - essential elements discussed in this respect include privacy policies, employee training and education, provisions for sub-contracting, audit process and privacy risk assessment;
- *introducing mandatory data security breach notification* - requiring notification to the privacy enforcement authority where there is a significant security breach affecting personal data and notification to individuals where such a breach is likely to adversely affect individuals;
- *the need for privacy enforcement authorities and national privacy strategies* - the revised Guidelines recognize the need to establish authorities with the governance, resources and technical expertise necessary to exercise their powers

116 Rowland D., Kohl U., Charlesworth A., Information Technology Law..., p. 5-6.
117 http://www.hrw.org/sites/default/files/related_material/UNGA_upload_0.pdf
118 OECD work on privacy, http://www.oecd.org/sti/ieconomy/privacy.htm

effectively and to make decisions on an objective, impartial and consistent basis; they also promote the development of a coordinated approach across governmental bodies up to the highest levels; Member countries should also consider complementary measures, including education and awareness raising, skills development and the promotion of technical measures;

- *improving global interoperability* - to be improved through international arrangements (examples mentioned include the U.S.-EU Safe Harbour framework, the EU Binding Corporate Rules and the Council of Europe Convention 108 on the Automated Processing of Personal Data) and global cooperation among privacy enforcement authorities.

Original OECD guidelines had strong influence on Data Protection Directive. Today revised provisions influenced the EU GDPR's final wording on data breach notification.[119]

In 1995, European Union adopted Data Protection Directive[120] that regulated the processing of personal data within the European Union. Controversies accompanied the history of the 1995 European Data Protection Directive, as once more there were tenacious attempts to eliminate or at least weaken an independent external control of data processors. There has also been a virtually indefinite postponement of the long overdue review of the Directive.[121]

Today we have got the regulation that supersede the old and, in many aspects, outdated directive - General Data Protection Regulation.[122] The main novelty of the Regulation is in fact the use of regulation in favour of directive. Rules on breach notification are new, but in general, Directive and Regulation cover mostly the same. According to Peter Blume, it is *due to the fact that the rules are technologically neutral*. He also points out that there is a risk of not including in the Regulation *new phenomena such as cloud computing in the better or more comprehensive way than it is made possible by the directive*.[123] Now not only we have to wait for Regulation to be enacted, but it will take many years before the next generation of data protection

119 Mitchell R., Revised OECD Privacy Guidelines Focus On Accountability, Notification of Breaches, September 16, 2013, http://www.bna.com/revised-oecd-privacy-n17179877087/

120 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

121 Simitis S., Privacy - An Endless Debate, California Law Review, Vol. 98, Issue 6, December 2010, p. 1997.

122 Regulation (EU) 2016/679 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 119/1

123 Blume P., An Evolving New European Framework for Data Protection, [in:] D. Svantesson, S. Greenstein (ed.), Nordic Yearbook of Law and Informatics 2010-2012. Internationalisation of Law in the Digital Information Society, Copenhagen 2013, p. 24.

rules will emerge.[124] Nevertheless, occurring changes and growing attention given to privacy and its protection give a hope for positive changes in European Union.

In United States, things are more complicated. First of all, there is no legislation following OECD and European Commission principles. Secondly, there is no general privacy laws including that there is nothing in US Constitution. The right to privacy is also not enumerated in the Bill of Rights. However, it is protecting some specific aspects of privacy as U. S. Supreme Court has found a right to privacy through its interpretation of the First, Third, Fifth and Ninth Amendments.[125] This interpretation allows recognizing:

- privacy of believes,
- privacy of the home against demands that it be used to house soldiers,
- privacy of the person and possessions as against unreasonable searches,
- privilege against self-incrimination, which provides protection for the privacy of personal information;

The right coming from Ninth Amendment is giving protection of privacy in ways not specifically provided in the first eight amendments.[126] U. S. Constitution's protection of privacy is rather the matter of very broad interpretation. Yet, polls show most Americans support this broader approach.[127]

If these examples of how imprecise regulation of privacy in United States were not enough to understand the issue, this is a statement by a U. S. Supreme Court on the subject of privacy:

> The makers of our Constitution understood the need to secure conditions favourable to the pursuit of happiness, and the protections guaranteed by this are much broader in scope and include the right to life and an inviolate personality -- the right to be left alone -- the most comprehensive of rights and the right most valued by civilized men. The principle underlying the Fourth and Fifth Amendments is protection against invasions of the sanctities of a man's home and privacies of life. This is a recognition of the significance of man's spiritual nature, his feelings, and his intellect.

---

124 Ibid. p. 35.

125 Westby J. R., Project Chair (ed.), International Guide to Privacy. American Bar Association Privacy & Computer Crime Committee Section of Science & Technology Law, ABA Publishing 2004, p. 11-12 [after:] Development of the Right to Privacy in Information, http://www.csu.edu.au/learning/ncgr/gpi/odyssey/privacy/orig_priv.html (from the U. S. Cogress, Office of Technology Assessment, Protecting Privacy in Computerized Medical Information, OTA-TCT-576, U. S. Government Printing Office, September 1993) (hereinafter Development of the Right to Privacy in Information).

126 The Right of Privacy. The Issue: Does the Constitution protect the right of privacy? If so, what aspects of privacy receive protection?, http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html

127 Ibid.

All above does not mean that the United States lacks provisions for data privacy. It is quite the opposite, and it seems that American legal system also suffers from the overregulation problem. According to InformationShield[128] United States Data Privacy Laws, consist of 28 acts![129]

One of the consequences of this division of laws concerning privacy is emergence of American Civil Liberties Union (ACLU). They say about themselves that *the ACLU is nation's guardian of liberty, working daily in courts, legislatures and communities to defend and preserve the individual rights and liberties that the Constitution and laws of the United States guarantee everyone in this country*.[130] ACLU is the most important organizations protecting privacy and fighting for civil rights in United States, established in 1920. The right to privacy understanding by ACLU is expressed as *freedom from unwarranted government intrusion into personal*

---

128 http://www.informationshield.com/

129 United States Privacy Laws, http://www.informationshield.com/usprivacylaws.html:

1. Americans with Disabilities Act (ADA)
2. Cable Communications Policy Act of 1984 (Cable Act)
3. California Senate Bill 1386 (SB 1386)
4. Children's Internet Protection Act of 2001 (CIPA)
5. Children's Online Privacy Protection Act of 1998 (COPPA)
6. Communications Assistance for Law Enforcement Act of 1994 (CALEA)
7. Computer Fraud and Abuse Act of 1986 (CFAA)
8. Computer Security Act of 1987 - (Superseded by the Federal Information Security Management Act (FISMA)
9. Consumer Credit Reporting Reform Act of 1996 (CCRRA) - Modifies the Fair Credit Reporting Act (FCRA).
10. Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003 law overview.
11. Electronic Funds Transfer Act (EFTA)
12. Fair and Accurate Credit Transactions Act (FACTA) of 2003
13. Fair Credit Reporting Act
14. Federal Information Security Management Act (FISMA)
15. Federal Trade Commission Act (FTCA)
16. Driver's Privacy Protection Act of 1994
17. Electronic Communications Privacy Act of 1986 (ECPA)
18. Electronic Freedom of Information Act of 1996 (E-FOIA)
19. Fair Credit Reporting Act of 1999 (FCRA)
20. Family Education Rights and Privacy Act of 1974 (FERPA; also known as the Buckley Amendment)
21. Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLBA)
22. Privacy Act of 1974 - including U.S. Department of Justice Overview
23. Privacy Protection Act of 1980 (PPA
24. Right to Financial Privacy Act of 1978 (RFPA)
25. Telecommunications Act of 1996
26. Telephone Consumer Protection Act of 1991 (TCPA)
27. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)
28. Video Privacy Protection Act of 1988 discussion and overview.

130 https://www.aclu.org/about-aclu-0

and private affairs. ACLU is nowadays mostly focused on issues connected to mass surveillance:

In the wake of 9/11, mass surveillance has become one of the U.S. government's principal strategies for protecting national security. Over the past decade, the government has asserted sweeping power to conduct dragnet collection and analysis of innocent Americans' telephone calls and e-mails, web browsing records, financial records, credit reports, and library records. The government has also asserted expansive authority to monitor Americans' peaceful political and religious activities.

Data protection and privacy often overlap but are not identical. Privacy generally protects against intrusion into an individual's "private space", whereas data protection regulates the processing of an individual's personal data, whether or not such data are considered "private". A good starting point for understanding the distinction between the two concepts in EU law and European human rights law is the article by Juliane Kokott and Christoph Sobotta[131] published in International Data Privacy Law.

Data protection law is designed to protect against the untransparent processing of data files which may not seem "private" when considered in isolation, but which when combined can reveal a great deal about an individual's personality.

Data protection law was originally derived from human rights instruments such as the UDHR (Article 12) and the ICCPR (Article 17) that protect the right to privacy and private life. The only legally binding convention of potentially global scope dealing with data protection is Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108). The European Court of Human Rights has interpreted Article 8 of the European Convention on Human Rights (covering the right to private life) to include data protection (e.g., Rotaru v Romania (2000) ECHR 191), and EU law protects data protection as a fundamental right in both the Charter of Fundamental Rights of the European Union (Article 8) and the Treaty on the Functioning of the European Union (Article 16). To give just one example of the spread of data protection as a fundamental right outside Europe, the Economic Community of West African States (ECOWAS) has adopted a "Supplementary Act on Data Protection" that is based in part on the African Charter on Human and Peoples' Rights.

To date, the European Commission has recognised Andorra, Argentina, Canada (commercial organisations falling under the scope of the Personal Information and Electronic documents Act – PIPEDA), Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay as providing adequate protection.[132]

131 Kokott J., Sobotta Ch., The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law, 2013, Vol. 3, No. 4, http://idpl.oxfordjournals.org/content/3/4/222.full.pdf+html

132 Handbook on European data protection law. 2018 edition, https://publications.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1

Regarding the transfers to the US, the European Commission adopted an adequacy decision in 2000 allowing transfers to companies that self-certified their protection of personal data transferred from the EU and compliance with the so-called Safe Harbour principles.[133] The CJEU invalidated this decision in 2015 and a new adequacy decision was adopted in July 2016, allowing companies to join as of 1 August 2016. After the CJEU declared the Safe Harbour arrangement invalid, the Commission and the US agreed on a new framework, the EU-US Privacy Shield. On 12 July 2016, the Commission adopted a decision declaring that the US ensures an adequate level of protection for personal data transferred from the Union to organisations in the US under the Privacy Shield.[134] Finally, on 16 July 2020, the Court of Justice of the EU invalidated the Commission adequacy decision underlying the EU-US Safe Harbour arrangement.[135]

A growing number of international bodies support recognition of a right to data protection, as demonstrated by the recent UN General Assembly Resolution[136] condemning the "arbitrary collection of personal data", and by General Comment No. 16 to the ICCPR[137], which refers to the obligations of States to enact measures deriving from data protection law (such as providing individuals with the right to request rectification or deletion of their personal data, see para. 10).

---

133 Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215. The Decision was declared invalid by the CJEU in http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362):-632/14, Maximilian Schrems v. Data Protectionhttp://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362):-632/14, Maximilian Schrems v. Data Protectionhttp://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362):-632/14, Maximilian Schrems v. Data Protectionhttp://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362):-632/14, Maximilian Schrems v. Data Protection[GC].

134 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207. The Article 29 Working Party welcomed the improvements brought by the Privacy Shield mechanism compared to the Safe Harbour decision and commended the Commission and the US authorities for having taken into consideration in the final version of the Privacy Shield documents the concerns voiced in their opinion WP238 on the draft EU-U.S. Privacy Shield adequacy decision. Nevertheless, it highlighted a number of outstanding concerns. For more details, see Article 29 Data Protection Working Party, Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision, adopted on 13 April 2016, 16/EN WP 238.

135 PRESS RELEASE No 91/20, Court of Justice of the European Union, The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield, Luxembourg, 16 July 2020, https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf, more in 5.1.3.

136 http://daccess-dds-ny.un.org/doc/UNDOC/LTD/N13/576/77/PDF/N1357677.pdf?OpenElement

137 http://www.unhchr.ch/tbs/doc.nsf/(Symbol)/23378a8724595410c12563ed004aeecd?Opendocument

Codification Division of the UN Office of Legal Affairs concluded in 2006 in a report for the International Law Commission (ILC) that data protection is an area "in which State practice is not yet extensive or fully developed" and the UN General Assembly Resolution referred to above reaffirms "the right to privacy" without specifically mentioning data protection. In addition, the 35th Annual Conference of International Data Protection Commissioners would hardly have called in September 2013 for the adoption of an additional protocol to Article 17 ICCPR[138] to "create globally applicable standards for data protection" if the right to data protection already enjoyed sufficient international recognition.

Discussion of the extraterritorial application of privacy rights has thus far dealt mainly with cases of intelligence surveillance by foreign governments.

Everyday processing of personal data online gives rise to questions concerning the extraterritorial applicability of data protection law that go beyond intelligence surveillance. Billions of individuals use the Internet, and there is uncertainty about basic questions such as whether data protection rights apply when an individual accesses a foreign web site, and how to resolve conflicts between data protection requirements "attaching" to data transferred internationally and the law enforcement requirements of the place to which they are transferred. For example, Indian law enforcement authorities regularly seek access to personal data accessible online from India, even when the data are stored in foreign countries that have strong data protection laws. It is thus not surprising that The Hague Conference on Private International Law noted in a paper published in 2010 (para. 14)[139] that "cross-border data transfers have raised serious questions of international jurisdiction".

Data processing is carried out not by the State, but by private entities. We lack a sound conceptual model of how the protective duty of the State under data protection law can be applied and enforced extraterritorially on the global Internet, a question that is even more difficult with regard to data processed by private parties.

It has argued[140] that the term "jurisdiction" as used in human rights treaties should be understood differently from its use in public international law. Most analysis of the extraterritorial applicability of human rights law has focused on cases involving armed conflict or military occupation, in the context of which the main concern has been to avoid a narrow, territorial interpretation of jurisdiction, in order to avoid leaving individuals caught in life-and-death situations without any legal protection.

Many situations involving data processing on the Internet deal not just with the question of whether any protection applies at all, but with the resolution of conflicts

138 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/13-09-24_International_Law_Resolution_EN.pdf

139 http://www.hcch.net/upload/wop/genaff2010pd13e.pdf

140 Akande D., Heller K., Book Discussion: Marko Milanovic's Extraterritorial Application of Human Rights Treaties, November 30, 2011, http://www.ejiltalk.org/book-discussion/

between different laws. Conflicts confuse individuals about what law applies to the processing of their personal data, waste regulatory resources, and can lead to political tensions. An example is the current disagreement between the EU and the US[141] with regard to what protections should apply to the online data of EU individuals that are processed in the US.

Jurisdictional rules under public international law can play a useful role in allocating regulatory competence between States about online data processing. Resolving conflicts with regard to online data protection will also require international agreement on data protection standards, through work such as the plans to draft a protocol to Article 17 ICCPR.[142] Also the Commission has presented measures that aim to make it easier for businesses and the public sector to access and re-use data coming from different sources, sectors and disciplines in the EU. Together with the initiatives that are already in place, such as the new regulatory framework for the protection of personal data, the GDPR, the proposal on the free flow of non-personal data and the initiatives on boosting connectivity and encouraging high-performance computing, these measures are meant to create a truly European common data space supported by both EU-wide policy measures and targeted research and innovation funding.[143]

Lastly, it is important to underline that right to data protection is not the same as right to privacy. According to CJEU, information that is no longer private will remain subject to data protection rules:

> ... a general derogation from the application of the directive (Data Protection Directive) in respect of published information would largely deprive the directive of its effect. It would be sufficient for the Member States to publish data in order for those data to cease to enjoy the protection afforded by the directive.[144]

Later in Google Spain[145] case and in Schrems case[146] CJEU emphasised that right to privacy and right to data protection are separate and both need to be respected and guaranteed:

---

141 https://edri.org/files/holder.pdf - European Digital Rights (EDRi) is an association of civil and human rights organisations from across Europe.

142 Extraterritoriality and the Fundamental Right to Data Protection, http://www.ejiltalk.org/extraterritoriality-and-the-fundamental-right-to-data-protection/

143 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. Towards a common European data space. Brussels, 25.4.2018 COM(2018) 232 final, https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-232-F1-EN-MAIN-PART-1.PDF

144 Case C-73/07, Satakunnan Markkinapörssi and Satamedia, [2008] ECR I9831, para 48

145 Case C-131/12, Gonzalez v Google Spain and Google

146 Case C-361/14, Schrems

> The importance of both the fundamental right to respect for private life, guaranteed by Article 7 of the Charter, and the fundamental right to the protection of personal data, guaranteed by Article 8 thereof, is, moreover, emphasised in the case law of the Court ...[147]

In Google Spain case the CJEU added that Directive 95/46 could not be interpreted restrictively in the light of its objective:

... of ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data ...[148]

No matter how effective the role of the EU legislator is in clarifying the concept and pushing for the approximation of minimum data protection standards, and despite the potential unpredictability it can generate, the role of the courts will remain crucial in concrete cases to ensure conflicting rights are each adequately protected.[149]

2.3.1. Introduction to European Union legislation

The first legal instrument that can be related to data protection dates back to 1948, the United Nations Universal Declaration of Human Rights ('UDHR'), which mentions the right to privacy (family, home and correspondence). It was followed by the European Convention on Human Rights ('ECHR'), in 1950, which gave legal effect to some of the rights mentioned in the UDHR and made them binding to the signatory states. Article 8 ECHR established the right to privacy and family life, mentioning, specifically, the prohibition of interference by public authorities (with some exceptions). All EU Member States are part of the ECHR, thus, any breach can be taken to the European Court of Human Rights ('ECtHR').[150] The Lisbon Treaty provides that the EU should access the ECHR, which would allow individuals to challenge EU acts before the ECtHR (although this is not in place, yet).[151]

The Council of Europe Convention 108 was the first, and still only, legally binding international instrument concerning data protection specifically. It was signed by all EU Member States and it applies to private and public entities that process data. Its objective was the protection against abuses, for that effect it provides special

147 Case C-361/14, Schrems, para 37

148 Case C-131/12, Gonzalez v Google Spain and Google, para 53

149 Eliantonio M., Galli F., Schaper M.,A Balanced Data Protection in the EU: Conflicts and Possible Solutions: Editorial, Maastricht Journal of European and Comparative Law 2016, https://www.academia.edu/27525378/A_Balanced_Data_Protection_in_the_EU_Conflicts_and_Possible_Solutions_Editorial?email_work_car, p. 403.

150 The Court was set on 1959 and since 1998 it is possible for individuals to launch a complaint directly

151 Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community [2007] OJ C 326, article 6(2).

provisions on the processing of sensitive data (such as race, politics, sexual life, etc.). Furthermore, it establishes the individuals' right to know what personal information is stored and it imposes some restriction on data flow between States.[152]

In October 1995, the first EU Directive 95/46/EC[153] concerning data protection was passed and it came into force in October 1998. Greatly influenced by the Convention 108, it viewed data protection as a part of the human right to privacy. The main objective was the harmonization of data protection in the Member States, since 21[154] countries already had national legislation, implementing Convention 108.[155]

The Directive served both economic and rights-based objectives, with the two being linked in an indissociable way. These dual objectives also underpin the Regulation, which seeks to further align national data protection regimes while strengthening the protection conferred upon individuals. However, this approach, or the connection between economic and fundamental rights leads to a question if the recognition of data protection as a fundamental right in EU, limits the regulatory tools available in the data protection context. Directive had two main objectives: to facilitate the free flow of personal data between EU Member States and to ensure the protection of fundamental rights, privacy in particular.[156]

The two main requirements were the protection of privacy and the prohibition to restrict the flow of data from one Member State to the other.

Regarding first requirement, there were a number of conditions for public and private parties to process data[157] including a general prohibition to the processing of sensitive data[158], obligation to inform the data subject on the identity of the data controller and the purpose of the collection under penalty of being considered unlawfully collected. Also, it requires Member States to create an independent authority that ensures compliance with the law. Moreover, it establishes a prohibition to transfer data to third countries that do not have an appropriate data protection in place.[159]

---

152 Fact Sheets on the European Union, Personal data protection, https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection

153 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.

154 Austria, Belgium, Cyprus, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Luxemburg, Netherlands, Norway, Portugal, Slovenia, Spain, Sweden, Turkey, United Kingdom - https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures

155 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28/01/1981, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

156 Lynskey O., The Foundation of EU Data Protection Law, Oxford 2015, p 8-9.

157 Directive 95/46/EC, article 7

158 Ibid, article 8.

159 Ibid, article 25 and 26.

The 1995 Directive was addressed only to the Member States. For that reason, it was necessary to ensure that data protection rights were respected by EU institutions. In order to accomplish that, the Regulation 45/2001[160] created the European Data Protection Supervisor ('EDPS')[161], whose task is to advise on policies and new legislation and also cooperate with similar authorities in the Member States and third countries.

In 2000 the Charter of Fundamental Rights of the European Union ('CFREU') was proclaimed but it only gained the same legal value as the treaties with the Lisbon Treaty in 2009[162]. The CFREU protects the right to privacy and family life, in article 7. Nonetheless, article 8 enshrines the right to protection of personal data as a different right. This distinction recognizes the importance of data protection, already at that time.[163]

The European Union is based on the respect for fundamental rights. Article 8 of the Charter of Fundamental Rights of the European Union expressly recognizes the fundamental right to the protection of personal data.

In order to remove potential obstacles to the flows of Personal Data and to ensure a high level of protection within the EU, data protection legislation has been harmonized.

The Commission also engages in dialogue with non-EU/EEA countries so as to achieve a high level of protection of individuals when exporting personal data to those countries. It also initiates studies on the development at European and international level on the state of data protection and negotiates international agreements to safeguard the rights of individuals where their personal data are transferred (shared) to (with) third countries for law enforcement purposes, such as the fight against terrorism and serious crime.

The issue of data protection in the EEA was addressed in 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. The Directive was incorporated into the EEA Agreement in 1999. The time limit within which the EFTA States were to have the Directive implemented into national law was 1 July 2000. The Data Protection Directive was complemented by the sector-specific Directive 97/66/EC of the European Parliament and the Council of 15 December 1997

160 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 [2000] OJ L 8/1.

161 https://edps.europa.eu/

162 Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community [2007] OJ C 326, article 6(1).

163 Handbook on European data protection law. 2018 edition, https://publications.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1

concerning the processing of the personal data and the protection of privacy in the telecommunications sector.

The aim of the Data Protection Directive was twofold:

- To ensure a minimum level of protection of individuals' right to privacy with regard to the processing of personal data.
- To provide for free movement of such data within the EEA, bearing in mind the 'adequate level of protection' as defined by the Directive.

The main provisions of the Data Protection Directive concerned the criteria for the lawful processing of personal data. "Processing" was defined in this context as virtually any handling or manipulation of information relating to a specific person. Processing of personal data was allowed, inter alia, where the data subject has given their consent, where processing is necessary for the performance of a contract to which the data subject is a party, and when the processing is necessary for the purposes of legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed.

The processing of confidential data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life, was generally prohibited, except when in accordance with the special requirements referred to in the Directive.

The Data Protection Directive also regulated the individual's right to information about the processing of their personal data.

Beyond the mere right to information as to whether, there is relevant personal data processed, individuals are entitled to have access to such data and to require that information which does not comply with the Directive is rectified, blocked, or erased. An individual may also, in certain cases, object to the processing of data about him.

Provisions in the Directive also regulated the quality of personal data and the confidentiality and security of its processing.

According to the Data Protection Directive, each EEA State shall provide that one or more public authorities are responsible for ensuring that the obligations under the Data Protection Directive are complied with. These authorities have to be wholly independent.

Data protection is also the responsibility of companies and they need to adhere to EU standards. Data of EU citizens is apparently being transferred to third parties, such as the US authorities, without informing the citizens concerned. Companies need to be forced to only transmit European data to third parties outside the EU after fulfilling very strict requirements.

After all, Europe is considered to be the one of the world's largest economies giving it substantial financial clout.[164] EU data protection standards need to be observed

164 https://unstats.un.org/unsd/snaama/Index

outside the EU. Where necessary, market access of certain companies needs to be restricted if they fail to comply.

Regulators' attention in the EU has been focused on protecting broad individual rights as they relate to big-data issues such as data processing, data flows and the use of personal information. They also set normative standards such as the emphasis on "fair" and "legitimate" processing of data.

The role of individual control became more central to data-protection discussions in the EU after a 2012 recommendation from the Article 29 Working Party.[165]

The Article 29 Working Party[166] was composed of a representative of the supervisory authorities designated by each EU country, a representative of the authorities established for the EU institutions, and a representative of the European Commission. The Working Party's recommendation called for an increased emphasis on individual control while also advocating for broad-scope enforcement. Specific reforms recommended included:

1) increasing transparency by clarifying the data-minimization principle;
2) reinforcing a comprehensive scheme of responsibilities and liabilities for the controller – that is, the entity "determining the purposes and means of the processing of personal data"[167];
3) requiring controllers and processors to implement a number of policies as well as technical and organizational measures to ensure data security;
4) requiring notification of the supervisory authority within 24 hours in the case of a personal-data security breach;
5) requiring that data subjects be notified if a breach could adversely affect individuals' privacy or personal data; and
6) imposing an obligation for controllers and processors to maintain documentation on all data-processing operations under their responsibility.[168] Under each of these provisions, FIP based individual-empowerment requirements are matched with liability for controllers of data.

---

165 Article 29 Data Protection Working Party. Opinion 05/2012 on Cloud Computing. May 2012. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

166 The Article 29 Working Party (Art. 29 WP) was the independent European working party that dealt with issues relating to the protection of privacy and personal data until 25 May 2018 (entry into application of the GDPR). All archived news on (Art. 29 WP) can be consulted here: https://ec.europa.eu/newsroom/article29/news-overview.cfm

167 Article 29 Data Protection Working Party. Opinion 1/2010 on the concepts of "controller" and "processor". Article 21 Data Protection Working Party. February 2010. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

168 Article 29 Data Protection Working Party, Opinion 01/2012 on the Data Protection Reform Proposals, 00530/12/EN, WP 191 (Mar. 23, 2012). http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf. See Online Privacy Law: European Union, Library of Congress (May 2014). www.loc.gov/law/help/online-privacy-law/eu.php

2.3.2. Data Protection Reform

Data Protection Directive was greatly out of date in a world where information technology plays a prominent role in all fields of life, thus leading to an increased flow of personal data. This increased flow is coupled with revelations of large-scale surveillance of unsuspicious individuals by law enforcement authorities for security purposes and with extensive monitoring of consumer behaviour by private companies for commercial purposes. The processing of personal data has become pervasive in society. Thus, at present, the challenges of new technologies and globalization have increased enormously and require new solutions for a more effective data protection framework.

Secondly, the legal nature of the Data Protection Directive necessarily resulted in generally formulated concepts and open standards, leaving broad discretion to the Member States regarding the actual implementation process. As a consequence, the instrument led to greater consistency between Member States' data protection provisions, but certainly not to fully consistent solutions in scope and definitions of national provisions, and sometimes resulted in very different versions of the same principles.[169] The lack of consistency in data protection throughout the EU could on the one side hamper the development of the internal market in a range of areas (including free movement of persons and services) where the processing of personal data plays an increasingly important role.

Thirdly, the institutional reform brought by the Lisbon Treaty has placed particular emphasis on the protection of personal data, with a separate right enshrined in Article 8 of the Charter and a new horizontal legal basis, Article 16 TFEU. Whereas the existing Data Protection Directive, in light of the internal market legal basis on which it was adopted, addresses the approximation of national provisions in the private sector most importantly, and only touches on the public sector, the new legal basis provides for a comprehensive protection for all policy areas, including both the internal market and law enforcement.[170]

A reform of data protection rules was announced by the European Commission in January 2012 and official texts, of both, the Regulation 2016/679 and Directive 2016/680[171] were published in the EU Official Journal in 4th May 2016. Both

169 Report from the Commission – First Report on the implementation of the Data Protection Directive (95/46/EC), COM/2003/0265 final.

170 Eliantonio M., Galli F., Schaper M.,A Balanced Data Protection in the EU: Conflicts and Possible Solutions: Editorial, Maastricht Journal of European and Comparative Law 2016, https://www.academia.edu/27525378/A_Balanced_Data_Protection_in_the_EU_Conflicts_and_Possible_Solutions_Editorial?email_work_car, p. 398-399

171 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 on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016].

entered into force in May 2016 but became applicable by May 2018 - the Directive had to be transposed into national laws by 6th of May 2018. Old Data Protection Directive was seen as outdated, and the reform was part of European Commission President Juncker's Digital Single Market Strategy.[172]

Importance of data protection and the new data protection regulation is hard to exaggerate - at stake are the future rules for online privacy, data mining, big data, targeted advertising, data-driven social science, governmental spying, and a thousand other activities that are at the heart of many of the internet's largest companies. That even leads to massive actions of lobbyists. Thousands of amendments and proposals were on the table – some good, some bad, and just making sense of them is a full-time job.

The GDPR changes the data protection law at points that are truly crucial for businesses. These changes have impact on the work of many divisions such as IT, Human Resources, Compliance, Revision, Law and Marketing, and number of other. Today any company has to obey all new rules in its daily operations. What is more, the Regulation cannot be overridden by national data protection laws that contradict the GDPR. It is hard to assess for how long legal situation will be confusing for companies as contradicting law may remain in force but is not applicable. Every contradictory law must be revised and clarified to explain which national laws remain relevant.[173]

The EU is being lobbied like never before, to the point where EU Commissioner Viviane Reding said she had not seen such a heavy lobbying operation.[174] What is more, apparently lobbyist-authored texts were finding its way into MEP's amendments.[175] Companies that initially supported SOPA[176], such as Dell, Intel, and Microsoft[177], had lobbyists in Brussels, along with companies that opposed SOPA, including Google, Facebook, Yahoo, and eBay, according to the EU's Transparency Register[178]. The American Chamber of Commerce to the European Union[179], which

172 Jean-Claude Juncker, President of the European Commission, 'A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change – Political Guidelines for the next European Commission' (Opening Statement in the European Parliament Plenary Session, Strasbourg, 15 July 2014)

173 Rücker D, Kugler T. (eds.), New European General Data Protection Regulation. A Practitioner's Guide. Ensuring Compliant Corporate Practice, Baden-Baden 2018, p. 8.

174 EU Privacy regulations subject to 'unprecedented lobbying', http://www.telegraph.co.uk/technology/news/9070019/EU-Privacy-regulations-subject-to-unprecedented-lobbying.html

175 First SOPA, Now Your Privacy: Facebook, Google Flex Lobbying Muscle in Europe, http://www.motherjones.com/politics/2013/03/google-facebook-sopa-privacy

176 H.R.3261 – Stop Online Piracy Act; House Judiciary Committee; October 26, 2011, http://www.webcitation.org/63oCICqjh

177 Which tech companies back SOPA? Microsoft, Apple, and 27 others, http://thenextweb.com/insider/2011/11/17/which-tech-companies-back-sopa-microsoft-apple-and-27-others/

178 http://europa.eu/transparency-register/

179 American Chamber of Commerce to the European Union, http://ec.europa.eu/transparencyregister/

speaks for American business in Europe, had nine lobbyists. Unfortunately, these businesses most certainly did not want to strengthen consumer privacy.

Putting aside the technical background of the data protection reform here are some of the main problems of the Data Protection Directive that had to be addressed:

- Differences in the way that each EU country (28) implements the law have led to an uneven level of protection for personal data, depending on where an individual lives or buys goods and services.
- Rules also needed to be modernized. They were introduced during era when the Internet was still in its infancy.
- Rapid technological developments and globalization have brought new challenges for data protection. For instance, social media, cloud computing, location-based services.

The new General Data Protection Regulation ('GDPR'), Regulation 2016/679[180], aims at harmonizing data protection in the EU.

Substance wise, the Regulation introduces a definition of personal data, which did not exist before in EU law:

"'*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*".[181]

In this sense, all data that can be traced back to an individual is personal data. There is no need for a name to be associated with it, for example a phone number without reference to a name or a mere IP address is considered personal data.

It introduces new rights for data subjects[182] and enhances the ones existent. The main objective is that data subjects gain back control over the way their personal data is collected and processed.[183] For instance, it establishes the obligation of an 'explicit' consent for the process of sensitive data[184] and 'unambiguous' consent for

public/consultation/displaylobbyist.do?id=5265780509-97

180 Regulation (EU) 2016/679 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 119/1.

181 Ibid, Article 4, sub (1).

182 The Regulation refers to data subject as anyone whose data is collected and processed.

183 Protection Of Personal Data, http://ec.europa.eu/justice/data-protection/

184 Ibid, article 9(2) a).

non-sensitive data.[185] It also regulated the 'right to be forgotten' mainly as introduced by the CJEU in the Google Spain case: individuals can request data processors to erase their data if, for instances, the data is not necessary for the purposes it was collected, the individual objects or withdraws its consent to the processing of such data or the processing is not complying with the regulation.[186]

This regulation transfers the burden of data protection to data controllers and processors[187], such is the case of data security[188], demonstration of the data subject's consent[189] or the implementation of 'data protection by design' and 'data protection by default'.[190] Data protection by design means that the entities processing personal data have to consider its protection, and the compliance with the data protection rules, throughout all the process. Data protection by default refers to direct applicability of data protection rules without being necessary a request by the data subject. For example, imagine signing up for a new social media service on which you can share personal information, life events and other content you may deem relevant. In order to successfully publish your profile only your name and email address are required, yet the new service also automatically publishes your age and location and makes it available to the public rather than just to your connections. This would be a clear breach of the privacy by default principle as more information is disclosed to the public than is necessary to provide you with the service. It is noteworthy that the regulation specifically identifies and prohibits services that by default make

185 Ibid, article 4, sub (11).
There can be some degree of discussion as to what the difference really is between the requirement of 'unambiguous' consent and 'explicit' consent. The Commissions' proposal uses the word 'explicit' consent for both sensitive and non-sensitive data. However, the final version of the text does make a distinction between the two, which shows that they are not exactly the same.
European Commission, '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)' (2012), p. 7, chapter 3.4.1.
It can be argued that the 'unambiguous' consent can lead to an implied consent, where the data subject does not say "Yes, I agree" but shows it with his actions. Nevertheless, it is agreed that both have to consist in an affirmative action by the data subject, as pointed out by Peter Hustinx, European Data Protection Supervisor between 2004 and 2014: Peter Huxtinx, 'EU Data Protection Law: The Review Of Directive 95/46/EC And The Proposed General Data Protection Regulation', http://www.statewatch.org/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf

186 Regulation (EU) 2016/679, article 17.

187 Ibid Article 4, sub (7): '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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law; article 4, sub (8): 'processor' as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".

188 Ibid, article 5 sub (f).

189 Ibid, article 7(1).

190 Ibid, article 25.

personal information accessible to an indefinite number of individuals. This is a significant step in ensuring privacy on social media platforms and it is of particular importance to younger users.[191] They are also obliged to notify data subjects[192] and the supervisory authority[193] in the event of a data protection breach, whenever there is a high risk for the data subject's rights.

Both data controllers and processors must designate a Data Protection Officer ('DPO')[194], whenever their activity involves "regular and systematic monitoring of data subjects on a large scale" or the processing of sensitive personal data.[195]

The public supervisory authorities (national data protection authorities)[196], will have to be completely independent bodies. Their enforcement powers will also be enhanced, namely with the ability to charge of fines that can go up to €10-20 million or 2% to 4% of the total worldwide annual turnover, depending on the type of infringement.[197] The value that will be possible to charge is comparable to the fines that competition law authorities can impose.

The Regulation also introduces a new EU body, the European Data Protection Board[198], whose goal is the consistent application of the Regulation[199]. It will not have enforcement powers, which remains within the competence of data protection national authorities.

Concerning the Regulations' territorial applicability, it is applicable to all undertakings that sell goods/services or that monitor data subjects behaviour in the EU "regardless of whether the processing takes place in the Union or not".[200] The transfer of data to third countries can only take place if those countries have "an adequate level of protection".[201] Such assessment should be carried by the Commission, which it will also monitor the third country's data protection development.[202]

Regarding this transfer of data, an agreement was signed between the EU, US and Switzerland that aims at the creation of a level playing field in data protection

191 EU Data Protection Regulation. EU Data Protection Legislation, http://www.eudataprotectionregulation.com/data-protection-design-by-default
192 Regulation (EU) 2016/679, article 34.
193 Ibid, article 33.
194 Ibid, article 37. DPO's tasks is to ensure the applicability of the Regulation, the specific tasks can be found in article 39 and 40.
195 Ibid, article 37(1)(b).
196 Ibid, article 51-62.
197 Ibid, article 83(4) and (5).
198 Ibid, article 68-76.
199 Ibid, article 70(1).
200 Ibid, article 3(2).
201 Ibid, article 45(1).
202 Ibid, article 45(2) and (3).

between these countries.[203] In short, this is a voluntary program, only the companies wishing to apply are subject to the rules it establishes. Once they do, if they breach their commitments they may face sanctions and be removed from the list.[204] Additionally, whenever citizens consider that their data privacy is being violated under this mechanism, it is possible to solve the dispute through an alternative dispute resolution free of charge (if the company fails to solve the problem).[205] In addition, citizens can reach their Data Protection Authorities, "who will work with the Federal Trade Commission to ensure that complaints by EU citizens are investigated and resolved."[206]

The regulation updates and modernize the principles enshrined in the 1995 Data Protection Directive to guarantee the right of personal data protection in the future. They focus is on:

- Reinforcing individuals ′ rights
- Strengthening the EU internal market;
- Ensuring a high level of data protection in all areas, including police and criminal justice cooperation;
- Ensuring proper enforcement of the rules; and
- Setting global data-protection standards.

More changes after the reform described in Appendix 1.

2..3.3. International reaction to the reform

The reform of EU data protection rules is of particular interest to countries like the United States, whose companies may have to abide by stricter provisions to do business in Europe. Some of the provisions raised many objections by the most business-minded at the time commissioners, including Neelie Kroes (Digital Agenda) and Karel de Gucht (Trade).[207]

---

203 Privacy Shield Program Overview, Privacy Shield, Privacyshield.gov, 2017, https://www.privacyshield.gov/Program-Overview
This is a mechanism aiming to replace US-EU Safe Harbour Framework that the CJEU ruled invalid in 2015. Case C-362/14 Schrems [2015] Court of Justice of the European Union, ECLI:EU:C:2015:650.

204 The list comprises the companies that have submitted to comply with the privacy requirements. Once a company is accepted there is no longer need for a requirement prior data transfers from the EU to the US or that requirement is automatically approved. 'Benefits Of Participation | Privacy Shield' (Privacyshield.gov, 2017), https://www.privacyshield.gov/article?id=Benefits-of-Participation

205 European Commission, 'European Commission Launches EU-U.S. Privacy Shield: Stronger Protection For Transatlantic Data Flows' (2016), http://europa.eu/rapid/press-release_IP-16-2461_en.htm

206 Ibid.

207 Guarascio F., US lobbying waters down EU data protection reform, February 2012, https://www.euractiv.com/section/digital/news/us-lobbying-waters-down-eu-data-protection-reform/

Many lobbies tried to soften the rules concerning:

- The newly introduced 'right to be forgotten,' enabling users to delete personal information that they no longer want to share with banks, online booking websites or social media.
- They also put their finger on the obligation to provide notification of data breaches and to obtain explicit consent to use personal data, as well as provisions related to the transfer of personal information to third countries.

Foreign countries got involved in the negotiations at an unusually early stage. For example, the United States was particularly active in trying to amend the draft, at the time, legislation to protect the interest of US companies operating in the EU, partly on security grounds.

An informal paper[208] of the US Commerce Department shows a number of concerns raised by Washington during the EU negotiations. The US complained about the negative impact of the proposed rules, which they said would affect consumer protection, public security cooperation and even human rights. The lobbying was successful since eventually the final text issued by the Commission took on board many of the concerns raised by Washington.

The text eventually proposed by the Commission provided strong data protection guarantees with respect to international data transfers, whilst giving some flexibility to address the specific context of the law enforcement area. For quite long there was a hope that existing EU-US deals will not be challenged by the new proposals. Today we know that Safe Harbour agreement became victim of the changes in EU.

Since personal information is mainly exchanged online through the worldwide web, the best solution should be to decide common rules at global level. But it is not what is happening, as each country moves on its own to regulate the sector. Despite the intense lobbying against the EU's legislation, the US is also planning an overhaul of data protection rules, but the touch will be much softer in a country where business interests are more prominent, and citizens' awareness of personal data is much lower than in Europe.[209]

India and China have also been moving towards stricter regimes for those who deal with private data.[210] However, at this point India has no specific legislation on privacy and data protection. Instead, India's data privacy legislation is made up of several different laws and acts[211], but is currently in the midst of drafting one single,

208 https://edri.org/files/US_lobbying16012012_0000.pdf

209 More in Chapter 2.4.3.

210 Guarascio F., US lobbying waters down EU data protection reform, February 2012, https://www.euractiv.com/section/digital/news/us-lobbying-waters-down-eu-data-protection-reform/

211 Information Technology Act (No. 21 of 2000) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (Privacy Rules 2011) contain specific provisions to protect personal data and other data privacy requirements.

comprehensive piece of legislation for data privacy, titled the Indian Personal Data Protection Bill 2018. In China, the Standardization Administration of China unveiled the final version of a new privacy bill in January 2018 and by May 2018 the law was in effect. The new data privacy law, Information Technology – Personal Information Security Specification (GB/T 35273-2017), contains more strenuous requirements than the GDPR.[212]

2.3.4. Brexit and the GDPR

The United Kingdom officially withdrew from the European Union on 31 January 2020 and has entered a Brexit transition period. Based on the Withdrawal Agreement[213] that was ratified by the European Union and the UK, EU law applied in the UK until 31 December 2020. Consequently, during this period the current legal and practical implications with respect to the data protection regime remained as it was prior to Brexit. Accordingly, the General Data Protection Regulation continued to apply in the UK and as a result, currently no additional third country data transfer mechanisms are required. The Withdrawal Agreement provides that, after the end of the transition period, the United Kingdom has to continue applying the EU data protection rules to this stock of personal data, until the Commission has established, by way of a formal, so-called adequacy decision, that the personal data protection regime of the United Kingdom provides data protection safeguards which are essentially equivalent to those in the EU. The formal adequacy decision by the Commission must be preceded by an assessment of the data protection regime applicable in the United Kingdom. In the case where the adequacy decision was annulled or repealed, the United Kingdom shall ensure that data received will be subject to essentially equivalent standard of protection to that under the EU data protection rules.[214]

However, the UK left the transition period at 11pm 31 December 2020. The new EU–UK Trade and Cooperation Agreement now governs the UK's trading and security relationship with the EU. GDPR remains applicable in the UK for a maximum period of six months, at the latest until 1 July 2021. From 1 January 2021, the one-stop-shop mechanism no longer applies to the UK and to the Information Commissioner's Office (ICO). Appropriate alternative transfer mechanisms can

212 Yahnke K., A Practical Guide to Data Privacy Laws by Country. Improve your knowledge of (and compliance with) data protection laws around the world with this introductory guide, November 5, 2018, https://i-sight.com/resources/a-practical-guide-to-data-privacy-laws-by-country/

213 Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community, OJ L 29, 31.1.2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12019W/TXT(02)

214 Notice to stakeholders, Withdrawal of the United Kingdom and EU rules in the field of data protection, Brussels, 6 July 2020, https://ec.europa.eu/info/sites/info/files/brexit_files/info_site/data_protection_en.pdf

be used in order to avoid any potential interruptions to services, i.e., standard contractual clauses (standard data protection clauses adopted by the European Commission or "ad hoc" contractual clauses); binding corporate rules applicable to the European Economic Area (EEA); codes of conduct or certification mechanisms; or legally binding and enforceable instruments between public authorities or bodies. On 19 February 2021, the European Commission launched the procedure for the adoption of two adequacy decisions for transfers of personal data to the United Kingdom, under the GDPR and the Law Enforcement Directive respectively. The publication of the draft decisions is the beginning of a process towards their adoption. This involves obtaining an opinion from the European Data Protection Board and the green light from a committee composed of representatives of the EU Member States. Once this procedure will have been completed, the Commission will adopt the two adequacy decisions.

In the meantime, the UK already has in place a new domestic data privacy law called UK-GDPR that is exactly the same as the EU version and is supported by the older Data Protection Act of 2018.

2.3.5. US legislation

In the United States of America, there is no single, uniform legislation for the protection of personal data. Rather, protection is covered under federal and state legislations aimed at specific sectors with specific goals – consumer protection, electronic communications, and health information privacy, for e.g. Thus, the type of information protected depends on the provisions of each statute.[215]

American privacy laws are sector-specific, meaning they use the context of how and where the data is moving to define relevant legal parameters. Some privacy laws in the United States have been instituted as a reaction to current events, such as the Video Privacy Protection Act of 1998, which was enacted after contentious confirmation hearings for Supreme Court nominee Robert Bork. Others originated in states such as California and Texas, which have consistently legislated on an array of privacy laws, recently producing provisions on social media in schools and the confidentiality of personal information in mobile health apps.[216]

Many key US privacy laws draw upon concepts of individual control to regulate data collection. The Children's Online Privacy Protection Act (COPPA) and the Privacy Act are two examples of laws that require disclosure of data practices (notice) and give consumers the right to access and correct personal data

215 Thoren-Peden D.S, Meyer C.D., Data Protection 2018: USA, June 26, 2018, https://www.pillsburylaw.com/en/news-and-insights/data-protection-2018-usa.html

216 De Mooy M., Rethinking Privacy Self-Management and Data Sovereignty in the Age of Big Data. Considerations for Future Policy Regimes in the United States and the European Union, 2017, https://cdt.org/files/2017/04/Rethinking-Privacy_2017_final.pdf, p. 11.

(redress).[217] But these laws offer only partial protection for personal information, and are often inconsistent in applying important components of the FIPs; for example, COPPA restricts data practices only for operators of websites and online services aimed at children under the age of 13.[218]

The sector-based system in the United States is supplemented by guidelines issued by government agencies and industry organizations that function as best practices on data protection. While the law does not require these guidelines to be implemented, they create a unique self-regulatory framework that includes accountability and enforcement components and are increasingly being used as a tool for enforcement by regulators such as the FTC.[219] The FTC is the U.S. consumer-protection agency responsible for policing privacy, and acts as a counter to the lack of comprehensive data-security and privacy laws in the country. However, the FTC has limited authority under Section 5 of the FTC Act, and must rely on an "unfair or deceptive" standard when it investigates commercial data practices. The agency's interpretation of this standard has centered on the company's intent to knowingly deceive or otherwise defraud customers, a focus that has led to strong emphasis on the issues of notice, choice and informed consent.[220]

The only US act that from a European point of view can be taken as general is The Privacy Act of 1974, 5 U.S.C. § 552a. The main points include that it:

- establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.
- requires that agencies give the public notice of their systems of records by publication in the Federal Register.
- prohibits the disclosure of a record about an individual from a system of records absent the written consent of the individual, unless the disclosure is pursuant to one of twelve statutory exceptions.
- provides individuals with a means by which to seek access to and amendment of their records and sets forth various agency record-keeping requirements.

217 Other FIP-style (Fair Information Practices) privacy laws in the U.S. include: the Privacy Act of 1974, the Family Educational Rights and Privacy Act of 1974, the Right to Financial Privacy Act of 1978, the Cable Communications Policy Act of 1984, the Electronic Communications Privacy Act of 1986, the Employee Polygraph Protection Act of 1988, the Video Privacy Protection Act of 1988, the Telephone Consumer Protection Act of 1991, the Driver's Privacy Protection Act of 1994, the Children's Online Privacy Protection Act of 1998, the CAN-SPAM Act of 2003, and the Fair and Accurate Credit Transaction Act of 2003.

218 Federal Trade Commission Summary of Rule 16 CFR Part 312 COPPA: www.ftc.gov/enforcement/rules/rulemaking-regulatory-reformproceedings/childrens-online-privacy-protection-rule

219 Thomson Reuters Practical Law. Data Protection in the United States. July 1, 2015. http://us.practicallaw.com/6-502-0467

220 De Mooy M., Rethinking Privacy Self-Management and Data Sovereignty in the Age of Big Data. Considerations for Future Policy Regimes in the United States and the European Union, 2017, https://cdt.org/files/2017/04/Rethinking-Privacy_2017_final.pdf, p. 13.

Otherwise, US legislation has no general privacy law, nothing in Constitution[221], as well as no legislation following OECD & EC principles. On the other hand, there is a huge number of privacy-related acts:

1. Americans with Disabilities Act (ADA)
2. Cable Communications Policy Act of 1984 (Cable Act)
3. California Senate Bill 1386 (SB 1386)
4. Children's Internet Protection Act of 2001 (CIPA)
5. Children's Online Privacy Protection Act of 1998 (COPPA)
6. Communications Assistance for Law Enforcement Act of 1994 (CALEA)
7. Computer Fraud and Abuse Act of 1986 (CFAA)
8. Computer Security Act of 1987 - (Superseded by the Federal Information Security Management Act (FISMA)
9. Consumer Credit Reporting Reform Act of 1996 (CCRRA) - Modifies the Fair Credit Reporting Act (FCRA).
10. Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003
11. Electronic Funds Transfer Act (EFTA)
12. Fair and Accurate Credit Transactions Act (FACTA) of 2003
13. Fair Credit Reporting Act
14. Federal Information Security Management Act (FISMA)
15. Federal Trade Commission Act (FTCA)
16. Driver's Privacy Protection Act of 1994
17. Electronic Communications Privacy Act of 1986 (ECPA)
18. Electronic Freedom of Information Act of 1996 (E-FOIA)
19. Fair Credit Reporting Act of 1999 (FCRA)
20. Family Education Rights and Privacy Act of 1974 (FERPA; also known as the Buckley Amendment)
21. Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLBA)
22. Privacy Act of 1974 - including U.S. Department of Justice Overview
23. Privacy Protection Act of 1980 (PPA
24. Right to Financial Privacy Act of 1978 (RFPA)
25. Telecommunications Act of 1996
26. Telephone Consumer Protection Act of 1991 (TCPA
27. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)
28. Video Privacy Protection Act of 1988[222]

221 Later I explain that by very broad interpretation some very general rules can be found in the US Constitution.

222 http://www.informationshield.com/usprivacylaws.html

Huge number of detailed oriented legislation causes American privacy legislation to be fragmented and confusing. Therefore, it is nothing like European law, which is much more uniform, with common and general rules.

Mentioning other examples, the White House is working with bipartisan sponsors on a bill to protect data collected from students through educational apps. Former president Barack Obama has pushed to do more to protect privacy in an age when consumers leave a trail of digital footprints through smart phones, personal devices, and social media - information that can be collected, analysed and sold.

Protecting America's children from Big Data should not be a partisan issue according to Indiana Congressman Luke Messer, the chairman of the House of Representatives Republican Policy Committee. Congress is trying to find the appropriate balance between technology in the classroom and a parent's right to protect their child's privacy. The lawmakers have long worked on the issue with privacy advocates and more than 100 companies including Microsoft, Google and News Corp subsidiary Amplify to develop a privacy pledge to prevent misuse of data collected in classrooms.

After Edward Snowden leaked classified information about government use of Big Data analytics for surveillance Obama proposed a new national standard to require companies to tell consumers within 30 days from the discovery of a data breach that their personal information had been compromised.

Another example is the update to the outdated Electronic Communications Privacy Act (ECPA)[223] to protect email and other data stored in the cloud. The Email Privacy Act[224], to amend ECPA, is the bill introduced in the United States Congress. It passed the House of Representatives on a voice vote on February 6, 2017, but never made it out of Senate committee.[225]

Big Data techniques have accelerated price discrimination, raising concerns about fairness, particularly when consumers do not control their own data or understand how companies are using it.[226]

As it was getting closer to finalising draft reports on reforming EU data protection legislation, there were opinions from US that Europe should overcome its misconceptions and stereotypes to find regulatory convergence with the US to pave the way for an interoperable transatlantic data-privacy system. According to

223 Electronic Communications Privacy Act of 1986 (ECPA), An Act to amend title 18, United States Code, with respect to the interception of certain communications, other forms of surveillance, and for other purposes, https://www.govinfo.gov/content/pkg/STATUTE-100/pdf/STATUTE-100-Pg1848.pdf

224 H.R.387 - Email Privacy Act

225 Summary: H.R.387 — 115th Congress (2017-2018), https://www.congress.gov/bill/115th-congress/house-bill/387

226 Obama finds bipartisan support for first 'Big Data' privacy plan, http://www.reuters.com/article/2015/02/05/us-usa-privacy-exclusive-idUSKBN0L90D320150205?feedType=RSS&feedName=technologyNews

US commentators the transatlantic privacy discussion is too often side-tracked by misconceptions about the US legal system – myths that obscure US fundamental commitment to privacy and the extensive legal protections US provide to data. Americans stand on the side that there is the pretentious attitude that the European Union does a better job at protecting data than the United States.[227]

The EU and the US share similarities in their approaches to personal data protection, but there are also differences that have made negotiating agreements on data transfers particularly difficult – like SWIFT (on personal and commercial financial transactions) and passenger name recognition (PNR). But these are only the brightest examples. Same differences can be found when the discussion reaches anything connected to biggest US companies.

The United State, like the EU, was in 2012 in the process of reforming parts of its data privacy framework. President Barack Obama released his Privacy Blueprint. But there is always a risk that reforms on both sides of the Atlantic settle on some rules that will hamper interoperability.[228]

Additionally, the United States, which relies on a system of enforceable codes of conduct, complains that there is no mention in the possibility to use codes of conduct and certification schemes as a basis for cross-border transfers. Removing protection gaps and discrepancies between the EU-US legal systems and thereby improving legal certainty must be at the core of the transatlantic dialogue on the issue.[229]

The US authorities should not be allowed to demand data from companies headquartered in the EU, and the Commission should be supporting that position. However, even within the EU, security services enjoy broad powers to access personal data.[230]

US do not have an omnibus privacy legislation at the federal level. US don't have a statute that recognizes generally that privacy is a right that's secured by federal law. And that puts US at the opposite end of the spectrum from some for example European Union. It's not that living in the US means that your privacy is not

227 Vincenti D., EU urged to choose transatlantic convergence on data protection, December 2012, https://www.euractiv.com/section/digital/news/eu-urged-to-choose-transatlantic-convergence-on-data-protection/

228 The White House - Office of the Press Secretary, We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online. Internet Advertising Networks Announces Commitment to "Do-Not-Track" Technology to Allow Consumers to Control Online Tracking, February 2012, https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights

229 Vincenti D., EU urged to choose transatlantic convergence on data protection, December 2012, https://www.euractiv.com/section/digital/news/eu-urged-to-choose-transatlantic-convergence-on-data-protection/

230 EU lawmaker warns of data protection rules delay till 2016, http://www.euractiv.com/sections/infosociety/eu-lawmaker-warns-data-protection-rules-delay-till-2016-311100

protected from dominant ICT companies. The FTC has a modicum of authority and has used it when companies grossly overreach — as it did against Facebook in 2011.[231]

2.4. Privacy

Privacy is subjective, contextual, and therefore hard to evaluate. In this regard, one of the main challenges that researchers are currently exploring is linked with the analysis of individual attitudes on privacy. For instance, research has shown that most users of websites with customizable privacy settings, such as Online Social Networks (OSNs), maintain the default permissive settings, which may lead to unwanted privacy outcomes.[232] The explanation to this behaviour is not necessarily that users do not care about their privacy. Instead, existing studies demonstrate an ambivalence of the users' attitudes towards privacy.[233]

Privacy as a concept has a larger function in society. What are the effects on our democratic societies of massive-scale data collection, trend prediction and individual targeting? Are people forced into higher conformance? Is conformance pressure affecting the building of political opinions?[234]

Privacy allows us to be who we are. It offers us the freedom to think and act without being afraid of repercussions. Privacy allows us to be who we are. When we choose to tell people things about ourselves, we are in control of who we would like to be to the outside world. It is up to us to decide what info to keep to ourselves and what to share.

Also, privacy offers us the freedom to think and act without being afraid of repercussions. We want to be able to join an event, for example, without having to answer to an authority afterwards why we were there in the first place. We need to be able to be anonymous at times.

---

231 Barret B., WHAT WOULD REGULATING FACEBOOK LOOK LIKE?, March 2018, https://www.wired.com/story/what-would-regulating-facebook-look-like/?CNDID=24507553&mbid=nl_032218_daily_list1_p4, PRESS RELEASE: Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises, November 29, 2011, https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep

232 Krishnamurthy B., Wills C. E., Characterizing privacy in online social networks, [in:] Proceedings of the 1st Workshop on Online Social Networks (WOSN '08), 2008, pages 37–42

233 Turow J., Hoofnagle C. J., Mulligan D. K., Good N., Grossklags J., The federal trade commission and consumer privacy in the coming decade, I/S: A Journal of Law & Policy for the Information Society, (723), 2007–08.

234 Fischer-Hu¨bner S., Hoofnagle Ch. J., Krontiris I., Rannenberg K., Waidner M., Online Privacy: Towards Informational Self-Determination on the Internet (August 29, 2011). Dagstuhl Manifestos, Vol. 1, Issue 1, 2011, http://drops.dagstuhl.de/opus/volltexte/2011/3205/pdf/dagman_v001_i001_p001_11061.pdf, p. 6.

Lastly, good privacy rules and regulations ensure our safety. We need governments and enterprises to be transparent about the data they keep, use and share. Only then can we trust that our personal information will not be abused.[235]

Online, consumers should be able to use the Internet without their every move being tracked so they become targets of advertising or so corporate decisions about them are made without their knowledge. In the bricks and mortar world, banks and corporations should be required to get your permission before trading or selling private information such as Social Security numbers or account balances.[236]

2.4.1. History

Privacy is a fundamental human right recognized in the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights and in many other international and regional treaties. Privacy underpins human dignity and other key values such as freedom of association and freedom of speech. It has become one of the most important human rights issues of the modern age.

Privacy is at the very soul of being human. Legal rights to privacy appeared 2000 years ago in Jewish laws.

Privacy is the right to autonomy, and it includes the right to be let alone. It includes the right to control information about ourselves, including the right to limit access to that information. Most important, the right to privacy means the right to enjoy solitude, intimacy, and anonymity.

"Right to be let alone" defined as "the most comprehensive of rights, and the right most valued by civilized men."[237] - "Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls "the right to be let alone". Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that" what is whispered in the closet shall be proclaimed from the house-tops". For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; the evil of invasion of privacy by the newspapers..."

Many American legal scholars have written about the privacy and developed the privacy-concept in Common Law. For example, William L. Prosser in his article Privacy (1960).

Prosser criticized the literature, which only focused to evaluate the possible existence of privacy protection in jurisprudence. He preferred analyzing what is the real content of privacy.

---

235 Privacy Matters, http://www.respect-my-privacy.eu/privacy-matters

236 Privacy, http://www.consumerwatchdog.org/focusarea/privacy

237 Warren S. D., Brandeis L. D., The Right to Privacy,1890 Harvard Law Review

Prosser found four different dimensions or intrusion-forms to the privacy under the concept "the right to be let alone ":

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.

One of the most important writers was Alan Westin in his book *Privacy and Freedom* (1967). Westin presented the four basic forms of privacy:

1. In *Solitude-possession* an individual is a part of the group and not under surveillance of other people.
2. *Intimacy-possession* gives an individual right to choose one or several more intimate relationship to other people.
3. *Anonymity* means the possibility for a person to move and take care of his businesses in public places without identification or control.
4. The last possession, *Reserve* means the possibility to build psychological "wall" against unlawful intrusion in cases, where an individual wants to restrict the access of other people to his or her personal information.

When it comes to other scholars, it should be also mentioned for instance Vance Packard, Ruth Gavison, Donald Madgwick, Arthur Miller, Robert Holmes, Raymond Wacks, Richard Posner, Edward Bloustein, Richard Hixon, William H. Parent, David H. Flaherty and Ethan Kash in the Anglo-American world. All these scholars have written about privacy and personal data protection during the last four decades. This tradition is continued by privacy experts such as Daniel Solove[238], Tom Gerety[239] or Fred H. Cate[240].

238 Daniel J. Solove is the John Marshall Harlan Research Professor of Law at the George Washington University Law School. He founded TeachPrivacy, a company providing privacy and data security training. One of the world's leading experts in privacy law.

239 Tom Gerety is Collegiate Professor at New York University and teaches in both the Law School and the College of Arts and Sciences. Mr. Gerety first came to NYU in 2003 to head up the Brennan Center for Justice at the Law School. Before that he served as president of Amherst College from 1994 to 2003 and of Trinity College in Hartford, Connecticut, from 1989 to 1994. From 1986 to 1989 he was the Dean and Nippert Professor at the College of Law of the University of Cincinnati. Received his B.A. from Yale College in 1969 and completed his Ph.d and J.D. at Yale in 1976.

240 Fred H. Cate is the Vice President for Research, Indiana University, Distinguished Professor and C. Ben Dutton Professor of Law, Senior Fellow, Center for Applied Cybersecurity Research. Professor Cate specializes in information privacy and security law issues. He has testified before numerous congressional committees and speaks frequently before professional, industry, and government groups. In addition to his appointment in the Law School and as Vice President for Research, he is an Adjunct Professor of Informatics and Computing at Indiana University. Attended Oxford University and received his J.D. and his A.B. with Honors and Distinction from Stanford University.

The American discussion and studies have affected strongly to the European development of privacy-theories. Of course, the viewpoints might be little bit different in many European countries compared to American Common Law-tradition, where the legislation will be formulated by the court cases and legal praxis.

"(...) the privacy concept is pregnant with definitional variation. Analysis of the literature on privacy reveals four major ways of defining the concept."[241]

1. Privacy viewed essentially in terms of non-interference (Right to be let alone)
2. Privacy in terms of degree of access to a person (Limited accessibility)
3. Privacy in terms of information control (When, what and how information is communicated to others)
4. Privacy related to aspects of persons' lives that are intimate and/or sensitive (As a result not every disclosure of information is a loss of privacy)

Finally, I would like to mention the eleven core areas that closely affect our right to self-determination: physical privacy, spatial privacy, social privacy, media privacy, anonymity, privacy in the processing of personal data, ownership of information, right to be assessed in the proper light, patient privacy, privacy in working life and communication privacy.[242] This is however is not exhaustive and is more of an extensive example as the understanding of privacy evolves with societal and technological changes.

The right to privacy is an internationally recognized right, articulated in Article 17 (1) of the International Covenant on Civil and Political Rights and Article 8 of the European Convention on Human Rights.

The European Court of Human Rights has consistently held[243] that the interception of telephone communications, as well as facsimile and e-mail communications content, are covered by notions of "private life" and "correspondence" and thus constitute an interference with Article 8 (See Malone v United Kingdom (1985) 7 EHRR 14 [64][244]; Weber v Germany (2008) 46 EHRR SE5 at [77][245]; and Kennedy v United Kingdom (2011) 52 EHRR 4 at [118][246]).

European Court has found[247] the interception and/or storage of a communication constitutes the violation, and that the "subsequent use of the stored information has no bearing on that finding", nor does it matter "whether the information gathered

241 Bygrave L., Data Protection Law: Approaching its Rationale, Logic and Limits, page 128-9

242 Saarenpää A., Data Protection in the Network Society. The exceptional becomes the natural, [in:] Galindo F. (ed.), El derecho de la sociedad en red, Zaragoza 2013, p. 100

243 http://hudoc.echr.coe.int/eng?i=001-87207#{"itemid":["001-87207"]}

244 http://hudoc.echr.coe.int/eng?i=001-57533#{"itemid":["001-57533"]}

245 http://hudoc.echr.coe.int/eng?i=001-76586#{"itemid":["001-76586"]}

246 http://hudoc.echr.coe.int/eng?i=001-98473#{"itemid":["001-98473"]}

247 http://hudoc.echr.coe.int/eng?i=001-57519#{"itemid":["001-57519"]} , http://hudoc.echr.coe.int/eng?i=001-58497#{"itemid":["001-58497"]}

on the applicant was sensitive or not or as to whether the applicant had been inconvenienced in any way".

Therefore, the right to privacy, extending as it does to the privacy of communications, is a relatively unique right in the sense that its realization can occur remotely from the physical location of the individual. That is, when an individual sends a letter, email, or a text-message, or makes a phone call, that communication leaves their physical proximity and travels to its destination. In the course of its transmission the communication may pass through multiple other States and, therefore, multiple jurisdictions.

Individuals have a legitimate expectation that their human rights will be respected not only by the State upon whose territory they stand, but by the State within whose territory their rights are exercised. States have interference-based jurisdiction for particular negative human rights obligations when the interference with the right occurs within their territory. The way the global communications infrastructure is built requires that the right to privacy of communications can be exercised globally, and communications can be monitored in a place far from the location of the individual to whom they belong.[248]

Privacy is a sweeping concept, including freedom of thought, control over one's body, solitude in one's home, control over information about oneself, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations. In the discussion, philosophers, legal theorists, and jurists have emphasised the great difficulty in reaching a satisfying conception of privacy.[249] The reason behind it is for example as Arthur Miller has declared that privacy is "difficult to define because it is exasperatingly vague and evanescent."[250] William Beaney has noted, "Even the most strenuous advocate of a right to privacy must confess that there are serious problems of defining the essence and scope of this right."[251] Robert Post stated that "Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all."[252] The consequence of all these is the difficulty in articulating what privacy is and why it is important has often made privacy law ineffective and blind to the larger purposes for which it must serve.

---

248 Interference-Based Jurisdiction Over Violations of the Right to Privacy, http://www.ejiltalk.org/interference-based-jurisdiction-over-violations-of-the-right-to-privacy/

249 Solove Daniel J., Conceptualizing Privacy. California Law Review, Vol. 90, p. 1087, 2002, http://ssrn.com/abstract=313103, p. 1088, after: Gavison R., Privacy and the Limits of Law, 89 Yale L.J. 421, 422 (1980)

250 Miller A. R.,, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 25 (1971).

251 Beaney W. M., The Right to Privacy and American Law, 31 Law & Contemp. Probs. 253, 255 (1966).

252 Post R. C., Three Concepts of Privacy, 89 Geo. L.J. 2087, 2087 (2001).

The extreme difficulty in defining privacy or even in simply answering the question "What is privacy?" lead Solove propose of a new approach for conceptualizing privacy. In this approach, he makes two principal arguments.[253] Firstly, he assumes that certain concepts might not have a single common characteristic, but rather they draw from a common pool of similar elements.[254] Secondly, he propounds a pragmatic[255] approach to conceptualizing privacy. He identifies his approach as "pragmatic" because it emphasizes the contextual and dynamic nature of privacy. This approach diverges from traditional accounts of privacy that seek to conceptualize it in general terms as an overarching category with necessary and sufficient conditions. Solove suggests an approach to conceptualize privacy from particular contexts rather than in the abstract.[256]

Unfortunately, it seems that his idea did not lead him to the conclusion he wanted to reach. Conceptions that attempt to locate the core or essence of privacy are being too broad or too narrow. It does not mean that we must always avoid referring to privacy in the abstract; sometimes it is easiest and most efficient to do so. Rather, such abstract reference to privacy often fails to be useful when we need to conceptualize privacy to solve legal and policy problems. However, Solove points that contextualized approach toward conceptualizing privacy will prove quite fruitful in today's world of rapidly changing technology.[257]

Defining privacy, being able to point it, name it, and answer the question "What privacy is?" in the context of this Dissertation might be very important. I write, "might", because so far, I cannot do that, I have doubts anyone can. The reason it is

253 Solove Daniel J., Conceptualizing Privacy..., p. 1090, 1091.

254 Wittgenstein L., PHILOSOPHICAL INVESTIGATIONS §§ 66-67 (G.E.M. Anscombe trans., 1958).

255 Charles Sanders Peirce, William James, John Dewey, Josiah Royce, George Herbert Mead, and others originally developed pragmatism. For more background about the origins of pragmatism Solove suggests to see Richard Shusterman, Practicing Philosophy: Pragmatism and the Philosophical Life (1997); John J. Stuhr, Genealogical Pragmatism: Philosophy, Experience, and Community (1997); Daniel J. Solove, The Darkest Domain: Deference, Judicial Review, and the Bill of Rights, 84 Iowa L. Rev. 941, 970-71 (1999). A number of prominent contemporary scholars identify themselves as pragmatists, such as Richard Rorty, Judge Richard Posner, Cornell West, Robin West, Daniel Farber, and Thomas Grey. See Richard A. Posner, Overcoming Law (1995); Richard Rorty, Consequences of Pragmatism: Essays, 1977-1980 (1982); Cornell West, Keeping Faith: Philosophy and Race in America (1993); Daniel A. Farber, Legal Pragmatism and the Constitution, 72 Minn. L. Rev. 1331 (1988); Thomas C. Grey, Holmes and Legal Pragmatism, 41 Stan. L. Rev. 787, 814 (1989); Robin West, Liberalism Rediscovered: A Pragmatic Definition of the Liberal Vision, 46 U. Pitt. L. Rev. 673 (1985). For critical views of the "new" legal pragmatism, see David Luban, Legal Modernism 125-78 (1997); Steven D. Smith, The Pursuit of Pragmatism, 100 Yale L.J. 409 (1990); William Weaver, Why Pragmatism? The Puzzling Place of Pragmatism in Critical Theory, 1993 U. Ill. L. Rev. 535. Although many of the contemporary scholars who identify themselves as pragmatists share certain ideas and assumptions, they also have profound differences—sometimes more differences than similarities.

256 Solove Daniel J., Conceptualizing Privacy..., p. 1092.

257 Solove Daniel J., Conceptualizing Privacy..., p. 2001.

important, is how hard it is to protect our privacy and our right to privacy when we do not know what privacy is, and therefore how broad our right is.

However, it is not only about troubles with the definition of privacy. Too often, we hear people claiming they have nothing to hide, that what we reveal in the Internet is not important and will not lead to us back. When discussing whether government surveillance and data mining pose a threat to privacy, many people respond that they have nothing to hide. The argument that no privacy problem exists if a person has nothing to hide is frequently made in connection with many privacy issues. It is connected to both surveillance from the government as well as data collection from major ICT companies. Of course, in some cases, as Snowden revealed, it is the same. Additionally, when the government engages in surveillance, many people believe that there is no threat to privacy unless the government uncovers unlawful activity. Many people contend that a privacy harm exists only if skeletons in the closet are revealed.[258] It is similar with sharing private details in social media. As long as these are not embarrassing, people feel there is no harm in it.

The "nothing to hide" argument and its variants are surprisingly popular in discourse about privacy. Data security expert Bruce Schneier calls it the "most common retort against privacy advocates"[259] and legal scholar Geoffrey Stone refers to it as "all-too-common refrain."[260] Some of the most popular arguments backing up the idea that we have nothing to hide are[261]:

- I do not have anything to hide from the government. I do not think I had that much hidden from the government in the first place. I do not think they care if I talk about my ornery neighbour.[262]
- Do I care if the FBI monitors my phone calls? I have nothing to hide. Neither does 99.99 percent of the population. If the wiretapping stops one of these Sept. 11 incidents, thousands of lives are saved.[263]
- Like I said, I have nothing to hide. The majority of the American people have nothing to hide. And those that have something to hide should be found out and get what they have coming to them.[264]

258 Solove Daniel J., 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. San Diego Law Review, Vol. 44, p. 745, 2007; GWU Law School Public Law Research Paper No. 289. Available at SSRN: http://ssrn.com/abstract=998565, p. 747.

259 Bruce Schneier, Commentary, The Eternal Value of Privacy, WIRED, May 18, 2006, http://www.wired.com/news/columns/1,70886-0.html.

260 Geoffrey R. Stone, Commentary, Freedom and Public Responsibility, CHI. TRIB., May 21, 2006, at 11.

261 Solove Daniel J., 'I've Got Nothing to Hide'..., 749-750.

262 Comment of annegb to Concurring Opinions, http://www.concurringopinions.com/archives/2006/05/is_there_a_good.html#comments (May 23, 2006, 11:37 EST).

263 Joe Schneider, Letter to the Editor, NSA Wiretaps Necessary, ST. PAUL PIONEER PRESS, Aug. 24, 2006, at 11B.

264 Polls Suggest Americans Approve NSA Monitoring (NPR radio broadcast, May 19, 2006), available at 2006 WLNR 22949347.

It seems that people mostly do not realize the consequences of losing privacy, either by revealing private details or by being surveilled.

Economists and adherents tend to be sceptical of privacy because, privacy hides information from the market that the market needs to function efficiently.[265] We are being encouraged to think of privacy as a commodity to be traded. In theory, you can make a market for anything.[266] Privacy, details about us are most definitely not the strangest things to make money on. In addition, we are poor at managing our privacy, and we undervalue it.[267] On every occasion we ae being subtly encouraged into disclosing more information than may be good for us. The question is, should we trade our privacy at all. For example, Anita Allen sees privacy as indispensable to society to the degree that coercing a measure of privacy is justified on various instrumental and normative grounds.[268]

We should not forget about ICT companies. They can and do abuse the power they hold over consumers by knowing so much about them. For example, companies have an incentive to engage in individualized market manipulation whereby each consumer is targeted based on their specific set of biases or approach at a time when they are most vulnerable.[269]

2.4.2. Privacy as a social value

Privacy protection is a social institution, a group of norms, which governs practices involving flows of information and access to individuals.[270]

Besides its value for individuals, privacy also has an irreducibly social value. This perspective has important implications for the way in which conflicts between privacy and other values are interpreted. If it can be argued that the protection of individual privacy serves the interests of society, then the alleged conflict between privacy in terms of individual interest and the interests of society should be reconsidered.[271]

Priscilla Regan, for example, wrote:

I argue that privacy is not only of value to the individual but also to society in

265 Calo R., Privacy and Markets: A Love Story (August 6, 2015). Notre Dame Law Review, Forthcoming; University of Washington School of Law Research Paper No. 2015-26. Available at SSRN: http://ssrn.com/abstract=2640607 or http://dx.doi.org/10.2139/ssrn.2640607, p. 19.

266 MICHAEL J. SANDEL, WHAT MONEY CAN'T BUY: THE MORAL LIMITS OF MARKETS 1-4 (2012)

267 Solove Daniel J., Privacy Self-Management and the Consent Dilemma, 126 HARV. L. REV. 1880, 1883-88 (2013).

268 Allen A., Coercing Privacy, 40 WILLIAM & MARY L. REV. 723 (1999).

269 Calo R., Digital Market Manipulation, 82 GEO. WASH. L. REV. 995 (2014).

270 Minkkinen M., Futures of privacy protection: A framework for creating scenarios of institutional change, Futures, Volume 73, October 2015, https://www.sciencedirect.com/science/article/pii/S00163287, p. 51

271 Roessler B., Mokrosinska D., (2013). Privacy and social interaction. Philosophy & Social Criticism, 39(8), https://doi.org/10.1177/0191453713494968, p. 772

general. Privacy is a common value in that all individuals value some degree of privacy and have some common perceptions about privacy. Privacy is also a public value in that it has value not just to the individual as an individual or to all individuals in common but also to the democratic political system.... Privacy is rapidly becoming a collective value in that technology and market forces are making it hard for anyone person to have privacy without all persons having a similar minimum level of privacy.[272]

Daniel Solove stated that by understanding privacy as shaped by the norms of society, we can better see why privacy should not be understood solely as an individual right. Instead, privacy protects the individual because of the benefits it confers on society. The value of privacy should be understood in terms of its contribution to society.[273] In 1987 Spiros Simitis already described privacy as a constitutive element of a democratic society.[274]

Legislators and participants in the public debate also must take into account the consequences of limiting privacy on social interaction itself, the ways in which relationships would change and therefore the ways in which social practices would be potentially distorted or threatened.[275]

The future of privacy is not determined by any technological or other trend. However, equally importantly, the future of privacy is not purely the product of imagination and visioning. Privacy protection is a social institution with a particular history and dynamics, and it is important to understand these when making statements about possible futures of privacy and when attempting to influence institutional change.[276]

2.5. EU and US approach differences

Views on data protection in the European Union and the United States are very similar, with individuals in all three places expressing a belief that the internet brings value to their lives, while also feeling trepidation regarding the collection and use of their personal information.[277] However, some changes are easily seen.

---

272 Regan Priscilla M. (1995) Legislating Privacy. Chapel Hill, NC: University of North Carolina Press, p. 213

273 Solove Daniel J., Understanding Privacy, Cambridge, MA: Harvard University Press 2008

274 Simitis S., Reviewing Privacy in an Information Society, University of Pennsylvania Law Review 135, 1987

275 Roessler B., Mokrosinska D., Privacy and social interaction. Philosophy & Social Criticism, 39(8), 2013, https://doi.org/10.1177/0191453713494968, p. 785

276 Minkkinen M., Futures of privacy protection: A framework for creating scenarios of institutional change, Futures, Volume 73, October 2015, https://www.sciencedirect.com/science/article/pii/S00163287, p. 58

277 Dutta S., Dutton W. H., Law G., The New Internet World: Perspective on Freedom of Expression, Privacy, Trust and Security, April 2011, http://ssrn.com/abstract=1916005

While the EU Charter of Fundamental Rights states in Article 8(1) that everyone has the right to the protection of his personal data, the US view stringent data protection as a potential threat to innovation and its big ICT companies like Google or Facebook. These companies, the US government and its agencies invest huge amounts of time, effort and money into collecting a wealth of data, that they consider truths, to profile every one of us for commercial and national security purposes.

The US remains less stringent on data protection especially with the Cyber-Security Information Sharing Act (CISA), which makes data transfers between companies and the US government even easier. Therefore, there seems to be a certain level of divergence between the approach to data protection in the EU and US.

Also attitudes on privacy and individual control as captured by surveys of Americans and Europeans reflect cultural narratives. Generally, Americans are more enthusiastic about the notion of an individual being in control of his or her personal information, according to several surveys performed[278] by the Pew Research Center.[279]

The American public has long expressed deep concerns regarding the privacy of their information in automated systems. Already a 1973 report from the Electronic Privacy Information Center noted that Americans' worries and anxieties about computers and personal privacy show up in the replies of about one-third of those interviewed.[280]

Similarly, those from the European Union have indicated a mistrust of large-scale data processing for decades.[281]

Less than a third of European respondents in one survey believed that there were advantages to big data, while less than a quarter thought that companies respected the privacy of users' personal information.[282]

In both the United States and the European Union, individuals have expressed feeling defeated and resigned over their inability to control their personal

278 Rainie L., The State of Privacy in America, Pew Research Center, September 2016, www.pewresearch.org/fact-tank/2016/09/21/thestate-of-privacy-in-america/

279 https://www.pewresearch.org/ - The Pew Research Center is a nonpartisan American think tank based in Washington, D.C. It provides information on social issues, public opinion, and demographic trends shaping the United States and the world.

280 Secretary's Advisory Committee on Automated Personal Data Systems. Records, Computers, and the Rights of Citizens. Dept. of Health, Educ. and Welfare, July 1973, www.epic.org/privacy/hew1973report/

281 Freude A., Freude T., Echoes of History: Understanding German Data Protection, Bertelsmann Foundation Newpolitik, October 2016, https://www.bfna.org/research/echos-of-history-understanding-german-data-protection/

282 Meyer D., Europeans Remain Far from Sold on the Benefits of big data, Fortune, Jan. 18, 2016, http://fortune.com/2016/01/18/europe-data/

information, as well as a strong desire to decide how their information is shared and used.[283]

In a Harvard Business Review survey that included interviews with individuals from the United States, the United Kingdom and Germany, 80 percent of Germans and 72 percent of Americans were reluctant to share their information with businesses because of a desire to maintain personal privacy.[284]

Individuals on both sides of the Atlantic and across the web feel they have lost control over the way their personal information is collected and used.[285]

In the, EU 70 percent (along with 82 percent of online shoppers and 74 percent of social network users) felt that they did not have complete control over their personal information,64 that companies were not straightforward about their data practices, and that consumers had only partial, if any, control of their own data.[286]

As much as 86 percent of users in the United States have taken steps to cover their digital footprints, with most individuals saying they want to do more to protect their data online, but lack the means to be anonymous online.[287] EU residents are also concerned about their online privacy, and were more likely to have used technical or procedural means to protect it, such as implementing tools and strategies to limit unwanted emails (42 percent), checking that an electronic transaction is protected on the site (40 percent), or using anti-spyware software (39 percent).[288] A total of 62 percent of EU respondents also said they provide only the minimum amount of information required online in order to protect their identity.[289]

---

283 De Mooy M., Rethinking Privacy Self-Management and Data Sovereignty in the Age of Big Data. Considerations for Future Policy Regimes in the United States and the European Union, 2017, https://cdt.org/files/2017/04/Rethinking-Privacy_2017_final.pdf, p. 20.

284 Forbath T., Morey T., Schoop A., Customer Data: Designing for Transparency and Trust, Harvard Business Review, May 2015, https://hbr.org/2015/05/customer-datadesigning-for-transparency-and-trust

285 Madden M., Public Perceptions of Privacy and Security in the Post Snowden Era. Pew Research Center, Nov. 12, 2014. www.pewinternet.org/2014/11/12/public-privacy-perceptions/

286 European Commission. "Data Protection: Europeans Share Data Online, but Privacy Concerns Remain — New Survey." European Commission press release, June 16, 2011. http://europa.eu/rapid/press-release_IP-11-742_en.htm

287 Madden M., Public Perceptions of Privacy and Security in the Post Snowden Era. Pew Research Center, Nov. 12, 2014.
www.pewinternet.org/2014/11/12/public-privacy-perceptions/

288 European Commission. Attitudes on Data Protection and Electronic Identity in the European Union. Special Eurobarometer 359, European Commission, June 2011. http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

289 European Commission. Attitudes on Data Protection and Electronic Identity in the European Union. Special Eurobarometer 359, European Commission, June 2011. http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

In November 2014, in an open letter to the US Senate, nine ICT companies implored the body to pass the USA Freedom Act[290], which would curb much of the massive data collection by the NSA and other agencies. The legislation should prevent the bulk collection of internet metadata under various authorities. The bill also aims to allow for transparency about government demands for user information from technology companies and to assure that the appropriate oversight and accountability mechanisms are in place. Apple, AOL, Dropbox, Evernote, Facebook, Google, LinkedIn, Microsoft, Twitter and Yahoo signed the letter. Proposed by them reforms include:

- preventing government access to data without proper legal process;
- assuring that providers are not required to locate infrastructure within a country's border;
- promoting the free flow of data across borders;
- and avoiding conflicts among nations through robust, principled, and transparent frameworks that govern lawful requests for data across jurisdictions.[291]

Since not so long also biggest US companies turned again their interest towards more consistent privacy protection. The chief executive officers (CEOs) of 51 tech companies (including Amazon, AT&T, Dell, IBM, Qualcomm, SAP, Salesforce, Visa, Mastercard, JP Morgan Chase, State Farm, and Walmart) have signed and sent an open letter to Congress leaders in September 2019, asking for a federal law on user data privacy to supersede the rising number of privacy laws that are cropping up at the state level. The companies would like one law that governs all user privacy and data protection across the US, which would simplify product design, compliance, and data management.[292]

In February 2019, the US Government Accountability Office (GAO), a US government auditing agency, gave Congress the go-ahead for passing a federal internet data privacy legislation to enhance consumer protections, similar to the

290 USA Freedom Act, To reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes, https://www.govinfo.gov/content/pkg/PLAW-114publ23/html/PLAW-114publ23.htm

291 Microsoft, Google & friends urge passage of USA Freedom Act, http://reformgs.tumblr.com/post/102821955852/open-letter-to-the-us-senate

292 Cimpanu C., 51 tech CEOs send open letter to Congress asking for a federal data privacy law, September 10, 2019, https://www.zdnet.com/article/51-tech-ceos-send-open-letter-to-congress-asking-for-a-federal-data-privacy-law/

EU's General Data Protection Regulation (GDPR). Earlier, the 56-page report[293] was put together by the US Government Accountability Office (GAO), a bi-partisan government agency that provides auditing, evaluation, and investigative services for Congress. Its reports are used for hearings and drafting legislation. [294]

In 1950, the European Convention for the Protection of Human Rights (art. 8) already guaranteed to everyone the "right to respect for his private and family life, home and correspondence,"[295] and a formulation that was literally repeated thirty years later in the European Union's Charter on Fundamental Rights (art. 7).[296] However, like the Human Rights Convention, the Charter had no immediate practical effects. Therefore, the European Union's organs and institutions were only obliged to strictly comply with the Charter when the Lisbon Treaty came into force.[297] Dignity concerns are weightier in Europe while liberty interests predominate in the United States.[298] Importance of both dignity and liberty, the European Union and its Member States are obliged to protect privacy in both their internal regulations and external agreements. Since the Lisbon Treaty the European Union has no choice: privacy cannot be determined at will. The Union's considerations have always been grounded on article 7 as well as on all other privacy-relevant provisions of the Charter, in particular article 8.

Consequently, contrary to the arguments of some scholars, the European Union neither acts against the background of an "antiquated" Privacy Directive of the European Commission, nor intends to impose its views on the rest of the world as a kind of "privacy cop,"[299] but merely follows the Charter and the duties imposed on it there.

US have been hesitant to bring forward comprehensive private sector legislation to protect privacy on the basis of human rights arguments and that while codes of conduct are the method of choice for dealing with privacy in the private sector, this approach is not without its problems with respect to the scope and enforcement of

293 Report to the Chairman, Committee on Energy and Commerce, House of Representatives, INTERNET PRIVACY - Additional Federal, Authority Could Enhance Consumer Protection and Provide Flexibility, January 2019, https://www.gao.gov/assets/700/696437.pdf

294 Cimpanu C., GAO gives Congress go-ahead for a GDPR-like privacy legislation, February 15, 2019, https://www.zdnet.com/article/gao-gives-congress-go-ahead-for-a-gdpr-like-privacy-legislation/

295 Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocol No. 11, Rome 4.XI. 1950, European Treaty Series [ETS] no. 5.

296 Charter of Fundamental Rights of the European Union, proclaimed by the European Council on December 7, 2000 in Nice, O.J., 18.12.2000, C 364/1.

297 Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Communities, Dec. 13 2007, 2007 O.J. (C 306) 1.

298 Whitman J. Q., The Two Western Cultures of Privacy: Dignity Versus Liberty, 113 YALE L.J. 1151 (2004).

299 Santolli J., Terrorist Finance Tracking Program: Illuminating the Shortcomings of the European Union's Antiquated Data Privacy Directive, 40 GEO. WASH. INT'L. L. REv. 553 (2008), Federal Constitutional Court, 54 NJW 1921 (2001); see also Federal Supreme Court, BGHZ 128, 1 (1996).

those protections. More often than not, individuals are largely left on their own to protect their privacy.[300] The European Union is bound by the EU Data Protection Directive, while the Americans continue to support self-regulation.

Legal protection of privacy, but more specifically, of the events of an individual life, both private and public, developed differently in Europe and in the US. However, there are similarities in the development of mass media and the importance of protection the privacy of personal life. The connection between mass media and private life is important to mention because of two reasons. Mass media are responsible for revealing events or information that should remain private, therefore violating the individual right to privacy or by publicizing events whose social or political relevance prevails over their private nature.[301]

What the European unease, at both the popular and senior political levels, highlights, however, is the big difference between the US and Europe. Europeans still operate under the assumption that it is critical to uphold the rule of law. The US government is more than flexible with the rule of law by turning any notion of privacy into a long discussion. This leads to dangerous implications for the core ideas of democracy.

As allies, there is little Europeans can do to make the Americans reconsider. At least this is what history teaches us, so far. However, we try by observing and constantly attacking the biggest US companies, especially recently. If US do not believe in the rule of law, in the way understood by Europeans, for themselves, even in extenuating circumstances like dealing with a very broadly defined terrorist threat, then there is little we can achieve with Washington – other than keeping our distance and whenever possible forcing our solutions. At least in Europe and for European citizens.

The fact that US social media companies are effectively making common cause with the American government, in systematically hollowing out any rights of privacy of European citizens, provides us with a potent tool. - Americans, in the end, only take notice of things when it hits their pockets. When we make European privacy regulations binding for US firms operating on our territory, and impose serious penalties in cases of violation, only then will we have a chance of defending our European rights.[302]

---

300 Cavoukian A., Privacy as a Fundamental Human Right vs. an Economic Right: An Attempt at Conciliation, September 1999, http://www.ontla.on.ca/library/repository/mon/10000/211714.pdf, p. 8.

301 Mantelero A., The EU Proposal for a General Protection Regulation and the roots of the 'right to be forgotten', Computer Law & Security Review 29 (2013), p. 229-230.

302 NSA spying on Europe reflects the transatlantic culture gap by Jan Philipp ALBRECHT, http://www.respect-my-privacy.eu/en/blog/jan-albrecht/nsa-spying-europe-reflects-transatlantic-culture-gap

According to Professor Joel Reidenberg[303] in Europe, there is a sense that privacy and control over personal data are basic human rights, whereas in America, freedom of speech and free-market solutions tend to prevail.[304]

EU approach in this matter is focused more on recent events with terrorism. In wake of Paris shootings, former British Prime Minister David Cameron wanted to ban encryptions that government cannot read in extreme situations. Cameron wanted to be able to block WhatsApp and Snapchat as part of his plans for new surveillance powers. He claimed that he would stop the use of methods of communication that cannot be read by the security services even if they have a warrant. Nevertheless, that could include popular chat and social apps that encrypt their data, such as WhatsApp. Apple's iMessage and FaceTime also encrypt their data and could fall under the ban along with other encrypted chat apps like Telegram. The connection between encrypted communications tools and letters and phone conversations was made, both of which can be read by security services in extreme situations and with a warrant from the home secretary.[305]

Former president Barack Obama's rollout of privacy and data security policies offered big promises to protect consumer information online, but the reality is his legislative ideas are a long shot in Congress and his voluntary industry initiatives lack enforcement basis. The package of proposals — including a data-breach notification law and a privacy bill of rights — are mostly a rehash of previous administration proposals. While some lawmakers have expressed interest in data breach and student privacy bills, such legislation has made little progress in the past. Congress has even less enthusiasm for the base-line privacy bill. According to Obama mission of protecting information and privacy in the information age, this should not be a partisan issue. Later he stated that it is one of those new challenges in the modern society that crosses the old divides — transcends politics, transcends ideology. Liberal, conservative, Democrat, Republican, everybody is online, and everybody should understand the risks and vulnerabilities as well as opportunities that are presented by this new world. Obama's data-breach proposal aimed to impose a national standard for companies to notify consumers, in the event their information is stolen or compromised, within 30 days of the discovery of an incident. His student privacy bill, modelled on a California measure, would impose new restrictions on

303 Joel R. Reidenberg is the Stanley D. and Nikki Waxberg Chair and Professor of Law at Fordham University School of Law where he is the Founding Academic Director of Fordham's Center on Law and Information Policy. His research and teaching center on privacy, Internet, and intellectual property law. http://faculty.fordham.edu/jreidenberg/

304 Google 'Right To Be Forgotten' Ruling Unlikely to Repeat in U.S., http://www.nbcnews.com/tech/internet/google-right-be-forgotten-ruling-unlikely-repeat-u-s-n114731

305 WhatsApp and iMessage could be banned under new surveillance plans, http://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-and-snapchat-could-be-banned-under-new-surveillance-plans-9973035.html

companies that collect or store student data while providing products and services to schools.[306]

Some privacy advocates, while bullish for laws that will tighten consumer privacy, remained sceptical towards Obama's ideas, seeing it more as a public relations manoeuvre designed to reassure European privacy officials. Apparently, an unannounced but intended audience for the administration's plan is to remove a serious obstacle to its plans for a US-EU trade deal, known as TTIP (the Transatlantic Trade and Investment Partnership). Consumer privacy has been one of the sticking points with EU officials who worry that the US does not have a comprehensive privacy framework. Interestingly, such legislation has repeatedly run into fears that a federal standard would weaken stricter rules enacted by states.[307]

Not forcing but convincing, even asking companies, including those biggest, former president Obama touted the 75 education tech companies that have voluntarily committed to keeping student data private, including Microsoft. Apple, which did not sign on initially, has now committed to the pledge. However, other major players in the education tech market, including Google and Pearson, are still not listed as signatories.

The reason behind it might be, because some parts of the tech industry said the president should have broadened his proposal to include surveillance reform, a key issue for Internet companies following Edward Snowden's leaks about the National Security Agency. Apparently, the president missed an opportunity to address the continued push by law enforcement and intelligence agencies to weaken security for the purpose of surveillance. These actions may threaten the competitiveness of the US tech sector and discourage consumer confidence in digital products and services.[308]

Already in 2007, there was major concern about collecting too much data. A coalition of privacy groups asked the government to set up a mandatory do-not-track list for the Internet. The groups, which include the Consumer Federation of America, World Privacy Forum and several others — are worried that online advertising companies are collecting too much data about consumers' Web habits. The goal of providing a consumer with advertising that matches their interests is something that provides a lot of value to consumers, but there are questions about whether it may also come with costs that consumers do not want to pay.[309]

---

306 Does Obama privacy push have oomph?, http://www.politico.com/story/2015/01/obama-cybersecurity-privacy-initiatives-114184.html

307 Does Obama privacy push have oomph?, http://www.politico.com/story/2015/01/obama-cybersecurity-privacy-initiatives-114184.html

308 Does Obama privacy push have oomph?, http://www.politico.com/story/2015/01/obama-cybersecurity-privacy-initiatives-114184.html

309 Consumer Advocates Seek a 'Do-Not-Track' List, http://www.nytimes.com/2007/10/31/technology/31cnd-privacy.html

Unfortunately, the idea never reached happy conclusion: The Federal Trade Commission announced, with fanfare, a plan to let American consumers decide whether to let companies track their online browsing and buying habits. The plan would let users opt out of the collection of data about their habits through a setting in their web browsers, without having to decide on a site-by-site basis. Although many digital advertising companies agreed to the idea in principle, the debate over the definition, scope, and application of "Do Not Track" has been raging for several years.[310]

Now, finally, an industry-working group is expected to propose detailed rules governing how the privacy switch should work. The group includes experts but is dominated by Internet giants like Adobe, Apple, Facebook, Google, and Yahoo. It is poised to recommend a carve-out that would effectively free them from honouring "Do Not Track" requests. If regulators go along, the rules would allow the largest Internet giants to continue scooping up data about users on their own sites and on other sites that include their plug-ins, such as Facebook's "Like" button or an embedded YouTube video. This giant loophole would make "Do Not Track" meaningless. However, it is important to remember, that the Federal Trade Commission does not seem to fully understand the nature of the Internet.[311]

In US nowadays, there are hundreds of laws pertaining to privacy: the common law torts, criminal law, evidentiary privileges, constitutional law, at least twenty federal statutes, and numerous statutes in each of the fifty states. Although the federal government has enacted privacy laws, most privacy legislation in the United States is enacted at the state level. Many states have privacy legislation on employment privacy (drug testing, background checks, employment records), SSNs, video rental data, consumer reporting, cable television records, arrest and conviction records, student records, tax records, wiretapping, video surveillance, identity theft, library records, financial records, insurance records, privileges (relationships between individuals that entitle communications to privacy), and medical records.[312]

The last decade of the twentieth century presented profound new challenges for the protection of information privacy, such as rise of the Internet and the increasing use of email in the mid-1990s. The Internet presented new methods of gathering information.

---

310 Consumer Advocates Seek a 'Do-Not-Track' List, http://www.nytimes.com/2007/10/31/technology/31cnd-privacy.html

311 Consumer Advocates Seek a 'Do-Not-Track' List, http://www.nytimes.com/2007/10/31/technology/31cnd-privacy.html

312 Solove Daniel J., Hoofnagle Chr. J., A Model Regime of Privacy Protection (Version 3.0). GWU Law School Public Law Research Paper No. 132; University of Illinois Law Review, Vol. 2006, No. 2, 2006. Available at SSRN: http://ssrn.com/abstract=881294, p. 402 after: ROBERT ELLIS SMITH, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS (2002).

Information privacy law has come a long way. Spurred by the development of new technologies, the law has responded in numerous ways to grapple with emerging privacy problems. Several scholars, including Daniel Solove have criticized[313] the ability of information privacy laws to handle the growing collection and use of personal information in computer databases.[314] Additionally, Paul Schwartz stated that "personal information in the private sector is often unaccompanied by the presence of basic legal protections. Yet, private enterprises now control more powerful resources of information technology than ever before."[315]

Europeans believe that it is none of Americans business to collect information about European citizens as well as implicitly that Americans ought to be more respectful of their own citizens' privacy rights. However, many Americans think that it is none of the Europeans' business what American firms do with personal data on American soil.[316]

Among the intriguing questions discussed in None of Your Business is why the United States and the European Union take such different approaches to data protection. According to Swire and Litan, one factor is the "different information cultures" of the two jurisdictions. Americans generally favour a freer flow of information than do their European counterparts.[317]

The main reasons for differences, US side:[318]

1. Americans are generally more trusting of the private sector and the market. Rather than having the government adopt strict rules that industries may ignore or subvert, Americans would prefer it if firms would voluntarily adopt and abide by appropriate standards.
2. Americans tend to believe in the power of the mass media to hold private sector abuses in check.

313 Solove Daniel J., Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 STAN. L. REV. 1393 (2001); Daniel J. Solove, Access and Aggregation: Public Records, Privacy, and the Constitution, 86 MINN. L. REV. 1137 (2002); Daniel J. Solove, Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75 S. CAL. L. REV. 1083 (2002); Julie E. Cohen, Examined Lives: Informational Privacy and the Subject as Object, 52 STAN. L. REV. 1373 (2000); Elbert Lin, Prioritizing Privacy: A Constitutional Response to the Internet, 17 BERKELEY TECH. L.J. 1085 (2002); Stan Karas, Privacy, Identity, Databases, 52 AM. U. L. REV. 393 (2002).

314 Solove Daniel J., A Brief History of Information Privacy Law. PROSKAUER ON PRIVACY, PLI, 2006; GWU Law School Public Law Research Paper No. 215. Available at SSRN: http://ssrn.com/abstract=914271, p. 3, 46.

315 Schwartz P. M., Privacy and Democracy in Cyberspace, 52 VAND. L. REV. 1609, 1633 (1999).

316 Samuelson P., A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy, Information Economy, 87 Cal. L. Rev. 751 (1999), https://www.jstor.org/stable/3481032?seq=1#metadata_info_tab_contents, p. 755

317 Swire P., Lotan R., NONE OF YOUR Business: WORLD DATA Flows, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY Directive (1998), p. 153-154

318 Swire P., Lotan R., NONE OF YOUR Business: WORLD DATA Flows, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY Directive (1998), p. 7-18

3. Americans are inclined to think that technologies can contribute to the solutions of problems created by technologies.
4. Even when Americans are considering government intervention, they are much more inclined than Europeans to engage in a cost-benefit analysis of regulatory alternatives. Identifying a market failure may suggest the need for government intervention, but Americans are more likely to ask whether possible unintended consequences of a proposed regulation would make the cure worse than the disease.
5. Americans are more inclined to adopt reactive rather than proactive regulations. That is, Americans are generally disinclined to regulate until problems have actually occurred, and they prefer to tailor regulatory solutions to those problems rather than to adopt broad regulations anticipating problems yet to arise.
6. Americans are more prone to adopt regulations that give consumers information about private sector practices so that consumers can exercise their market power to shop for firms with good policies. Once they have such information, Americans tend to think that the market will work things out.

The main reasons for differences, EU side:[319]

1. Europeans tend to think of self-regulation as tantamount to no regulation, in part because individuals will have no remedy if firms violate self-imposed codes of conduct.
2. Europeans prefer to err on the side of overprotection rather than on the side of underprotection. The European data protection legislation illustrates this preference. It strictly regulates the kinds of data that can lawfully be collected, the purposes for which the data can be collected, the uses that can be made of the data, and the length of time the data can be stored.
3. Europeans tend to craft relatively narrow exceptions to broadly applicable rules. The European data protection legislation, for example, contains relatively few and relatively narrow carve-outs.

Finally, another deep-rooted difference between the United States' and the European Union's approaches to data protection arises from their different conceptions about the nature of people's interests in data about themselves. The GDPR includes data protection in its conception of the "fundamental rights" of citizens.' Although Americans cherish certain rights as fundamental to citizenship, they do not generally consider data privacy to be among them. Americans are more

319 Swire P., Lotan R., NONE OF YOUR Business: WORLD DATA Flows, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY Directive (1998), p. 153-154, 159

likely to cherish the principles embodied in the First Amendment-which favours a free flow of information-as fundamental human rights.[320]

Maybe sometimes the law that is given and is external to individuals, I the meaning that it is a set of general rules, which solve any given case in advance, should be given up.[321] Maybe the US approach, less regulated and reactive rather than EU overregulated and proactive is the answer.[322] However, for now, none of the approaches really works against Dominant ICT Companies. On the other hand, it is not without reason to suggest that very often US approach is too broad while EU's is too narrow.[323]

2.6. Direction of the changes

The shifting sands of online privacy are not going to solidify any time soon, judging by the responses to a recent survey of technology experts, internet pioneers and prominent sociologists done by the Pew Research Center's Internet Project[324]. The survey asked respondents whether they thought the minefield of issues, surrounding online privacy rights would be solved either by government or by society as a whole by 2025. The verdict? Not likely at all.

The report is part of a series of studies the Pew Center has done to mark the 25th anniversary of Sir Tim Berners-Lee's invention of the worldwide web and includes responses from hundreds of experts as well as some anonymous answers from those who didn't want to provide their names. The main question was: Will policy makers and technology innovators create a secure, popularly accepted, and trusted privacy-rights infrastructure by 2025?

As one respondent described it, "privacy is still a fluid concept," with different users defining it in different ways — and that is unlikely to change in the next decade. Here are some of the responses that stood out from the Pew Center's report:

- Danah Boyd, Microsoft research scientist: "I expect the dynamics of security and privacy are going to be a bloody mess for the next decade, mired in ugly politics and corporate greed. I also expect that our relationship with other countries is going to be a mess over these issues. People will be far more aware

320 Swire P., Lotan R., NONE OF YOUR Business: WORLD DATA Flows, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY Directive (1998), p. 153.

321 Aguiló-Regla J., Introduction: Legal Informatics and the Conceptions of the Law, [in:] Benjamins V.R., Casanovas P., Breuker J., Gangemi A. (eds) Law and the Semantic Web. Lecture Notes in Computer Science, vol 3369. Springer, Berlin 2005, p. 23.

322 Wiener J. B., Rogers M. D., Comparing precaution in the United States and Europe, Journal of Risk Research 5 (4), 2002, p. 342-343.

323 O'Reilly C., Finding jurisdiction to regulate Google and the Internet, European Journal of Law and Technology, vol. 2, no. 1, 2011, p. 8.

324 http://www.pewinternet.org/

of the ways that data is being used and abused, although I suspect that they will have just as little power over their data as they do now."

- Howard Rheingold, Institute for the Future: "Citizens will join the state and digital businesses in the surveillance game. Privacy is a social construct — for example, until central heating, most people in most houses slept in the same room; in Japan, for centuries, walls were made of paper. Ask any teenager about his or her 'Facebook-stalking' habits. Privacy has already changed."
- Hal Varian, chief economist for Google: "By 2025, the current debate about privacy will seem quaint and old-fashioned. The benefits of cloud-based, personal, digital assistants will be so overwhelming that putting restrictions on these services will be out of the question. Of course, there will be people who choose not to use such services, but they will be a small minority. Everyone will expect to be tracked and monitored, since the advantages, in terms of convenience, safety, and services, will be so great."
- Vint Cerf, co-developer of TCP/IP: "By 2025, people will be much more aware of their own negligent behaviour, eroding privacy for others, and not just themselves. The uploading and tagging of photos and videos without permission may become socially unacceptable. As in many other matters, the social punishment may have to be accompanied by legislation—think about seat belts and smoking by way of example."
- David Weinberger, Harvard's Berkman Center: "Unfortunately, the incentives are unequal: There is a strong incentive to enable strong privacy for transactions, but much less for enabling individuals to control their own info. So, of course, I do not actually know how this will shake out. I assume we will accept that humans do stupid things, and we will forgive one another for them. When your walls are paper, that is what you have to do."
- Mark Rotenberg, Electronic Privacy Information Center: "There will be many contentious battles over the control of identity and private life. The appropriation of personal facts for commercial value — an issue that emerged with Google's 'shared endorsements' and Facebook's 'sponsored stories' — are a small glimpse of what lies ahead. The key will be the defaults: either individuals will control their online persona or it will be controlled by others."
- John Savage, professor of computer science: "A secure, accepted, and trusted privacy-rights infrastructure on the Internet, at the global scale, is impossible for the foreseeable future. For too many large nations a tension exists between state security and privacy rights. They will not sacrifice the former for the latter."
- Kalev Leetaru, Yahoo fellow: "While people publicly discuss wanting more privacy, they increasingly use media in a way that gives away their privacy

voluntarily—for example, broadcasting their location via phone GPS when posting to social platforms, photographing their entire lives, etc. People seem to want to be famous, documenting their lives to the most-minute detail, in ways that would have been unheard of to a past generation."

- Stowe Boyd, Gigaom Research: "We have seen the emergence of publicy as the default modality, with privacy declining. In order to 'exist' online, you have to publish things to be shared, and that has to be done in open, public spaces. If not, people have a lesser chance to enrich friendships, find or grow communities, learn new things, and act as economic agents online."
- Kate Crawford, research scientist: "In the next 10 years, I would expect to see the development of more encryption technologies and boutique services for people prepared to pay a premium for greater control over their data. This is the creation of privacy as a luxury good. It also has the unfortunate effect of establishing a new divide: the privacy rich and the privacy poor."[325]

Putting aside private sector conclusions, it is worth to come back to US Government efforts. Former president Obama asked intelligence agencies to determine whether there is a way to gather phone data for detecting potential terrorist activity without relying on bulk collection. The request came about after ex-NSA contractor Edward Snowden revealed details of government practices of mass collection of phone metadata – such as the time and length of calls – from millions of Americans. Apparently, the US needs to preserve its capability to track electronic communications of terrorist suspects but is working with companies to ensure the government meets legitimate privacy concerns. Obama had already proposed some surveillance reforms, including nixing the government's storage of the phone records and forcing the NSA to gather them from company databases instead.[326]

The Federal Trade Commission confirmed some of the worst fears about Internet-connected devices, saying the technology presented serious data security and privacy risks, and urged companies to make data protection a top priority. While the agency noted the potential benefits for owners of smart devices like connected fitness bands, regulators also said the technology generated enormous amounts of personal data that could be misused or obtained by hackers.[327]

Although the report highlights the issues that the agency intends to monitor and underlines the best practices regulators hope companies will adopt, it does not carry the weight of enforceable regulations. The agency has urged Congress to enact a

325 Online privacy will still be a mess a decade from now, experts say, https://gigaom.com/2014/12/18/online-privacy-will-still-be-a-mess-a-decade-from-now-experts-say/

326 Privacy advocates say NSA reform doesn't require 'technological magic', http://www.csmonitor.com/World/Passcode/2015/0116/Privacy-advocates-say-NSA-reform-doesn-t-require-technological-magic

327 opposite to what Google would like us to believe – The role of Dominant ICT Companies

baseline federal consumer privacy law. However, such legislation is unlikely to pass with Congress controlled by Republicans.

Data security and privacy experts predicted that at least larger, well-known technology companies would take the agency's data security recommendations into account — if only to reduce the business risk of federal investigations.

Companies may be reluctant to adopt those practices (putting limits on the volume of information their devices collect from consumers and on the amount of time they retain those records) because data storage costs are decreasing and the ability to quickly analyse huge data sets is increasing. If a company collected 300 to 400 facts about millions of individual consumers, it would be costly and cumbersome to figure out which details to delete and which were important to retain.[328]

2.6.1. Safe Harbor Judgment

The European Commission's Directive on Data Protection went into effect in October of 1998 and would prohibit the transfer of personal data to non-European Union nations that do not meet the European 'adequacy' standard for privacy protection. While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Union.

In order to bridge these different privacy approaches and provide a streamlined means for U.S. organizations to comply with the Directive, the U.S. Department of Commerce in consultation with the European Commission developed a "Safe Harbor" framework and this website to provide the information an organization should need to evaluate – and then join – the Safe Harbor.[329]

The US Safe Harbor was an agreement between the European Commission and the United States Department of Commerce that enables organizations to join a Safe Harbor List to demonstrate their compliance with the European Union Data Protection Directive. This allows the transfer of personal data to the US in circumstances where the transfer would otherwise not meet the European adequacy test for privacy protection.

The Safe Harbor is best described as an uneasy compromise between the comprehensive legislative approach adopted by European nations and the self–regulatory approach preferred by the US. The Safe Harbor Framework has been the subject of ongoing criticism, including two previous reviews (2002 and 2004). Those reviews expressed serious concerns about the effectiveness of the Safe Harbor as a privacy protection mechanism.

---

328 F.T.C. Says Internet-Connected Devices Pose Big Risks, http://bits.blogs.nytimes.com/2015/01/27/f-t-c-calls-for-strong-data-and-privacy-protection-with-connected-devices/

329 http://www.export.gov/safeharbor/

The first public draft of the Safe Harbor Principles was released in November 1998, (although they were not officially accepted by the EU until 2000.):

'The European Union's comprehensive privacy legislation, the Directive on Data Protection, which became effective on October 25, 1998, prohibits the transfer of personally identifiable data to third countries that do not provide an "adequate" level of privacy protection. Because the United States relies largely on a sectoral and self-regulatory, rather than legislative, approach to effective privacy protection, many US organizations are uncertain about the impact of the "adequacy" standard on personal data transfers from the European Community to the United States.

Safe Harbor Principles:

Identifying the appropriate privacy principles is clearly central to this approach. Such principles must provide "adequate" privacy protection for European citizens. They must also reflect US views on privacy, allow for relevant US legislation, regulation, and other public interest requirements, and provide a predictable and cost-effective framework for the private sector. Accordingly, we have drafted the attached principles, based on the Department's discussion paper, "The Elements for Effective Privacy Protection," the 1980 OECD Privacy Guidelines, private sector self-regulatory, online privacy programs, and discussions with industry and the European Commission.

Principles were designed to facilitate a bilateral understanding between the US and European Community and thus to enhance commerce between the US and the European Community. They were not intended to govern or affect US privacy regimes, which are being addressed by other government and private sector efforts. Adoption of the principles was voluntary, and their use was intended solely by US organizations receiving personal data from the European Union for the purpose of qualifying for the safe harbor.

Benefits of participating in Safe Harbor Agreement:

- All Member States would be bound by the Commission's recognition of the safe harbor principles as adequate;
- The scope of any legal action by European citizens contesting data transfers under the Directive would be narrowed to alleged noncompliance with stated practices rather than addressing adequacy of the safe harbor privacy principles;
- In those EU Member States that require prior approval before data transfers can occur, organizations that belong in the safe harbor would either not have to seek such approval or would, generally, have their applications automatically approved;
- The organization would have access to streamlined and expedited procedures in the event of a dispute; and

- A grace period for safe harbor participants to give them time to implement the principles.

Some of the principles could undergo additional revisions as the negotiations proceed.[330]

All this now belongs to the past as The European Court of Justice has ruled that Safe Harbour is invalid. This Safe Harbour was contested by Austrian data protection activist Maximillian Schrems in a case concerning the treatment of personal data by Facebook.[331]

This was the second ruling about data protection from an EU court. The first[332] ruled that businesses had to comply with the laws of member-countries as well as those of the EU when processing data across nations. After the invalidation of the safe harbour decision by the Court of Justice of the EU (CJEU), based on the finding that data transfers under the safe harbour decision do not guarantee an adequate level of protection of the data in the US and underlining the importance of the fundamental right to data protection, this safe harbour has ceased to exist.

Implications of Safe Harbour decision:

1. US and EU negotiators had to update the Safe Harbour framework. Both sides renegotiated the agreement since the Snowden revelations. Negotiators were reportedly close[333] to an agreement when they got wind of the breadth of the upcoming ECJ decision. The Commission wanted to use the decision to gain more advantage in these negotiations. However, Congress was already considering bipartisan legislation[334] that would provide US Privacy Act protections to European citizens.
2. The spotlight was on European national data protection regulators. In addition to their new ability to examine data transfers, they had a role approving other mechanisms companies may deploy to replace Safe Harbour, including binding corporate rules[335] for intra-company transfers of personal data. In a number of EU countries, national regulators also had the power to confirm whether

330 Safe Harbor Principles as of Nov 4, 1998 - http://www.ita.doc.gov

331 Case C-362/14, Maximillian Schrems v Data Protection Commissioner.

332 http://curia.europa.eu/juris/document/document.jsf?text=&docid=168944&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=93833

333 Europe's top court just gave U.S. tech firms a huge headache, http://fortune.com/2015/10/06/safe-harbor-facebook-data/

334 H.R.1428 - Judicial Redress Act of 2015, https://www.congress.gov/bill/114th-congress/house-bill/1428

335 Overview on Binding Corporate rules, http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm

model clauses[336] are being used to transfer personal data to the United States and other third countries. Many of these national authorities had backlogs of several months. It became unclear if they would order suspension of transfers of personal data to the United States under model clauses arrangements until they work through what would surely become a much bigger backlog.

3. This decision was a direct fallout of Edward Snowden's revelations of NSA surveillance. It was argued[337] that the ECJ based its ruling on erroneous factual assumptions regarding the nature and oversight of U.S. surveillance. Moreover, some experts note that the United States provides adequate privacy protections, especially in comparison to European countries many of which have no independent data protection oversight of law enforcement and intelligence surveillance. The ECJ also based its decision on a 2013 European Commission report on US surveillance, parts of which was outdated given US surveillance reforms[338] spurred by President Obama's 2014 executive order[339]. Robert Litt, general counsel for the Office of the Director of National Intelligence, wrote an opinion piece[340] for the Financial Times before the ruling to argue that the surveillance program at issue in the ECJ's decision does not give the US unrestricted access to data.[341]

The last point is indeed very arguable. At any given point in time, it is extremely hard to tell which point of view should be believed. Back in 2013, Barack Obama claimed that all revelations about mass surveillance are a simple overreaction and no one should be worried, that everything is under judicial control. Yet, even from the words coming directly from NSA we know it was quite the opposite. We may never know the truth, but in my opinion, in this situation of uncertainty, ECJ made

336 COMMISSION DECISION of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF

337 Don't Strike Down the Safe Harbor Based on Inaccurate Views About U.S. Intelligence Law, https://iapp.org/news/a/dont-strike-down-the-safe-harbor-based-on-inaccurate-views-on-u-s-intelligence-law/

338 SIGNALS INTELLIGENCE REFORM 2015. ANNIVERSARY REPORT, http://icontherecord.tumblr.com/ppd-28/2015/overview

339 Presidential Policy Directive -- Signals Intelligence Activities, https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

340 Europe's court should know the truth about US intelligence, http://www.ft.com/intl/cms/s/90be63f4-6863-11e5-a57f-21b88f7d973f,Authorised=false.html?siteedition=uk&_i_location=http%3A%2F%2Fwww.ft.com%2Fcms%2Fs%2F0%2F90be63f4-6863-11e5-a57f-21b88f7d973f.html%3Fsiteedition%3Duk&_i_referer=http%3A%2F%2Fblogs.cfr.org%2Fc5a52a1175b96da3ad2f95a79beaf0fa&classification=conditional_standard&iab=barrier-app#axzz3x2GajVs1

341 The Implications of the European Safe Harbor Decision, http://blogs.cfr.org/cyber/2015/10/07/the-implications-of-the-european-safe-harbor-decision/

a right decision. As EU cannot be 100% sure about what happens with the data of European citizens, Safe Harbour should become invalid. As it was designed. Now it has become invalid.

Nevertheless, there is a lot of discussion about how EU is unfair towards US intelligence law. It seems that US commentators forget about how strict EU privacy and data protection laws are. The Safe Harbour decision should not be determined by what is changing or will change in US legislation, but about how US approach to privacy and spying showed the agreement's weaknesses. Even if it could be accepted that US has far more extensive legal rules, oversight and other checks and balances on intelligence agencies than is generally true in EU member states[342], there is other issue. Did this "extensive legal rules, oversight and other checks and balances" stopped NSA to unleash full-scale spying attack on EU states and citizens? The answer is no. Therefor I stand with opinion that US solutions are not enough.

After Safe Harbour decision, we can find opinions on how PRISM and NSA actions were actually covered by legislation. According to Review Group[343], the PRISM program is governed by Section 702 of the law enacted in 2008 to amend the Foreign Intelligence Surveillance Act. The Review Group, in its Appendix B, set forth privacy protections applicable to Europeans and other non-U.S. persons under the law. If we, Europeans, believed in US system then these are the rules behind PRISM and NSA actions in general:

1. Targeting must be for a valid foreign intelligence purpose in response to National Intelligence Priorities;
2. Targetings must be under a Foreign Intelligence Surveillance Court (FISC) approved Section 702 Certification and targeted at a person overseas;
3. All targeting is governed by FISC-approved targeting procedures;
4. Specific communications identifiers (such as a phone number or email address) are used to limit collections only to communications to, from, or about a valid foreign intelligence target;
5. Queries into collected data must be designed to return valid foreign intelligence and overly broad queries are prohibited and supervised by the FISC;
6. Disseminations to external entities, included select foreign partners (such as E.U. member states) are made for valid foreign intelligence purposes; and
7. Raw data is destroyed after two years or five years, depending on the collection source.[344]

342 Don't Strike Down the Safe Harbor Based on Inaccurate Views About U.S. Intelligence Law, https://iapp.org/news/a/dont-strike-down-the-safe-harbor-based-on-inaccurate-views-on-u-s-intelligence-law/

343 President Obama created an independent Review Group on Intelligence and Communications Technology, to advise him on how to respond to concerns about intelligence agency activities.

344 Don't Strike Down the Safe Harbor Based on Inaccurate Views About U.S. Intelligence Law, https://iapp.org/news/a/dont-strike-down-the-safe-harbor-based-on-inaccurate-views-on-u-s-intelligence-law/

The problem is that this set of rules do not overlap with real actions of US agencies. They remained a theory, not a reality. It was confirmed by Edward Snowden and by NSA employees. The violation of EU privacy was to massive, to accept that only some mistakes were made or that EU reaction is too paranoid.

The good thing behind the mass surveillance scandal are all the changes in US law regarding intelligence. US continue reforms and reviews, release assessments, try to create new procedures with stricter definitions and documentation of the purpose of each request, subject to two levels of approval within the NSA with some independent judiciary review.[345] I hope that, US solutions will be enough to protect EU citizens and states.

The Federal Trade Commission released its report on consumer privacy[346] to provide policy recommendations for American businesses and legislators. Combined with the Privacy Bill of Rights[347], the report helps lay out a path for the emerging comprehensive US data privacy framework. With EU new regulation a key factor to examine is how the two continents' modified approaches will interact, are the two distinct privacy regimes becoming more interoperable or are they diverging?

One of the first concerns is consent – in US known as consumer choice. The FTC report and Privacy Bill of Rights may result in a simplification of consumer choice principles. On the other hand, the EU regulation aims to toughen the concept by requiring "explicit consent". The major difference is in the two continents' approach to individual control, i.e. when and to what degree must choice and transparency be provided to the data subject before the controller is able to collect data. The US's proposed approach relies on the concept of "context", meaning that processing should only be carried out in the context of the services requested by the consumer. The EU's regulation, by contrast, calls for controllers to demonstrate a "legitimate basis" for data processing.

Additionally, companies are limited to processing data for purposes that are compatible with the original collection of data. Furthermore, both concepts have been proposed in an effort to allow companies to fulfil their contractual obligations

345 The USA Freedom Act: A Partial Response to European Concerns about NSA Surveillance, http://peterswire.net/wp-content/uploads/gtjmce2015-1-swire.pdf
Recommendation Assessment Report January 29, 2015, https://www.pclob.gov/library/Recommendations_Assessment-FactSheet.pdf
SIGNALS INTELLIGENCE REFORM. 2015 ANNIVERSARY REPORT, http://icontherecord.tumblr.com/ppd-28/2015/overview
Presidential Policy Directive 28 (PPD-28), January 12, 2015, http://fas.org/irp/nsa/nsa-ppd-28.pdf

346 Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers, https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers

347 CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY, https://www.whitehouse.gov/sites/default/files/privacy-final.pdf

to data subjects without having to solicit permission for each required data operation. EU's "legitimate basis" is exclusively intended to be a derogation from a process which otherwise relies on explicit consent. Meanwhile, under US framework, companies need only provide choice and heightened transparency when data is used in a manner diverging from "commonly accepted principles", i.e., when processing is outside the context of why a particular set of data was collected.[348]

However, what does this actually mean for the people of Europe and the companies they interact with on a regular basis?

Safe Harbour was a deal between the US and the EU that allowed for the easy transfer of personal data. It was established because US data protection laws did not match EU standards. EU data protection laws state that companies can only transfer EU citizens' data outside of member states if the destination country has data protection laws that match those of the Union. The 4,000 or so businesses that were part of the Safe Harbour agreement include the major tech companies Airbnb, Apple, Google, Facebook, LinkedIn, Twitter and Yahoo. In addition, big businesses like Adobe, Coca-Cola Enterprises, Ford Motor Company and eBay were signed up. The full list of companies is available to read here[349].

EU and US had to renegotiate a data sharing agreement. For companies to continue operating across the Atlantic, either the EU had to bend to the US, or the US had to draft stronger data protection laws.

According to Anna Fielder, Privacy International's[350] chair of the board, Safe Harbour should not have been agreed to 15 years ago. Indeed, there is a lot of data transfers, not just between the EU and the US but between the EU and lots of other countries. Those countries do not have special arrangements like Safe Harbour. They have to operate under EU legislation.

Businesses that relied on the Safe Harbour agreement for processing and storing their data in the US had to rethink. Solutions involved drafting new contractual agreements with users; encrypting US servers; or building EU-based servers. Companies were able to transfer data if they have the free and informed consent of users, and if it was in interest of the public or an individual. There always must be a balance between protecting privacy and enabling digital services. Nevertheless, the more restrictions that are put on digital services, access to data, and using technology across borders, the more encouragement there is for innovators to set up outside of the EU.

In the short term, the ruling did not affect day-to-day use of the products from Safe Harbour-licensed companies.[351]

---

348 Context and Legitimate Basis: US-EU approaches to data processing, https://fpf.org/2012/03/27/context-and-legitimate-basis-us-eu-approaches-to-data-processing/

349 https://safeharbor.export.gov/list.aspx

350 https://www.privacyinternational.org/

351 What does the end of Safe Harbour mean for you?, http://www.wired.co.uk/news/archive/2015-10/06/what-does-the-end-of-safe-harbour-mean

Does this mean it was illegal for EU companies to transfer personal data to the US under the Safe Harbour Program? The ECJ has invalidated the blanket "stamp of approval" given to data transfers under the Safe Harbour Program by Commission Decision 2000/520/EC. This meant that individual countries could review transfers on a case-by-case basis to determine if they are valid. The Safe Harbour Program constituted a de facto legal mechanism for the transfer of such data, and the national data protection authorities had no right to review/challenge those transfers. This change allowed for legal challenge and therefore placed an additional burden on European companies to show that an 'adequate level of protection' is afforded to the personal data being transferred. Until the new agreement between US and EU.

Some of the more conservative authorities (e.g., Germany, France, and Italy) said that the Safe Harbour Program alone cannot be relied upon as a legal method of data transfer. Other countries took a more relaxed approach and state that whether or not a transfer under Safe Harbour is legal will depend on a number of factors, including the nature of the data being transferred (and how likely it is to be the subject of US government surveillance) and the purposes for which it is processed. Likewise, companies themselves had different reactions depending on where they (and their data subjects) were located, the nature of the data transferred, and their sensitivity to risk.[352]

The Commission wanted to use the decision to gain more advantage in these negotiations.[353] To sum up, officials had been trying to reach a new Safe Harbour deal since 2013, and the decision has intensified pressure on those negotiations. An agreement was needed to reduce much of the legal uncertainty arising from the court's landmark ruling. Both sides stressed that the remaining sticking points are surmountable, and that a new data agreement was imminent.

The European Commission was charged with dealing with the consequences of the court's privacy ruling. European policy makers pointed out that the United States had wanted provisions in the new deal to allow American intelligence agencies access to European data for national security reasons. And therefore, they stalled negotiations. According to Christopher Kuner[354], both the US and Europe are equally to blame - it has been a somewhat dysfunctional relationship. Neither side realized that this ruling was coming or what impact it would have.

In EU, it is strongly believed that citizens' privacy cannot be guaranteed until Europeans can bring legal cases in the United States when their data is misused. Any new Safe Harbour agreement was expected to give Europeans that right. Officials

352 ECJ Rules: Decision 2000/520/EC on U.S./EU Safe Harbor Framework Invalid, https://www.hollandhart.com/safe-harbor-framework-invalid

353 https://www.congress.gov/bill/114th-congress/house-bill/1428

354 Co-director of the Brussels Privacy Hub, a research centre at the Vrije Universiteit Brussel in Belgium.

also wanted to limit the ability of American intelligence agencies to access European citizens' data when it is transferred outside the European Union.[355]

Agreement on a new data transfer framework between the EU and US was reached after the deadline on the 2nd of February 2016. The agreement that has been named the EU-US Privacy Shield according to a European Commission press release provides for strong obligations for US companies dealing with data of EU citizens, clear safeguards and transparency obligations on US government access to data, a yearly review of the framework for EU-US data transfers and the creation of an ombudsperson.[356]

Discussion about Safe Harbour and the new agreement between US and EU is continued in Chapter 5.

2.6.2. Right to be Forgotten Judgment

Right to be forgotten enables people to request web companies to delete personal information from their servers and is part of a General Data Protection Regulation revising EU privacy law.

ECJ judges ruled that Google collects and processes data as part of its search engine. This brought it under a 1995 EU directive, giving individuals the right to have access to and request the deletion of data held by companies.

In July 2014, Advocate-General Jääskinen's opinion[357] on the case, a non-binding yet influential document, argued against the imposition of a right to be forgotten. It stated, *this would entail sacrificing pivotal rights such as freedom of expression and information*.

The CJEU applied EU data protection law to the Google search engine under Article 4(1)(a) of the Directive, based on its finding that Google Spain was "inextricably linked" to the activities of Google Inc. by virtue of its sale of advertising space on the search engine site provided by Google Inc, even though Google Spain had no direct involvement in running the search engine. In short, the Court found that data processing by the search engine was "carried out in the context of the activities of an establishment of the controller" (i.e., Google Spain).

Thus, it seems that there would be no impediment under EU law, for example, to a Chinese citizen in China who uses a US-based Internet search engine with a subsidiary in the EU asserting the right to be forgotten against the EU subsidiary with regard to results generated by the search engine (note that Article 3(2) of the

355 In Europe-U.S. Clash on Privacy, a Longstanding Schism, http://www.nytimes.com/2015/10/08/technology/in-europe-us-clash-on-privacy-a-longstanding-schism.html?_r=1

356 European Commission - Press Release, Strasbourg, 2 February 2016, EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield, http://europa.eu/rapid/press-release_IP-16-216_en.htm.

357 Opinion of Advocate General Jääskinen delivered on 25 June 2013, https://publications.europa.eu/en/publication-detail/-/publication/36af7add-c149-11e3-86f9-01aa75ed71a1

proposed EU General Data Protection Regulation would limit the possibility of asserting the right to be forgotten by individuals without any connection to the EU, since the application of EU data protection law would be limited to "data subjects residing in the Union")

Since only the US entity running the search engine would have the power to amend the search results, in effect the Chinese individual would be using EU data protection law as a vehicle to bring a claim against the US entity. The judgment therefore potentially applies EU data protection law to the entire Internet, a situation that was not foreseen when the Directive was enacted (as noted by the Court in paragraphs 69-70 of its 2003 Lindqvist judgment). It could lead to forum shopping and "right to be forgotten tourism" by individuals from around the world.

It is likely that the judgment will be interpreted more restrictively than this. For example, the UK Information Commissioner's office has announced that it will focus on "concerns linked to clear evidence of damage and distress to individuals" in enforcing the right to be forgotten.[358]

In any event, the Court's lack of concern with the territorial application of the judgment demonstrates an inward-looking attitude that fails to take into account the global nature of the Internet. It also increases the need for enactment of the proposed Regulation, in order to provide some territorial limits to the right to be forgotten.[359]

There is understandable discomfort concerning implementation of this ruling by Google and other intermediaries. It applies to 500 million European citizens whose data are strewn across billions of webpages. When Google first responded with an online complaint form allowing individuals to identify "irrelevant, outdated, or otherwise inappropriate" links, apparently 40,000 claims were made within the first six days, with another 30,000 in the month following.[360]

The risk is that, in order to manage the interests recognised in the ruling at scale, powerful but blunt tools may be deployed. Such tools, it is feared, may serve the interests of disinformation, rather than better information and more social cohesion.

We are likely to see more and more automated requests, with some people using specially developed intermediary reputation services that will perform rapid searches on the users' names, automatically categorizing results as negative, neutral or positive, and then acting as the users' agents to file automatic takedown requests.

---

358 Wright Tremaine D., UK gives search engines time to comply with 'right to be forgotten', May 23, 2014, https://www.lexology.com/library/detail.aspx?g=ad5225dc-5e52-45fe-b3b0-6681681bee3a

359 The right to be forgotten and the global reach of EU data protection law, http://concurringopinions.com/archives/2014/06/the-right-to-be-forgotten-and-the-global-reach-of-eu-data-protection-law.html

360 A manifesto for the future of the 'right to be forgotten' debate, http://www.theguardian.com/technology/2014/jul/22/a-manifesto-for-the-future-of-the-right-to-be-forgotten-debate

This could result in a large volume of requests untouched by human hands, including those of the requester.[361]

Today, episodes of our lives in the infosphere appear as digital traces across sources beyond our control. As those traces grow ever larger and move towards near complete reflection and inspection of our lives, it is important that we reflect carefully on how this information and its sedimentation can be pro-actively and safely managed.[362]

Google has a market share of more than 80% of Europe's search engine market, according to research firm comScore. The company already voluntarily removes search results worldwide if requests are made under US law.[363]

The judgment applies to all search engines operating within the European Union. However, in practice that means Google, given that 90 percent of all online searches there use Google's search engine.

Google and other commentators listed number of problems behind Right to be forgotten:

- Problem 1: This is logistically complicated, not least because of the many languages involved and the need for careful review.
- Problem 2: Because the court's ruling applies only within Europe, it will mean some fragmentation of search results. That is, Europeans and Americans will see slightly different versions of the Internet
- Problem 3: There will be serious technological challenges. It seems aspirational, not a reality, to comply with such a standard. The re-engineering necessary to implement the right to be forgotten is significant.
- Problem 4: Wikipedia founder Jimmy Wales, who has been an outspoken critic of the ruling, summarized it for The Associated Press as a "technologically incompetent violation of human rights." He said it amounts to censorship, and he predicted it will ultimately be scrapped. "The danger is that search engines now are faced with an uncertain legal future which may require them to censor all kinds of things when someone thinks it is 'irrelevant'," Wales said.

Some commentators say that the right to be forgotten is a great idea philosophically, but it is wrong to put the onus on Google or Facebook. Apparently, these companies have no idea where all our data is, and this is not their job. Consumers need tools with the ability to add expiration dates to their personal data.[364]

361 Zittrain J., Europe's Bad Solution to a Real Problem, December 5, 2014, https://www.usnews.com/debate-club/should-there-be-a-right-to-be-forgotten-on-the-internet/europes-bad-solution-to-a-real-problem

362 A manifesto for the future of the 'right to be forgotten' debate, http://www.theguardian.com/technology/2014/jul/22/a-manifesto-for-the-future-of-the-right-to-be-forgotten-debate

363 EU court ruling opens door for 'right to be forgotten' on the Internet, http://www.euractiv.com/sections/infosociety/eu-court-ruling-opens-door-right-be-forgotten-internet-302094

364 Google 'Right To Be Forgotten' Ruling Unlikely to Repeat in U.S., http://www.nbcnews.com/tech/internet/google-right-be-forgotten-ruling-unlikely-repeat-u-s-n114731

The ruling only applies in the EU, meaning Googling the same person in the United States and dozens of other countries could look much different than it does from Europe. However, although the court ruling only applied to 28 countries in the EU, Google is extending the right to be forgotten to four other countries — Iceland, Liechtenstein, Norway and Switzerland. More than 500 million people live in the area affected by Google's potential purge of personal information from its European search results.[365]

Google will need to build up an army of removal experts in each of the 28 European Union countries, including those where Google does not have operations. Whether those experts merely remove controversial links or actually judge the merits of individual takedown requests. The company has said it is disappointed with the ruling, which it said differed dramatically from a non-binding opinion by the ECJ's court adviser last year, which noted that deleting information from search results would interfere with freedom of expression.[366]

There is an important point to be addressed as to the wisdom of the Court to leave it entirely in Google's hands to decide what complaints should be upheld and which should not. Nonetheless, Google is not deleting data. Google has not been asked to delete data. The websites in question remain findable in Google. On the other hand, Google deletes hundreds of millions of search results globally on the basis of US law and has an agreement with the White House to take punitive action globally, outside the rule of law, against online services suspected of breaching US intellectual property law.[367] According to edri.org - Pages will not be removed as a result of this ruling. This ruling does not create a right to be forgotten.[368]

Right to be Forgotten is not censorship. It simply restores an element of privacy by obscurity to the digital age, restoring a balance between the right to know and privacy. The original published article is not removed or altered; it remains on the Internet. The link from a person's name may be removed, but the article can still be accessed using other search terms.[369]

It also set off conflicts such as those between privacy and freedom of the press.[370] While in Europe, for example German law confirms the duty to secure the best possible privacy protection for persons concerned, freedom of the press generally

365 Google Opens Privacy Web Form For 'Right To Be Forgotten' Requests, http://www.nbcnews.com/news/world/google-opens-privacy-web-form-right-be-forgotten-requests-n118211

366 Google Gets Search Take-Down Requests After European Court Ruling, http://www.nbcnews.com/tech/tech-news/google-gets-search-take-down-requests-after-european-court-ruling-n105496

367 https://torrentfreak.com/bad-google-dmca-takedown-is-hurting-us-hosting-site-says-140330/ and http://www.whitehouse.gov/blog/2013/07/15/coming-together-combat-online-piracy-and-counterfeiting

368 Google's right to be forgotten – industrial scale misinformation?, https://edri.org/forgotten/

369 Simpson J., Restore 'Privacy by Obscurity', December 4, 2014, https://www.usnews.com/debate-club/should-there-be-a-right-to-be-forgotten-on-the-internet/restore-privacy-by-obscurity

370 European Court of Human Rights, Von Hannover v. Germany, 294 Eur. Ct. H.R. (2004).

prevails over privacy in the United States. The Wikipedia case is an illustration of the diverging approach.[371] In 1990, two people killed Walter Sedlmayr, an actor, and were sent to jail. They were released from prison in 2007 and 2008 and almost immediately tried to have their names removed from prior publications and to prohibit any further reference to their past. Their lawyer claimed that they should be rehabilitated and be able to lead their life without being publicly stigmatized.[372] For exactly this reason, the editors of Wikipedia's German-version deleted all mention of the two men in an article about Walter Sedimayr. Both have also sued the Wikipedia Foundation to have their names removed from the English-language version. In the United States, the reaction thus far has been rather disinterested comments such as the lapidary remark that every Justice on the United States Supreme Court would agree that the Wikipedia article is easily, comfortably protected by the First Amendment.[373]

Not all Americans criticize the Right to be Forgotten. The European Union and the United States are in sync when it comes to the right to be forgotten, though less so regarding the operationalization of this right.[374]

2014 survey found that 61 percent of U.S. residents supported the right to be forgotten in general,[375] only 39 percent wanted a European-style blanket of the right, without restrictions.[376] According to one survey, many Americans, echoing common viewpoints in the European Union, felt that the appeal of the right to be forgotten law is not based on fears of the negative consequences of search results but rather, is based on a belief in the individual's right to privacy.[377] Many respondents in the United States feel that there's not much we can do to find out which aspects of our personal lives are being bought and sold by data brokers.[378]

---

371 Schwartz J., Two German Killers Demanding Anonymity Sue Wikipedia's Parent, N.Y. TIMEs, Nov. 13, 2009, at A13; Evgeny Morozov, Free Speech and the Internet, INT'L HERALD TRIB., Nov. 28, 2009, p. 8.

372 Schwartz J., Two German Killers Demanding Anonymity Sue Wikipedia's Parent

373 Schwartz J., Two German Killers Demanding Anonymity Sue Wikipedia's Parent

374 De Mooy M., Rethinking Privacy Self-Management and Data Sovereignty in the Age of Big Data. Considerations for Future Policy Regimes in the United States and the European Union, 2017, https://cdt.org/files/2017/04/Rethinking-Privacy_2017_final.pdf, p. 22.

375 Attitudes on Data Protection and Electronic Identity in the European Union, European Commission 7 (June 2011). http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf, Humphries, Daniel "US Attitudes Toward the 'Right to Be Forgotten.'" Software Advice, Sept. 5, 2014. www.softwareadvice.com/security/industryview/right-to-be-forgotten-2014/.

376 Kemp C., "61 Percent of Americans Support the Right to Be Forgotten as California Enacts New Law." The Whir (Sept. 29, 2014). www.thewhir.com/web-hosting-news/61-percent-americanssupport-right-forgotten-california-enacts-new-law

377 Humphries D., "US Attitudes Toward the 'Right to Be Forgotten.'" Software Advice, Sept. 5, 2014. www.softwareadvice.com/security/industryview/right-to-be-forgotten-2014/

378 Lafrance A., "Why can't Americans find out what big data knows about them?" The Atlantic (May 28, 2014). www.theatlantic.com/technology/archive/2014/05/why-americans-cant-find-outwhat-big-data-knows-about-them/371758/

There is indeed a strong voice asking for same level of protection in US. In times when it is believed that American companies are working hard on protecting the privacy, John Simpson, a consumer advocate for Consumer Watchdog says EU Right to be Forgotten is an important way to protect privacy in the digital age. Google and the other search engines like Microsoft's Bing and Yahoo should, if they care about users' privacy as they claim, extend this important protection to Americans. Quoting after John Simpson, Americans apparently support the right to be forgotten. A poll[379] by Software Advice, Inc. found that 61 percent of Americans believe some version of the right to be forgotten is necessary. Thirty-nine percent want a European-style blanket right to be forgotten, without restrictions. 47 percent were concerned that irrelevant search results can harm a person's reputation.

Importance of Right to be Forgotten, the idea that privacy can be protected by obscurity, comes from the fact that before the digital age and the Internet a balance between the need for public records and personal privacy was maintained by the difficulty in gathering information from disparate and distant files as well as the tendency of humans to forget. Google and its search algorithms do not allow that now. The right to be forgotten offers a clear path forward to help protect our privacy in the digital age. Americans deserve the same right to be forgotten that is now being invoked in Europe. Companies like Google that repeatedly claim to care about users' privacy should be ashamed that they are not treating people on both sides of the Atlantic the same way.[380]

As the issue of Right to be Forgotten was and is still broadly discussed in US, here are some statements from US security experts and advisors about EU legislation:

- Joseph Steinberg[381]: I support the legislation – if it's done right. The concept might be appropriate, but the details aren't worked out. For example: Who makes the decision? Right now, in Europe, Google and other search engines are making the decision of what to block – but it should be an outside party. There are no standards; there are no criteria; a lot of this law is very vague. A European-style blanket right to be forgotten may not be the right way, but these problems need to be addressed. Some may get addressed because of civil lawsuits; some may get addressed by legislation; some may just remain unaddressed; and some may get addressed by search engines improving their algorithms.
- Andy Kahl[382]: There is a positive aspect to this debate: It's bringing the notion of data management into greater light. But we are entering an age where trading data about individuals is the status quo. It bothers me to think about

379 http://www.softwareadvice.com/security/industryview/right-to-be-forgotten-2014/

380 Op-Ed: Restore 'Privacy by Obscurity', http://www.usnews.com/debate-club/should-there-be-a-right-to-be-forgotten-on-the-internet/restore-privacy-by-obscurity

381 Security expert, regular Forbes contributor and CEO of SecureMySocial, a service that instantly warns clients if "problematic" material appears about them online

382 Senior director of transparency at Ghostery, one of the world's top privacy tools for Web browsers

all the time and energy we put into [trying to figure out] how to Band-Aid over that – as opposed to educating consumers about how to manage the way their data is being shared with gigantic corporations. There is precedent for the upcoming California law, granting underage Web users the right to have content they have posted online removed, because juvenile criminal records are often sealed – so it's conceivable to see that extending to general online information. A blanket law, like in Europe, would be complicated; the freedom-of-speech issue would be a big hurdle. But a lot of these penalties in Europe are being levied against U.S. companies, and I don't think it would be crazy to consider that someone might suggest that practices companies are already being forced to follow in Europe should also be adopted in America.

- Heather Buchta[383]: I think, in certain contexts, the justification is there to impose an obligation like this. For example, as the parent of two small children, I see why laws like the one in California are developing. It's incredibly difficult to do this from a legal perspective. Our existing set of laws and regulations do favour free speech; they do allow people to post opinions and allow the free exchange of information. So, basically, if there's something posted online and it's accurate but perhaps not flattering, under existing laws, you're going to be hard-pressed to find a way to get it removed.
- Pavel Krcma[384]: The right to be forgotten is an excellent example of the huge gap between how the world is perceived by lawmakers and how current technology works. The first problem is that there's nothing like, "Let's forget everything in the past." Everything I did in the past counts. It simply happened, and I have to live with the consequences. But things are more complicated now. We have technology [hat is able to record and search in all the details of our lives, and people even actively insert sensitive data into various services. I'm afraid that if the government decides to do it, they will be able to slowly change the rules towards this legislative direction. I agree that it's improbable that the same law as exists in the EU will be implemented in the USA, but there are many ways to implement a rule. The most important thing is [whether] enough citizens are against such rules, to stop any attempt from the very start. I'm not sure if we are there.

No doubt the debate will continue, as the consequences of the European law influences rest of the world. Even those experts who disagreed with the law agreed that it was at least an attempt to deal with serious issues of individual privacy in an age when we all lead part of our lives online. Businesses, governments and individuals

383 Partner, Quarles and Brady LLC, whose legal practice covers e-commerce, software and technology

384 Chief technology officer at password-manager Sticky Password and former head of Viruslab for AVG Technologies

will have to negotiate this tricky terrain as technology races ahead; whether the results will satisfy anyone remains to be seen. Additionally, the comments of these experts suggest that some of them still do not fully understand the idea behind right to be forgotten. Maybe the biggest problem here is the name itself, which is fooling even those who are supposed to understand legislation by its content.[385]

Marc Rotenberg[386] also advocates for the right saying that the right to privacy is global. Search engines provide a valuable service to Internet users. On that point there is no dispute. However, that does not mean they are above the law or ethical responsibilities. Simply because private information can be found on the Internet does not mean it should be made widely available. The European Court of Justice decided that commercial search firms should remove links to private information when asked. That policy will only work if the search company removes the links across all domains for which it provides search.[387]

Google's position on this issue makes little sense. The company could not reasonably claim to protect a US citizen's credit card details by removing links to the private information from only the google.us domain. Similarly, Google does not address the privacy problem elsewhere by only removing links from search provided for only one country. The solution is simple: Google should remove all links to private information when requested to do so.[388]

In the light of Google case, some feel that it is time for the US government to step up and defend US high tech internet companies such as Google, Yahoo and Microsoft against the protectionism embedded in the European Union's right to be forgotten principle. US clearly feel that EU has upped the ante, and in effect attacked US and their high-tech companies. A group of regulators implementing the court decision issued a set of guidelines that would expand the right to be forgotten worldwide. Google and others would have to expunge contested links throughout the entire global Internet. This is an outrageous extraterritorial demand that, to add insult to injury, proposes to utilize U.S. companies to institute worldwide censorship. There is an idea that it should be challenged and ultimately vetoed by other governments, particularly the US government. The critics of Right to be forgotten goes so far, there is an opinion saying, the lesson for the United States is that Europe must be made aware that it will pay a heavy price for its reckless extraterritorial action.[389]

---

385 U.S. Attitudes Toward the 'Right to Be Forgotten', IndustryView | 2014, http://www.softwareadvice.com/security/industryview/right-to-be-forgotten-2014/

386 President of the Electronic Privacy Information Center (EPIC)

387 European Action Focuses Debate On Right To Be Forgotten, http://www.consumerwatchdog.org/blog/european-action-focuses-debate-right-be-forgotten

388 The Right to Privacy Is Global, http://www.usnews.com/debate-club/should-there-be-a-right-to-be-forgotten-on-the-internet/the-right-to-privacy-is-global

389 The Misbegotten 'Right to Be Forgotten', http://www.usnews.com/debate-club/should-there-be-a-right-to-be-forgotten-on-the-internet/the-misbegotten-right-to-be-forgotten

Europeans take a very different view of free speech than Americans do, largely because US have the First Amendment and EU not. Europeans routinely ban speech that would be legal and acceptable in the US, such as hate speech.[390] A broad legal right to be forgotten could never be accepted in US. US law, of course, provides legal recourse against falsehoods that are damaging. However, as to truthful speech, other than gross invasions of privacy, actual threats and copyright infringement, the First Amendment does not allow legal censorship. Up to now, the US and EU approaches have co-existed, with the understanding that EU rules apply in the EU, and US rules apply in the US. But EU regulators have said they believe the European court's right to be forgotten rule applies to search engine results that appear on Google.com, the search engine used in the US to access information, and also available as an alternative to local Google search sites in EU countries. The effect of that regulatory interpretation would be to apply the EU privacy rule that crosses our First Amendment barrier to searches on the .com domain that U.S. citizens use. In effect, US interprets it as if the EU propose to censor the Internet used by American citizens. As EU regulators seek to force search engines to apply the right to be forgotten by search results outside of the European Union, in eyes of Americans they may be opening the door to the suppression of legitimate and valuable information. At least in US understanding of this issue.[391]

According to US, the court's decision is both too broad and curiously narrow. It is too broad in that it allows individuals to impede access to facts about themselves found in public documents. In the light of American laws, this is a form of censorship, one that would most likely be unconstitutional if attempted in the US. Moreover, the test for removal that search engines are expected to use is so vague – search results are to be excluded if they are inadequate, irrelevant or no longer relevant – that search engines are likely to accede to most requests. However, the decision is considered to be oddly narrow in that it does not require that unwanted information be removed from the web. Therefore, nothing is being forgotten, despite the court's stated attempt to protect such a right.[392] I can agree on one thing with American commentators. What's once put in the Internet will never be forgotten. It is more about make the information less easily accessible, not visible to someone who is not willing to put more effort into digging after it.

In the wake of the decision by the European Court of Justice, search engine companies now face a potential avalanche of requests for redaction. Whatever the merits of the court's decision, Europe cannot expect to export its new approach to

390 McHangama J., Europe's Freedom of Speech Fail, July 7, 2016, https://foreignpolicy.com/2016/07/07/europes-freedom-of-speech-fail/

391 Europe Wants to Censor America's Internet, http://www.usnews.com/debate-club/should-there-be-a-right-to-be-forgotten-on-the-internet/europe-wants-to-censor-americas-internet

392 Don't Force Google to 'Forget', http://www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html

countries like the United States. Even in Europe, search engine users will no doubt cultivate the same Internet workarounds that Chinese citizens use to see what their government does not want them to see.[393]

According to Jonathan Zittrain[394] European Court of Justice has come up with a bad solution to a very real problem.[395]

Wikimedia Foundation also criticises Right to be Forgotten. The foundation which operates Wikipedia has issued new criticism of the right to be forgotten ruling, calling it unforgivable censorship. Speaking at the announcement of the Wikimedia Foundation's first-ever transparency report in London, Wikipedia founder Jimmy Wales said the public had the right to remember.[396]

Some more critics claim that the Court's analysis of the fundamental rights issues at stake is an example of what can be called[397] as the CJEU's self-referential and detached style of judgment that is largely unconcerned about the external impact and influence of its rulings" and that often fails to consider relevant materials from other jurisdictions. The Court emphasizes the right of individuals to remove their personal data from the results generated by search engines, but barely mentions the right to freedom of expression, and never refers at all to Article 11 of the Charter of Fundamental Rights. It also states, in paragraph 81, that the right to data protection generally overrides the interest of the general public in finding information relating to a data subject's name, while at the same time stating that the balance between the two must depend on the specific case at issue. The judgment requires data controllers, data protection authorities, and courts to strike a fair balance between these rights but gives almost no criteria for doing so.[398]

The judgment also seems inward-looking and represents a step backwards from the Court's Lindqvist judgment[399] of 2003, where it considered the implications for the Internet when interpreting the transborder data transfer restrictions of Article 25 of the EU Data Protection.

Advocate-General Jääskinen had recognized the implications of the case for the global Internet and the need to strike a correct, reasonable and proportionate

393 Don't Force Google to 'Forget', http://www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html

394 The George Bemis professor of law and professor of computer science at Harvard University, and co-founder of its Berkman Center for Internet & Society.

395 Europe's Bad Solution to a Real Problem, http://www.usnews.com/debate-club/should-there-be-a-right-to-be-forgotten-on-the-internet/europes-bad-solution-to-a-real-problem

396 How We'll Know the Wikimedia Foundation is Serious About a Right to Remember, http://concurringopinions.com/archives/2014/08/how-well-know-the-wikimedia-foundation-is-serious-about-a-right-to-remember.html

397 http://www.maastrichtjournal.eu/pdf_file/ITS/MJ_20_02_0168.pdf

398 http://www.maastrichtjournal.eu/pdf_file/ITS/MJ_20_02_0168.pdf

399 Case C-101/01, Lindqvist, ECLI:EU:C:2003:596, par. 69, http://curia.europa.eu/juris/showPdf.jsf?text=&docid=48382&doclang=EN

balance between the protection of personal data, the coherent interpretation of the objectives of the information society and legitimate interests of economic operators and internet users at large, an approach that the Court rejected.[400] The judgment does not mention even once the European Convention on Human Rights or the jurisprudence of the European Court of Human Rights in its reasoning.

Court seems to base its decision on what it views as the special data protection risks posed by Internet search engines.[401] Judgment would have benefited from a reference to the resolution of the UN Human Rights Council passed on 29 June 2012[402] that the rights to freedom of expression and to cross-border communication must apply in both worlds.

The judgment also raises important issues for determining the territorial extent of data protection rights. On its face, the judgment deals narrowly with the question of when an Internet service is established in the EU for jurisdictional purposes, but it opened the door to questions concerning the Directive's territorial scope that are left unanswered. For example, does the right to be forgotten extend to search engines operating under .com and other domains that are not EU-specific? And could individuals in regions outside Europe exercise such right with regard to searches that they carry out on search engines that are subject to EU law? These are just a few of the issues that will require further examination.[403]

The judgment has the potential to create a kind of EU Internet separate from the global Internet, with search results and other web content displayed differently in the EU from how they are in the rest of the world. This could adversely affect the right of EU individuals to receive information regardless of frontiers under Article 19 UDHR and Article 19 ICCPR.[404] The reason is, because Google has been following the judgement only when it comes to its European domains but not google.com or its other non-European domains.[405]

I would like to point out, that big portion of the debate regarding right to be forgotten seems to be suffering from misunderstanding of the decision. What we today know the right to be forgotten is not about having this kind of right. It is

400 OPINION OF ADVOCATE GENERAL JÄÄSKINEN delivered on 25 June 2013, Case C-131/12, par. 31

401 Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos [es], Mario Costeja González, ECLI:EU:C:2014:317, par. 36-38, 80

402 The promotion, protection and enjoyment of human rights on the Internet, The Human Rights Council, A/HRC/20/L.13 (June 29, 2012), http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A.HRC.20.L.13_en.doc

403 More on these topic in Chapter 5

404 The Court of Justice of EU's Judgment on the "Right to be Forgotten": An International Perspective, http://www.ejiltalk.org/the-court-of-justice-of-eus-judgment-on-the-right-to-be-forgotten-an-international-perspective/

405 Scott M., Google details requests in Europe „to be forgotten", International New York Times (10 October 2014) 16.

rather a qualified right to be de-indexed, or even qualified right not to figure in a public index of search results.[406] Additionally, there is a concern about the balance between privacy and free speech interests. According to Lee Bygrave, the Court devoted surprisingly little attention to freedom of expression and was remarkably silent about the broad implication of its decision for use of the Internet as a global communications network.[407]

The situation might be very serious considering two facts. First of all, Google has already experience in handling massive amounts of de-indexation requests related to infringement of intellectual property rights. Secondly, only over the first five months after the decision, Google received over 143,000 requests related to 491,000 links.[408] Together it shows how massive it the problem and how many, possible, information can become, at least on the first look, hard to find in European Internet.

Of course, it this situation there is a question if search engine operators are suitably placed to engage in the delicate balancing. One thing is to be capable, as the case with infringement of intellectual property rights shows, the other is should they be responsible on that. Fortunately, at least European data protection authorities have shown willingness to assist by drawing up guidelines to ensure consistency in assessing de-indexation requests.

It is no doubt that CJEU decision is not surprising or unexpected. The Court shows that personal data protection is a fundamental right under EU law[409] and data privacy must be treated on an equal par with other human rights, such as freedom of expression. In addition, it must be remembered that disagreement on Right to be Forgotten between EU and US comes from the fact that European approach to data privacy is more restrictive and in general different in many aspects.[410]

It is important to mention that, because in US, freedom of expression has much broader interpretation[411] than in EU, there is an impression that American law is unfamiliar to concept of right to be forgotten. In fact, in US similar solutions exist, and can portray by two cases – *Melvin v. Reid*[412] and *Sidis v. F-R Publishing Corporation*[413].

In the first case, the plaintiff was an ex-prostitute who had been involved in a murder but was acquitted. She completely abandoned her former life and hoped

406 Bygrave L., A Right to be Forgotten? [in:] L. A. Bygrave, A. G. B. Bekken (ed.), Yulex 2004, Oslo, p. 94.

407 Ibid, p. 96.

408 Ibid.

409 Article 8 of the Charter of Fundamental Rights of the European Union [2010] OJ C83/389; Article 16 of the Treaty on the Functioning of the European Union [2010] OJ C83/47.

410 More in point 2.5 of this Dissertation.

411 Barbas, The Death of the Public Disclosure Tort: A Historical Perspective, 22 Yale J.L. & Human. 171 (2010) and New York Times Co. v. Sullivan, 376 U.S. 254 (1964)

412 Melvin v. Reid, 112 Cal.App. 285, 297 P. 91 (1931).

413 Sidis v F-R Publishing Corporation 311 U.S. 711 61 S. Ct. 393 85 L. Ed. 462 1940 U.S.

for new start. Until in the movie The Red Kimono, without her knowledge or permission, her past was revealed. According to the court, plaintiff had right to pursue and obtain happiness and this right by its very nature includes the right to live free from the unwarranted attack of others upon one's liberty, property, and reputation. Any person living a life of rectitude has that right to happiness which includes a freedom from unnecessary attacks on his character, social standing, or reputation.

However, in the second case, *F-R Publishing Corporation,* the decision was different. Here, the plaintiff was famous child prodigy[414], who as an adult preferred not to be known for his childhood achievements. The New York Times described his past, publishing personal story of Mr Sidis. According to the court, right to be forgotten, or however we want to call it in this case, does not apply, because the misfortunes and frailties of neighbours and public figures are subject of considerable interest and discussion to the rest of the population". It shows that the right to be forgotten has its boundaries; it is not absolute and does not allow the generic deletion of information. It is about a balance between individual right to privacy and the right to be informed of aspects of public interest.

In another case, *Briscoe v. Reader's Digest Association, Inc.*[415], the court distinguished between cases in which, by reason of the nature of facts, and individual whose name is fixed in the public's memory never becomes an anonymous member of the community again and the different cases in which identification will no longer serve to bring forth witnesses or obtain succour for victims. Unless the individual has re-attracted the public eye to himself in some independent fashion, the only public interest that would usually be served is that of curiosity.

No matter how we look at right to be forgotten, from EU or from US perspective, judging this right has to be taken into the discussion of ICT companies and social media. European concept of this right has been highly criticised by media, scholars, and US companies. As I am mostly interested in the doings of ICT dominant companies, I will focus on their argumentation. These companies promote the idea that sharing information is a social norm and that privacy or forgetting is an outdated concept. At the same time, they are collecting vast amounts of data in order to profile their users and for marketing purposes.[416] It leads to great data concentration and in nowadays, the data represents money and power. No wonder that biggest ICT companies are so much against any changes in privacy legislation.

414 Mr Sidis at age of eleven lectured to distinguished mathematicians on the subject of Four-Dimensional Bodies and when he was sixteen, he graduated from Harvard College.

415 Briscoe v. Reader's Digest Association, Inc. , 4 Cal.3d 529 [L.A. No. 29813. In Bank. Apr. 2, 1971.]

416 Mantelero A., The EU Proposal for a General Protection Regulation and the roots of the 'right to be forgotten', Computer Law & Security Review 29 (2013), p. 234.

This kind of approach could eventually lead to the end of privacy. What is more, there is a theory that if everyone has possibility to know everything about the others and every aspect of their past life, probably overload of information will become the most important limit to privacy abuse.[417]

However, it is rather impossible with biggest companies collecting almost unlimited amounts of data. They can manage big data and extract value from it in an exclusive way.

Some more information about Right to be Forgotten in Chapter 5.

417 Ibid.

3. THE REALITY BACKGROUND

3.1. Virtual Reality as new Reality

Now there is a place to explain a bit why these databases are so big. That leads to the question "How virtual is virtual world and why is it important?".

In 1995 for the first time, I connected to the Internet on my home PC. Soon after I created my first e-mail address. I registered at one of two existing at that time Polish portals. Of course, I have given my name and surname, city I lived in and date of birth. Additionally, some other personal information like my hobbies and interests. Today I know that I was not a big of a deal. Those details that I gave could not have been used for a long time. There was no Facebook, Twitter or even Google. These data, even if stored was useless. Now let us move to 2015 and create an e-mail, giving in a process same information - name, surname, address, date of birth, hobbies. With this e-mail address we can register to literally hundreds of thousands of pages including of course Facebook or Twitter and to any online shop. All these actions, together with our IP address, web pages we visit every day, create a kind of profile of us. Profile which is far from being virtual - it consists all real details of us - address, hobbies, name, our friends, places we visit, how much money we spend, etc. Adding this to the fact that people in internet are willing to share information about them, we have an answer for two questions: "How virtual is virtual world and why is it important?" and "Why databases are so big".

World of the Internet may not be material but in my opinion, it is no longer virtual. This is important because in this "no longer virtual world" people are freely without proper understanding sharing information, which they wouldn't in "real world". My favourite example of this situation is Facebook application called "My Calendar". Users are invited to accept and use this application by their friends. Because invitation comes from friends, not Facebook itself, many users do not see the risks. By accepting My Calendar, we agree to share name and surname, Facebook identification number, e-mail, age and date of birth, sex, information about our hardware, favourite websites, information about friends, favourite pages on Facebook, the results achieved in the games, time spent on gaming, and even more listed in statue of My Calendar:

"Finally, any time you access the Service, We May collect aggregate information Including but not limited to internet protocol addresses, browser type, browser language, Referring / exit pages and URLs, platform type, number of clicks, domain names, landing pages, pages viewed and the order of Those pages, the amount of time spent on Particular pages, and the date and time of this activity."

3.2. The shift towards new society

With the little exaggeration, we call the 21st century the age of networks.[418]

Following that words van Dijk states that networks are becoming the nervous system of our society, with having expected influence on out social live, *higher than construction of roads in the past*. Network Society, together with older concept Information Society, became a way to define modern society, society of *high level of information exchange and use of information and communication technologies*.[419]

Van Dijk defines information society as a modern type of society in which the information intensity of all activities has become so high that this creates:

- an organization of society based on science, rationality and reflexivity;
- an economy with all values and sectors even the agrarian and industrial sectors, increasingly characterized by information production;
- a labour market with majority of functions largely or completely based on tasks of information processing requiring knowledge and higher education (hence, the alternative term *knowledge* society);
- a culture dominated by media and information products with their signs, symbols and meanings.

The Network Society he defines as:

> A modern type of society with an infrastructure of social and media networks that characterizes its mode of organization at every level: individual, group/organizational and societal. Increasingly, these networks link every unit or part of this society (individuals, group and organizations). In western societies, the individual linked by networks is becoming the basic unit of the network society. In eastern societies, this might still be the group (family, community, work team) linked by networks.

It could be said that the Network Society is built onto the foundations of Information Society and focuses on networks and their organizational forms.

The big spokesperson for network society is without a doubt Manuel Castells. In the interview from 2001,[420] he defined Network Society as follows:

> The network society itself is, in fact, the social structure which is characteristic of what people had been calling for years the information society or post-industrial society. Both "post-industrial society"

418 Van Dijk J., The Network Society, Sage Publications 2012, 3rd Edition, p. 2.

419 Ibid., p. 23.

420 Conversation with Manuel Castells, p. 4, http://globetrotter.berkeley.edu/people/Castells/castells-con4.html

> and "information society" are descriptive terms that do not provide the substance, that are not analytical enough. So, it's not a matter of changing words; it's providing substance. And the definition, if you wish, in concrete terms of a network society is a society where the key social structures and activities are organized around electronically processed information networks. So it's not just about networks or social networks, because social networks have been very old forms of social organization. It's about social networks which process and manage information and are using micro-electronic based technologies.

Frank Webster, in his *Theories of the Information Society*, rather puts the Network Society aside. Of course, he does not ignore it the existence of the term, but also does not mention van Dijk's ideas. In the chapter dedicated to Manuel Castells work, he seems to treat Network Society as one part of Information Society, the part merely being focused on importance of networks, and not the completely new idea, let alone new or higher level of society.[421]

I mention that Network Society may be the completely new idea, or higher level of describing and interpreting the changes in modern society, as I follow Ahti Saarenpää. He is a big and consistent advocate for the idea that we should forget about Information Society – *The age of the information society is over*.[422] The time has come to tell the world that we are now living in the Network Society - *The network society has been a big step forwards from what in fact was a very static information society.*[423] One of the reasons to abandon Information Society in favour of Network Society is not the end of information, but increasing role of networks. The society is now more than ever reliant on infrastructure rather than on information.[424]

This short introduction to Network Society is now followed by my idea that our society nowadays is simply trapped in the network. Is it only Network Society or maybe Society trapped in the Network? It leads to another question: *Do you ever wonder if you use the net, or the net uses you?*[425]

Without a doubt society today became dependent on technology and offered by it infrastructure. We reached the point of no return. We need it for work (ex. Driver's license databases), to live (ex. Health care databases), for pleasure (ex. Facebook). Large multinational companies are pinning down consumers' preferences, lifestyle

421 Webster F., Theories of the Information Society, 4th Edition, Routledge 2014, p. 106-136.

422 Saarenpää A., Legal welfare and legal planning in the network society, [in:] Barzallo J., Tellez Valdes J., Olmedo P., Amoroso Fernandez Y. (eds.), XVI Congreso Iberoamericano de Derecho e Informatica, p. 57.

423 Network Society as a Paradigm for Legal and Societal Thinking (NETSO), http://www.ulapland.fi/InEnglish/Units/Faculty-of-Law/Institutes/Institute-for-Law-and-Informatics/NETSO-Project

424 Saarenpää A., Openness, Access, Interoperability and Surveillance...

425 http://networksociety.org/about

choices and general web behaviour.[426] No matter if we share the information freely, because of using social media pages, or online shopping or we share it as a legal requirement, little we give a thought to it. Very often, we do not see any issue in sharing most personal details about us, including phone number, home address, etc. in the Internet. Additionally, social media pages are having tools to encourage us to reckless behaviour, for example by giving us more personalization, which leads to emotional attachment to our Internet profiles and as a consequence to share even more.[427] What we share became marketable good for companies and invaluable source for mass surveillance agencies.

3.3. Internet

The internet is a globally connected network system that uses TCP/IP to transmit data via various types of media. The internet is a network of global exchanges – including private, public, business, academic and government networks – connected by guided, wireless and fiber-optic technologies.[428]

The Internet has revolutionized the computer and communications world like nothing before. The invention of the telegraph, telephone, radio, and computer set the stage for this unprecedented integration of capabilities. The Internet is at once a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location. The Internet represents one of the most successful examples of the benefits of sustained investment and commitment to research and development of information infrastructure.

The Internet today is a widespread information infrastructure, the initial prototype of what is often called the National (or Global or Galactic) Information Infrastructure. Its history is complex and involves many aspects – technological, organizational, and community. And its influence reaches not only to the technical fields of computer communications but throughout society as we move toward increasing use of online tools to accomplish electronic commerce, information acquisition, and community operations.[429]

426 Rowland D., Kohl U., Charlesworth A., Information Technology Law, Fourth Edition, Routledge 2002, p. 4.

427 Barnes S. B., A privacy paradox...

428 The terms internet and World Wide Web are often used interchangeably, but they are not exactly the same thing; the internet refers to the global communication system, including hardware and infrastructure, while the web is one of the services communicated over the internet.

429 Leiner B. M., Cerf V. G., Clark D., Kahn R., Kleinrock L., Lynch D. C., Postel J., Roberts L. G., Wolff S., Brief History of the Internet, 1997, https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf, p. 3.

The Internet is now about twenty-seven years old — measured from the time that the federal government decided to release it from its governmental sponsorship and control in the research and national-security communities and launch it into the private sector as a global information infrastructure. As of June 2019, 58.8% of the world's population has internet access.[430]

No one owns the entire Internet. Instead, the Internet is a collection of concepts, technical protocols and format standards that permit thousands—indeed millions—of owners of communications channels and routers to exchange traffic with each other.

One of the Internet architectural principles: The overarching rationale, a result of honoring the first three, is that no central gatekeeper should exert control over the Internet. This governing principle allows for vibrant user activity and creativity to occur at the network edges. In such an environment, entrepreneurs with new ideas for applications need not worry about getting permission for their inventions to reach end-users. Closed networks like cable video systems provide a sharp contrast. There, network owners control what consumers can see and do.[431]

One of the most successful early search engines was AltaVista, developed by Digital Equipment Corporation and introduced in 1995.[432] By the beginning of 1999, Google began to emerge as a search engine with a better search algorithm,[433] and by the mid-2000s it dominated the search engine industry.[434]

The Internet cannot and should not be fully regulated, but attempts should be made in the area in which this is possible. [435] Figuring out how the Internet should be regulated involved figuring out how prescriptive and adjudicatory jurisdiction[436] should work.[437] Legal jurisdiction is fundamentally local, aligned with the boundaries of sovereign power; the Internet is inherently global, crossing sovereign boundaries. The Computer Science and Telecommunications Board of the National Academy of Sciences convened a committee on "Global Networks and Local Values" in the

430 https://www.internetworldstats.com/stats.htm

431 Perritt H. P. Jr., Sources of Rights to Access Public Information, 4 WM. & MARY BILL RTS. J. 179 (1995).

432 AltaVista: A Brief History of the AltaVista Search Engine, WEBSEARCHWORKSHOP, http://www.websearchworkshop.co.uk/altavista_history.php

433 Google History, GOOGLE, http://www.google.com/about/corporate/company/history.html

434 Google: A Brief History of the Google Search Engine, WEBSEARCHWORKSHOP, http://www.websearchworkshop.co.uk/google_history.php

435 O'Reilly C., Finding jurisdiction to regulate Google and the Internet, European Journal of Law and Technology, vol. 2, no. 1, 2011, p. 8

436 Known as "personal jurisdiction" in the United States. See Michael D. Ramsey, International Law Limits on Investor Liability in Human Rights Litigation, 50 HARV. INT'L L.J. 271, 296 (2009).

437 Prescriptive jurisdiction refers to the power to make rules. Adjudicatory jurisdiction refers to the power to adjudicate alleged rule violations. See Graeme B. Dinwoodie, Developing a Private International Intellectual Property Law: The Demise of Territoriality?, 51 WM. & MARY L. REV. 711, 785 (2009) (distinguishing between prescriptive and adjudicatory jurisdiction)

late 1990s to consider these questions.[438] The committee's report[439] stopped short of making policy recommendations, but observed that "extraterritorial enforcement of national laws is possible in principle, [but] this generally presupposes that the nation-state can exercise jurisdiction over some element of the transnational activity—e.g., by seizing local property or by restricting access to its market."[440]

At the turn of the century, the Hague Conference on Private International Law undertook an effort to negotiate an international convention on adjudicatory jurisdiction and transnational enforcement of judgments in the international e-commerce context.[441] Expert groups convened by the conference[442] considered the idea of "targeting" as a principle for localizing Internet activity: targeting consumers in a particular country would support jurisdiction; unsophisticated sites not engaging in targeting would not be subject to jurisdiction elsewhere based on the web site alone.[443]

The entertainment industry favoured expansive jurisdictional rules because they wanted to be able to sue alleged copyright infringers in United States courts.[444] The Internet industry, particularly internet service providers (ISPs), wanted restrictive jurisdictional rules because they wanted to insulate themselves from litigation in foreign forums.[445] The French Yahoo! case was on everyone's mind.[446] Because

438 Global Networks and Local Values, COMPUTER SCI. & TELECOMM. BD., http://sites.nationalacademies.org/CSTB/CompletedProjects/CSTB_042333

439 NATIONAL ACADEMY OF SCIENCES NATIONAL RESEARCH COUNCIL, GLOBAL NETWORKS AND LOCAL VALUES: A COMPARATIVE LOOK AT GERMANY AND THE UNITED STATES (2001), available at http://www.nap.edu/catalog/10033.html.

440 NATIONAL ACADEMY OF SCIENCES NATIONAL RESEARCH COUNCIL, GLOBAL NETWORKS AND LOCAL VALUES: A COMPARATIVE LOOK AT GERMANY AND THE UNITED STATES (2001), available at http://www.nap.edu/catalog/10033.html.

441 Press Release, Hague Conference on Private International Law, Geneva Round Table on Electronic Commerce an Private International Law (Sept. 2, 2001), available at http://www.hcch.net/upload/wop.press01e.html.

442 Hague Conference on Private International Law, Electronic Commerce and the Internet (Press Release Including Conclusions and Recommendations) (Sept. 2, 1999) (announcing round table of experts in Geneva), http://www.hcch.net/index_en.php?act=events.details&year=1999&varevent=63; HAGUE CONFERENCE ON PRIVATE INTERNATIONAL LAW, ELECTRONIC COMMERCE AND INTERNATIONAL JURISDICTION (Catherine Kessedjian, ed., 2000), available at http://www.hcch.net/upload/wop/jdgmpd12.pdf

443 HAGUE CONFERENCE ON PRIVATE INTERNATIONAL LAW, ELECTRONIC COMMERCE AND INTERNATIONAL JURISDICTION (Catherine Kessedjian, ed., 2000), http://www.hcch.net/upload/wop/jdgmpd12.pdf

444 Brand R. A, Intellectual Property, Electronic Commerce and the Preliminary Draft Hague Jurisdiction and Judgments Convention, 62 U. PITT. L. REV. 581, 594–97 (2001)

445 ibidem 597–98

446 In the Yahoo! case, a French court had ordered Yahoo! to block access to materials on Nazism that violated French law. See Yahoo! Inc. v. La Ligue Contre Le Racisme, 433 F.3d 1199, 1202–03 (9th Cir. 2006) (en banc) (holding that the district court lacked personal jurisdiction; summarizing procedural history). Yahoo! unsuccessfully argued that "there was no technical solution which would enable it to comply fully with the terms of the court order." The United States litigation was an attempt by Yahoo! to block enforcement of the French judgment in the United States.

of the conflict between the two most important stakeholders, the United States government was unable to take a position on the more important issues at the centre of the effort. This frustrated and annoyed the non-U.S. participants, and the result was essentially to abandon the effort to create an international convention.[447]

3.3.1. Governance

Technical designers of the internet quickly realized what is now common knowledge: it is hard to protect privacy online. The effort to protect privacy was a constant from the issuance of the first US government contract to link computers at different sites in 1969. About 17 percent of the 718 documents published through the close of 1979 in the technical document series that records the history of the design process – the Requests for Comments, or RFCs – deal with privacy.[448]

Those involved in designing the internet, 1969–1979, thought about privacy in ways that expand upon the conceptualizations available in the social science and legal literature then and now. Some of the ideas introduced by the computer scientists and electrical engineers foreshadowed notions introduced much later in the social sciences or the law, while others have not yet seen their parallels in other intellectual.

They acted on their awareness that privacy has to be revisited every time there is a change in technologies. Network designers during the 1970s appear extremely sophisticated in their thinking about privacy when evaluated vis-a-vis theoretical developments since that time. They viewed privacy as contextual and understood that it involves boundary setting. For now, policymakers can take away the message that general statements about protecting data privacy are inadequate. To protect privacy in the digital network environment, legal and regulatory mandates must be more specific in detailing the various sites and processes at which or during which privacy must be protected. No single technique can be effective if an entire bundle of practices affecting users, technologies, software, and the system itself are not all actively in play. For mandates regarding privacy protection techniques to make sense, lawmakers should be working together with those in the technical community rather than in isolation or in opposition.[449]

The Internet is a global network that comprises many voluntarily interconnected autonomous networks. It operates without a central governing body. To maintain interoperability, the principal name spaces of the Internet are administered by the Internet Corporation for Assigned Names and Numbers (ICANN). Role

447 von Mehren A. T., Drafting a Convention on International Jurisdiction andt he Effects of Foreign Judgments Acceptable World-wide: Can the Hague Conference Project Succeed?, 49 AM. J. COMP. L. 191, 193 (2001)

448 Braman, S. (2012). Privacy by design: Networked computing, 1969–1979. New Media & Society, 14(5), https://doi.org/10.1177/1461444811426741, p. 798-799.

449 Braman, S. (2012). Privacy by design: Networked computing, 1969–1979. New Media & Society, 14(5), https://doi.org/10.1177/1461444811426741, p. 810

of ICANN distinguishes it as perhaps the only central coordinating body for the global Internet.

ICANN is governed by a Board of Directors made up of 15 voting members, and the President and CEO, who is also a voting member. The board is further aided by five non-voting liaisons. Only the Directors have the power to determine the existence of a quorum and the validity of votes taken by the Board of Directors. The Nominating Committee is responsible for selecting the eight voting members who take seats 1 through 8; the Address Supporting Organization selects Directors who occupy Seats 9 and 10; the Country-Code Names Supporting Organization selects Directors for Seat 11 and Seat 12; the Generic Names Supporting Organization selects two directors for seats 13 and 14, while one director represents the At-Large Community who will take seat 15 and the ex officio President will occupy the 16th seat of the ICANN Board. The Chairman and Vice Chairman of ICANN are elected from the 16 Directors; the President is not a candidate.[450]

There are currently three Supporting Organizations:

1. The Generic Names Supporting Organization (GNSO) deals with policy making on generic top-level domains (gTLDs),
2. The Country Code Names Supporting Organization (ccNSO) deals with policy making on country-code top-level domains (ccTLDs),
3. The Address Supporting Organization (ASO) deals with policy making on IP addresses.[451]

ICANN also relies on some advisory committees and other advisory mechanisms to receive advice on the interests and needs of stakeholders that do not directly participate in the Supporting Organizations:

1. ICANN is part of the Governmental Advisory Committee (GAC), which is actively involved in the policy development process within ICANN. GAC is a formal advisory body providing important feedback and input for ICANN regarding its public policy.[452] ICANN relies on certain advisory committees to receive guidance and advice related to the interests and needs of stakeholders who are not able to directly participate in the Supporting Organizations. One of these advisory committees is the Governmental Advisory Committee, which is composed of representatives of national governments from all over the world - GAC has more than 140 members,

450 https://www.icann.org/resources/pages/board-of-directors
https://www.icann.org/resources/pages/governance/bylaws-en
451 https://www.icann.org/resources
452 https://gacweb.icann.org/display/gacweb/Governmental+Advisory+Committee

2. The At-Large Advisory Committee (ALAC)[453], which is composed of individual Internet users from around the world selected by each of the Regional At-Large Organizations (RALO)[454] and Nominating Committee,
3. The Root Server System Advisory Committee, which provides advice on the operation of the DNS root server system,
4. The Security and Stability Advisory Committee (SSAC), which is composed of Internet experts who study security issues pertaining to ICANN's mandate,
5. The Technical Liaison Group (TLG), which is composed of representatives of other international technical organizations that focus, at least in part, on the Internet.

3.3.2. Deep Web and Dark Web

Interest in the Deep Web peaked in 2013 when the FBI took down the Silk Road marketplace and exposed the Internet's notorious drug trafficking underbelly. Ross Ulbricht, aka Dread Pirate Roberts, was charged for narcotics trafficking, computer hacking conspiracy, and money laundering. While news reports were technically referring to the Dark Web – that portion of the Internet that can only be accessed using special browsing software, the most popular of which is TOR – negative stereotypes about the Deep Web spread.[455]

The Deep Web is the vast section of the Internet that is not accessible via search engines, only a portion of which accounts for the criminal operations revealed in the FBI complaint. The Dark Web, meanwhile, was not originally designed to enable anonymous criminal activities. In fact, TOR was created to secure communications and escape censorship as a way to guarantee free speech. The Dark Web, for example, helped mobilize the Arab Spring protests. However, just like any tool, its impact can change, depending on a user's intent.[456]

The discussion concerning all above, privacy, data protection and even Network Society has to be conducted while remembering that not everything is visible and not everything is accessible both in the legal and technical point of view. According to some estimation, even 99.97% of the widely understood Internet is hidden. Whether it is Deep Web - content that is not indexed by standard search engines or Dark Web – all unreachable network hosts on the Internet it may cause similar problems to already existing barriers and obstacles in discussion about dealing with

453 https://www.icann.org/resources/pages/governance/bylaws-en#XI

454 https://community.icann.org/display/atlarge/Regional+At-Large+Organisations

455 Ciancaglini V., Balduzzi M., McArdle R., Rösler M., Below the Surface: Exploring the Deep Web, 2015, https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf

456 Cyber criminals hide in the 'dark web' to remain anonymous, May 2 2019, https://economictimes.indiatimes.com/tech/internet/cyber-criminals-hide-in-the-dark-web-to-remain-anonymous/articleshow/69139795.cms?from=mdr

abuses in the area of data protection and data security. It also puts issues of Network Society and Social Media on completely new level.[457]

Deep Web is a very general concept. It is any portion of the Internet that can no longer be accessed through conventional means. BBC, already in December 2001, stated that: „The study found that up to 5% of the net - potentially 100 million hosts - is completely unreachable." Nowadays 99,97% is within Deep Web.[458]

Why Deep Web is harder to access? For two reasons. Some parts cannot be reached – The content is behind some kind of bot unfriendly interface, security block, has corrupted code, uses Flash or some other reason the bot can't traverse to the content. This also includes commercial databases that require login. Secondly, some content is unreadable to the bot – e.g. a picture, a movie, a pdf file with no metadata, or other non-html content. Bots can only read html, nothing more.[459]

Up to 90% can be accessed through specialized search engines designed specifically for the purpose of indexing content of Deep Web. About 10% is unreachable. There are estimations that 30% of the Deep Web are commercial databases and 20% military. About 50% of the Deep Web can be searched free with the right tools and determination.[460]

Dark Web is a small collection of sites hidden behind anonymity awarded to them by TOR. In essence, it is the World Wide Web as it was originally envisioned a space beyond the control of individual states, where ideas can be exchanged freely without fear of being censored. It is unclear how much of the Deep Web is taken up by Dark Web content and how much of the Dark Web is used for legal or illegal activities.[461]

The Dark Web can be reached through decentralized, anonymized nodes on a number of networks including TOR (short for The Onion Router) or I2P (Invisible Internet Project). The U.S. Naval Research Laboratory as a tool for anonymously communicating online originally created TOR, which was initially released as The Onion Routing project in 2002. TOR is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.[462]

---

457 Taylor K., What is the Surface Web?, https://www.hitechnectar.com/blogs/introduction-surface-web-deep-dark-web/, Thanjagari V., Deep Web & Dark Web Explained, May 7, 2019, https://hackernoon.com/deep-web-dark-web-explained-dd3b1e6855e

458 Rice M., The Deep Web Is the 99% of the Internet You Can't Google, May 22, 2018, https://curiosity.com/topics/the-deep-web-is-the-99-of-the-internet-you-dont-see-curiosity/

459 Kumar M., What is the Deep Web? A first trip into the abyss, May 31, 2012, https://thehackernews.com/2012/05/what-is-deep-web-first-trip-into-abyss.html

460 Ciancaglini V., Balduzzi M., McArdle R., Rösler M., Below the Surface: Exploring the Deep Web, 2015, https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf

461 Cox J., The Dark Web as You Know It Is a Myth, June 18, 2015, https://www.wired.com/2015/06/dark-web-know-myth/

462 https://www.torproject.org/about/history/

Reasons to access Deep Web and TOR Network:

- PRIVACY and ANONYMITY. People who want to remain anonymous or set up sites that can't be traced back to a physical location or entity. That includes people who need to protect their identity and communications from state and private surveillance, like whistleblowers and journalists. Also, dissidents in restrictive regimes may need anonymity in order to safely let the world know what's happening in their country.
- TO AVOID CENSORSHIP. Growing popularity of Deep Web in China
- MORE CONTENT. The deep Web is made up of closely 550 billion unique records and documents in contrast to the 1 billion from the surface Web. A lot more than 50 percent of the deep Web content is located in topic-specific directories
- MILITARY and LAW ENFORCEMENT ACTIVITY. U.S. Navy uses Tor for open source intelligence gathering, and one of its teams used Tor while deployed in the Middle East recently. Law enforcement uses TOR for visiting or surveilling web sites without leaving government IP addresses in their web logs, and for security during sting operations. In addition, some Police anonymous tip lines are located in Deep Web.
- ILLEGAL ACTIVITY. Black markets and child pornography

Some problems for law enforcement:[463]

- Encryption: Everything in the Dark Web is encrypted. That means the criminals in it are much more aware about being trapped or monitored. Encryption is their very first countermeasure to evade detection.
- Attribution: It's extremely difficult to determine attribution. Everything happens on .onion domains. Routing to these domains is also unclear.
- Fluctuation: The Deep Web is a very dynamic place. An online forum can be at a specific URL one day and gone the next. The naming and address schemes in the Deep Web often change. This means that the information we harvested two weeks ago is no longer relevant today. This has implications in proving crime.

3.4. Mass surveillance

The Soviet Union, East Germany, and other totalitarian states rarely respected the rights of individuals, and this included the right to privacy. Those societies were permeated by informants, telephones were assumed to be tapped and hotel rooms to

463 Ciancaglini V., Balduzzi M., McArdle R., Rösler M., Below the Surface: Exploring the Deep Web, 2015, https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf

be bugged: life was defined by police surveillance. Democratic societies are supposed to function differently.[464]

There is no agreement in the literature about how surveillance, in general, should be defined. All approaches have in common that they see surveillance connected to the systematic collection, storage, diffusion, processing, and use of personal data.[465]

We live in a surveillance society and privacy is an illusion.[466] The shift of information and communications to the Internet spawned concern from the law enforcement and intelligence communities that many of their traditional investigatory and intelligence-collection tools would become ineffective. The result has been the development of a variety of legal constraints and privileges related to electronic surveillance.[467]

Surveillance, by its very nature, impacts on personal privacy. Sharing surveillance intelligence with other governments greatly exacerbates the interference with personal privacy.[468] Mass surveillance is the distributive close observation of an entire population, or a substantial fraction of the entire population. Nowadays governments perform mass surveillance of their citizens so as to protect citizens from dangerous groups such as terrorists, criminals, or political subversives and to maintain social control. The disadvantages of mass surveillance are that it often violates right to privacy and political and social freedoms of individuals.[469]

Often, mass surveillance is carried out by the state, but it can also be carried out by corporations, either on behalf of government or on their own initiative.[470]

3.4.1. Background

PRISM (US) and Tempora (British) are both clandestine mass electronic surveillance data mining programs, both classified and secret until revealed by Edward Snowden, both are part of government sponsored mass surveillance programs. British spy agency collects and stores vast quantities of global email messages, Facebook posts, internet histories and calls and shares them with NSA according to Snowden. NSA stores massive information with examples including email, video and voice chat, videos, photos, voice-over-IP chats (such as Skype), file transfers, and social

464 W. Diffie, S. Landau, Privacy on the Line..., p. 143.

465 Sevignani S., The commodification of privacy on the Internet, Science and Public Policy 40 (2013), p. 734

466 Von Drehle D., The Surveillance Society, http://nation.time.com/2013/08/01/the-surveillance-society/, 2013

467 Henry H. Perritt Jr., The Internet at 20: Evolution of a Constitution for Cyberspace, 20 Wm. & Mary Bill Rts. J. 1115 (2012), https://scholarship.law.wm.edu/wmborj/vol20/iss4/5, p. 30

468 https://www.privacyinternational.org/topics/mass-surveillance

469 https://definitions.uslegal.com/m/mass-surveillance/

470 Egwuonwu B, What Is Mass Surveillance And What Does It Have To Do With Human Rights?, April 2016, https://rightsinfo.org/explainer-mass-surveillance-human-rights/

networking details. British Government Communications Headquarters (GCHQ) had probes attached to more than 200 internet links; each probe carried 10 gigabits of data a second. PRISM and Tempora both have centralized mass databanks. Data in PRISM is maintained for Archived system audit logs and backup data is stored for a minimum of two years.[471]

Even after all this information, got revealed U. S. President defended NSA and its mass surveillance program:

> When it comes to telephone calls, nobody is listening to your telephone calls. That's not what this program is about. (...)
> What the intelligence community is doing is looking at phone numbers, and durations of calls; they are not looking at people's names and they're not looking at content. (...)
> If the intelligence committee actually wants to listen to a phone call, they have to go back to a federal judge, just like they would in a criminal investigation.[472]
> Former President Obama on June 6, 2013

These words were said on June 6 2013. Only month later in July, another NSA operation was revealed, standing in contradiction to Barack Obama's statement. Xkeyscore - Formerly secret computer system used by the NSA for searching and analysing Internet data about foreign nationals across the world. The program is run jointly with other agencies including Australia's Defence Signals Directorate, and New Zealand's Government Communications Security Bureau.[473]

For a while, there was a claim that even low-level analysts are allowed to search the private emails and phone calls. The claim became a fact when The Guardian's Glenn Greenwald revealed that it is possible to *listen to whatever emails they want, whatever telephone calls, browsing histories, Microsoft Word documents. And it's all done with no need to go to a court, with no need to even get supervisor approval on the part of the analyst*.[474] If the words of a journalist are not enough then NSA summed up the program: *XKeyscore is its "widest reaching" system for developing intelligence from the Internet. The program gives analysts the ability to search through the entire database of your information without any prior authorization — no warrant, no court clearance, no signature on a dotted line. An analyst must simply complete a simple onscreen form, and*

471 Rifkind M, Porter H., Henry Porter v Malcolm Rifkind: surveillance and the free society, http://www.theguardian.com/commentisfree/2013/aug/24/rifkind-porter-debate-miranda-surveillance

472 J. Voorhees, Obama Defends NSA Surveillance: "Nobody Is Listening to Your Telephone Calls.", June 7 2013, http://www.slate.com/blogs/the_slatest/2013/06/07/obama_defends_nsa_surveillance.html

473 Active surveillance program XKEYSCORE, http://digital-era.net/active-surveillance-program-xkeyscore/

474 abcnews.go.com

seconds later, your online history is no longer private. The agency claims that XKeyscore covers "nearly everything a typical user does on the Internet."[475]

One of the results of growing mass surveillance threat is mentioned above United Nations Privacy Resolution on November 2013 Draft Resolution:

> In response to growing concern about the scope of electronic surveillance, the U.N. General Assembly is considering a resolution affirming that privacy is a fundamental right. Civil society organizations have long urged international organizations to update and strengthen global frameworks for privacy protection. The UN resolution now under consideration is a response to reports that the United States conducted surveillance of many foreign leaders, including Brazil's President Dilma Rousseff and German Chancellor Angela Merkel. Brazil and Germany are leading the effort at the United Nations on the privacy resolution.

PRISM and Tempora are giving the extreme examples of surveillance, including spying on world leaders.[476] Sadly, those two programs are not the only. Easily even 33 mass surveillance programs and initiatives can be named.[477] Even if not all of them are aggressive and the role is not to spy, it shows the range of collecting data. It is not hard to imagine how much it endangers the privacy. The other issue connected to large number of mass surveillance agencies and programs is the amount of collected data. Similarly, to overregulation in legislation, collecting too much data may cause the situation in which this data is useless or hard to analyse. For example, NSA using various programs collects all they possibly can from the Internet. Yet, United States agencies missed some details warning about terrorist attack, which later lead to Boston Marathon bombings on April 15, 2013. This raises two questions. What is the point of uncontrollable data collection? How much surveillance is too much?

Surveillance was supposed to be a tool in the fight with terrorism, however, especially now when we know so much about PRISM and other similar programs, it is hard to think differently than just that mass surveillance became similar threat as terrorism itself. Our privacy is endangered, because ways to protect as from external enemies now are also aimed on us, citizens. Governments should not forget that privacy is a basic human right and as such cannot be violated on daily basis by mass surveillance. Privacy has important role in promoting democracy and significant impact on other fundamental rights, for example freedom of expression. Mass

475 New leaks say NSA can see all your online activities, 31 July 2013, http://net-security.org/secworld.php?id=15328

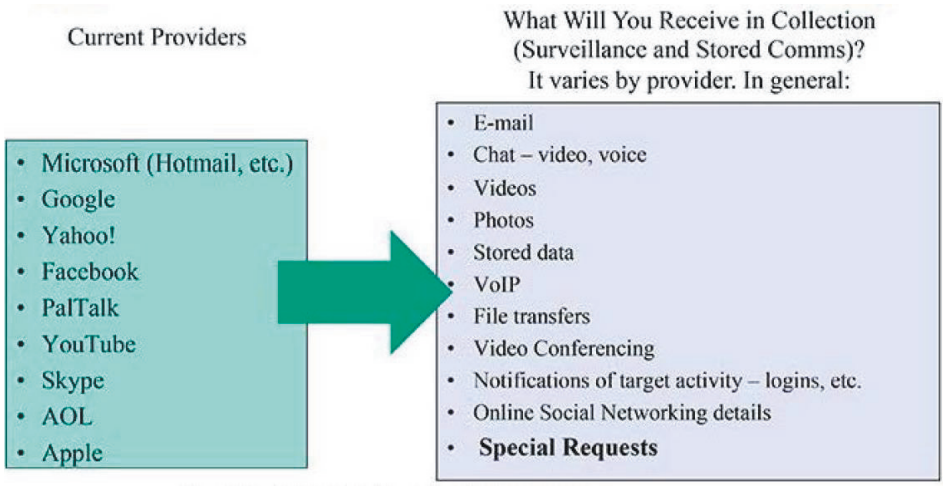
476 Ball J., NSA monitored calls of 35 world leaders after US official handed over contacts, 25 October 2013, http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls

477 List of government mass surveillance projects, http://en.wikipedia.org/wiki/List_of_government_mass_surveillance_projects

surveillance as a defensive tool cannot be also a tool costing us losing freedom and democratic values.[478] Uncontrollable data collection by mass surveillance agencies creates also other dangers – agencies may get access to files collected for other purposes, collected data may cause linking once separate information and eventually creating citizen profiles, finally mass databases are in big risk of losing confidential data.[479]

3.4.2. Role of Dominant ICT Companies

Thanks to Edward Snowden we now know how significant was and still is the role of biggest ICT companies. In the course of writing my Dissertation, it is interesting to see on the list all the dominant ICT companies that I like to call global dominant companies[480] - Facebook, Microsoft and Google and Apple. Facebook, Microsoft, and Google are the core of my dissertation project.



Most interestingly when rumours about biggest IT companies cooperating with NSA arisen, all four companies immediately denied taking part in any mass surveillance program:

> *Microsoft*: "We provide customer data only when we receive a legally binding order or subpoena to do so, and never on a voluntary basis. In addition, we only ever comply with orders for requests about specific

478 Goold B., How Much Surveillance is Too Much? Some Thoughts on Surveillance, Democracy, and Political Value of Privacy, [in:] Schartum D. W. (ed), Overvåking in en Rettsstat, 2010, p 45-46.

479 Webster F., Theories of the Information Society..., p. 299

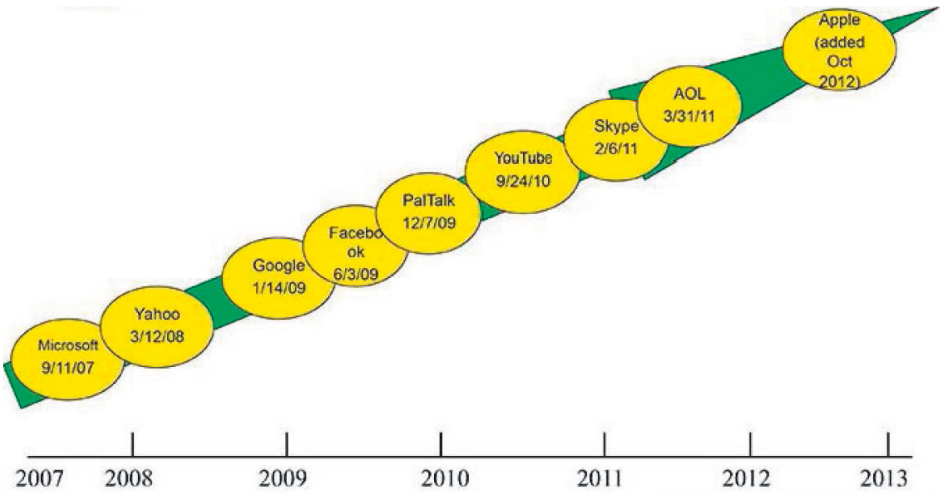
480 Wiatrowski A., The "Dominance" in Abuses of Dominant Companies: More Than Super Dominant, [in:] Svantesson D., Greenstein S. (eds.), Nordic Yearbook of Law and Informatics 2010-2012. Internationalisation of Law in the Digital Information Society, Copenhagen 2013, p. 358.

accounts or identifiers. If the government has a broader voluntary national security program to gather customer data, we don't participate in it."

Facebook: "We do not provide any government organization with direct access to Facebook servers. When Facebook is asked for data or information about specific individuals, we carefully scrutinize any such request for compliance with all applicable laws and provide information only to the extent required by law."

Google: "Google cares deeply about the security of our users' data. We disclose user data to government in accordance with the law, and we review all such requests carefully. From time to time, people allege that we have created a government 'back door' into our systems, but Google does not have a 'back door' for the government to access private user data,"

Apple: "We have never heard of PRISM. We do not provide any government agency with direct access to our servers, and any government agency requesting customer data must get a court order."[481]



Above graph indicates that companies' statements have more or less the same value as, already mentioned in this paper, words of President Obama about NSA mass surveillance programs.

The role of the dominant ICT companies is significant not only for PRISM but in general, when it comes to collecting data. Fred Cate, James Dempsey and Ira

481 Brustein J., The Companies' Lines on Prism, June 07, 2013, http://www.businessweek.com/articles/2013-06-07/the-companies-lines-on-prism

Rubinstein wrote an article about systematic government access to private-sector data.[482] Private sector has nowadays almost unlimited access to data shared by users all around the world. As shown above PRISM and Tempora were using the biggest companies in the world for their purposes. In the mentioned article, which is also an introduction to reports about systematic government access in nine countries[483], eight issues were pointed out:

1. *Lack of transparency* – difficulty in assessing activities and laws concerning systematic government access,
2. *Significant expansion in systematic access* – despite of difficulties with transparency, in every country addressed by these papers there is evidence of a significant expansion in government demands for private-sector data in general and for broad, systematic access in particular,
3. *Significant commonality across laws* – data collection for law enforcement and national security are either exempted from general data protection laws or constitute permissible uses under those laws,
4. *Inconsistency between law and practice* – inconsistencies between what law says and what governments are reportedly doing. It doesn't necessarily mean that the activity is illegal, but rather that it occurs subject to a legal interpretation that is withheld from the public or takes place in the interstices of national regulation,
5. *National security and law enforcement exceptions* - data collection and use for national security and law enforcement purpose is often excluded from oversight applicable to other data processing activities or subject to far less transparent standards and oversight regimes.
6. *The declining "wall" between national security and other uses* – national security and law enforcement gain access to private-sector data with greater ease plus the expanding freedom to share that information among agencies and use it for purposes beyond those for which it was collected causes a substantial weakening of traditional data protection,
7. *Systematic volunteerism* – the most plausible means for systematic government access to private-sector data us through voluntary agreements with the operators of the systems and databases,
8. *Importance of multinational access and sharing* – cross-border access to data is essential to national security, law enforcement, and other government activities.[484]

482 Cate F., Dempsey J., Rubinstein I., Systematic government access to private-sector data, [in:] International Data Privacy Law, volume 2, number 4, 2012, p. 195-199.

483 Canada, China, United Kingdom, Japan, United States, Australia, Israel, Germany, India

484 Cate F., Dempsey J., Rubinstein I., Systematic government access to private-sector data..., p. 197-199.

3.4.3. The good and the bad results

Mass surveillance crisis brought us several consequences. I like to believe that surprisingly they are mostly positive. To say at least this issue came out to the light. It became obvious to most that using Internet and broadly understood Social Media comes with a cost. The cost of losing all privacy, not only to companies, but also to governments. Most definitely to US and British governments, but it is hard to believe that there are no other states conducting similar practices.

This growing awareness lead to the situation in which global ICT companies must have changed their business policies. Simply stating that they had nothing to do with mass surveillance is not going to work anymore. Therefore, some companies decided to take different path, show that they are privacy and data protection friendly. Two best examples are Google's Project Zero[485] and Microsoft's campaign "Putting people in control" that can be concluded with the words: *Microsoft experiences will be unique as they will reason over information from work and life and keep a user in control of their privacy*.[486]

It seems that both Google and Microsoft realized that to keep customers' trust they need to prove that they really have nothing to do with mass surveillance. At least not anymore.

Project Zero is a group of top Google security researchers with the sole mission of tracking down and neutering the most insidious security flaws in the world's software. Those hackable bugs, known in the security industry as "zero-day" vulnerabilities, are exploited by criminals, state-sponsored hackers and intelligence agencies in their spying operations. Google hopes to get those spy-friendly flaws fixed. What is also very important, Project Zero's hackers won't be exposing bugs only in Google's products, but they'll be given free rein to attack any software whose zero-days can be dug up and demonstrated with the aim of pressuring other companies to better protect Google's users.[487]

Microsoft chose different path, path of informing and educating. They say that are helping put user in control in three ways:

1. Building privacy into policies and practices. Putting you in control means offering transparency, starting with company policies that provide simple and easy to understand explanations of how we use your personal information.
2. Building privacy into products. We design and build products with security and privacy in mind, from our software development processes to using best-in-class encryption to protect your data. These steps are critical to keeping your information safe.

485 https://googleonlinesecurity.blogspot.fi/2014/07/announcing-project-zero.html)

486 http://blogs.microsoft.com/on-the-issues/2015/01/28/data-privacy-day-2015-putting-people-control/

487 Greenberg A., Meet 'Project Zero,' Google's Secret Team of Bug-Hunting Hackers, July 15, 2014, https://www.wired.com/2014/07/google-project-zero/

3. Advocating laws and legal processes that keep people in control. We require governments around the world use legal process to request customer data. We have challenged laws to make privacy protections stronger. In addition, we advocate for better public policy to balance privacy and public safety. [488]

Additionally, Microsoft created a simple guidance including following tips:

1. Once posted, always posted: Think twice about posting comments, images or videos that you would not want your employer to see. Share, but do not over-share!
2. Be knowledgeable about security and privacy settings. Control who sees what you post by judiciously using social networks' privacy settings. For example, you may want to limit the people who can see Facebook photos from your cousin's bachelor's party to just a close circle of friends.
3. Keep personal info personal. Do not make cyber-criminals' jobs easier by sharing sensitive information such as your address or other personal data.
4. Correct any inaccuracies. If you see information about yourself that is wrong or that you do not want to share online, take the necessary steps to correct it. If someone posts a photo of you on Facebook that you don't want others to see, untag yourself or ask the original poster to remove the photo altogether.[489]

Finally, Microsoft promotes Microsoft's Safety and Security Center[490] and the National Cyber Security Alliance[491].

However, putting aside ICT companies attempts to prove us that suddenly they care about our security and privacy, there are attempts to stop biggest abusers both in EU and US.

Mass surveillance programs, knowledge about it, about PRISM in particular, the role of the companies with which we share sensitive data on a daily basis, it all has both very negative and some positive results for now and for the future of privacy and data protection.[492]

Today we live in the new Network Society, which is also a Surveillance Society. Together I like to call it a society that is trapped in the network and this network is under constant mass surveillance. The simplest way to explain it, the reason to call

488 https://googleonlinesecurity.blogspot.fi/2014/07/announcing-project-zero.html

489 http://lumiaconversations.microsoft.com/2015/01/28/stop-think-connect-safeguarding-online-reputation/

490 Protect your privacy on the Internet, http://www.microsoft.com/security/online-privacy/prevent.aspx

491 http://www.staysafeonline.org/

492 Rantham L., PRISM, Snowden and Government Surveillance: 6 Things You Need To Know, April 19, 2017, https://www.cloudwards.net/prism-snowden-and-government-surveillance/

this situation as being trapped in the network is that there is no choice anymore. As a society and as individuals we are in every aspect of our lives completely dependent on technology and infrastructure provided by technology. I cannot imagine a person living in modern society not being a subject of some kind of surveillance, as well as I cannot imagine this person being able to break with the access to technology.

However, there are attempts to seek for privacy in the Internet. Growing popularity of services hidden in Deep Web[493] are the sign of it. Unfortunately, hiding in Deep Web may expose us to even bigger threats to our privacy. Deep Web today is a place for all sorts of criminal activities, a haven for thieves, child pornographers, human traffickers, forgers, assassins and peddlers of state secrets and loose nukes.[494] Yet, more and more people chose to hide there, as this is the area unavailable for any kind of surveillance. It shows how desperate are some people in seeking privacy, but also it shows growing privacy awareness.[495]

I absolutely do not support the idea of popularizing Deep Web, as a place highly dangerous, but I like the idea presented by Susan Barnes. She suggests that education about dangers on social media pages, especially education of younger generation may be the way to protect privacy and to raise privacy awareness.[496] It may be little naive but knowing how recklessly young people give up sensitive data about themselves, it could be important solution and way to protect us from real life threats caused by losing our privacy on social media pages.

It is a good thing that there are attempts to save privacy or what has left of it, but the attention drawn to the problem suggests it seriousness and for how long we ignored this problem.

We must remember that challenges to privacy are even bigger now, when Information Society changes into the Network Society. There are more risks, society seems to be more willing to share sensitive data and standards of information security are very modest. Altogether, privacy requires sophisticated information security.[497]

---

493 The surface level of the Internet is basically everything that is indexed by search engines such as Google. Facebook, Youtube, these are all surface sites. But according to The Guardian, you can only access around 0.03% of the total internet on a search engine. Deep Web is World Wide Web content that is not part of the Surface Web, which is indexed by standard search engines. - Exploring the Hidden Internet ("Deep Web"), http://www.teamliquid.net/forum/general/229525-nsfw-exploring-the-hidden-internet-deep-web

494 Grossman L., The Secret Web: Where Drugs, Porn and Murder Live Online, November 11, 2013, http://time.com/630/the-secret-web-where-drugs-porn-and-murder-live-online/)

495 Naughton J., 'The goal is to automate us': welcome to the age of surveillance capitalism, January 20, 2019, https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook

496 Barnes S. B., A privacy paradox...

497 Saarenpää A., Perspectives on Privacy..., p. 24-25.

All these efforts for privacy are very positive, because there is no doubt that privacy will be beneficial for society also in the future. Legal systems must continue to contribute effectively to privacy and data protection. On national level, it may be almost impossible.[498] With international legislation it is and it will result in overregulation and consequently in loopholes, inconsistency and ultimately in even more interpretations leading to violating privacy.

Coming back to the topic of mass surveillance, I would like to emphasize that in my opinion it is impossible to simply end with these practices. Surveillance, in many forms is a necessity for governments as well as for private companies, those dominant in particular. Yet it is important to remember what ECHR article 8 gives us. "Any interference by a public authority with a Convention right must be directed towards an identified legitimate aim. The sorts of aims which are legitimate are interests of public safety, national security, the protection of health and morals and economic well-being of the country or the protection of the rights and freedoms of others." Convention approach is to decide whether a particular limitation from a right is justified. Meaning that limitation must be proportionate to the legitimate aim pursued.[499]

The way to protect our privacy is to limit surveillance's infinity. Ann Cavoukian is promoting the idea called Privacy-Protective Surveillance (PPS).[500] This idea is an answer to typical approaches of protecting privacy where while ensuring measures to counteract terrorism, we seek to strike a balance between these two interests. This often leads to making privacy the less important value, in favour of the more significant value, which is public safety. PPS an alternative to current counterterrorism surveillance systems. One of the most attractive elements of PPS is the fact that its intelligent agents will only collect data that is considered significant. Significant data is defined by transactions or events that are believed to be associated with terrorist-related activities. For example, purchasing fertilizer capable of bomb making or accessing a bomb-making website. An important consequence of PPS's collection of significant data is that its intelligent agents would effectively be blind to seeing any other information they may run across during their searches. Additionally, the use of homomorphic encryption would allow PPS to make computations or engage in data analytics on encrypted values – data that cannot be read because it is not in plain text. This provides additional assurance to individuals that recording or monitoring

498 Blume P., The Importance of Information Privacy and its Future, [in:] Greenstein S. (ed.), Vem reglerar informationssamhället?, Stockholm 2010, p. 169.

499 Wadham J., Human Rights and Privacy - The Balance, speech given at Cambridge (March 2000), http://www.liberty-human-rights.org.uk/mhrp6j.html, more in Solove D., Schwartz P. M., Information Privacy Law, Fourth Edition, New York 2011, p. 1072, 1073.

500 Cavoukian A., El Emam K., Introducing Privacy-Protective Surveillance: Achieving Privacy and Effective Counter-Terrorism, September 2013, http://www.privacybydesign.ca/content/uploads/2013/12/pps.pdf

their actions within the system is impossible. Finally, the intelligence gathered by PPS would be context-specific. In order to become information of value, data must be placed in the appropriate context.[501]

Fortunately, not only Internet users and scholars recognize privacy issues. International Data Privacy Day[502], watchdog organizations, coming Data Protection Regulation, revision of OECD principles, legal actions against Google[503], Max Schrems actions and recent CJEU ruling, these are all good signs. Together with realization that we actually do not need more legislation, but the legislation, which is better and more consistent, we still have a chance of keeping our privacy. Not the one we would like to have, for that it may be too late, not what has left of it, but new modern privacy for modern society, Network Society. This privacy cannot, nor will be complete but it must be ready for challenges that may come. Today mass surveillance is no longer surprising to us, now we must work to never be surprised by what can come in future.

3.5. The Cookies "situation"

Cookies are an essential part of modern websites. They were first implemented as a browser extension in 1995 and formally standardized in 1996 by the Internet Engineering Taskforce.[504]

EU governments are unknowingly allowing the ad tech industry to monitor citizens across public sector websites. The extent of tracking on public sector websites is especially alarming given that these websites do not rely on revenue from advertising. Although the governments presumably do not control or benefit from the documented data collection, they still allow the safety and privacy of their citizens to be compromised within the confines of their digital domains – in violation of the laws that they have themselves put in place.

The World Economic Forum values the global data economy at $3 trillion.[505] The growth of this sector has been fuelled by the increasingly pervasive collection, cross-referencing, and resale of personal data – including information about people's interests, locations, income, relationship status, gender, age, education, etc.

501 Cavoukian A., El Emam K., abstract of Introducing Privacy-Protective Surveillance: Achieving Privacy and Effective Counter-Terrorism, September 20, 2013, http://www.privacybydesign.ca/index.php/paper/introducing-privacy-protective-surveillance-achieving-privacy-effective-counter-terrorism/

502 https://www.staysafeonline.org/data-privacy-day/

503 Dixon H., Warman M., Google gets 'right to be forgotten' requests hours after EU ruling, May 14, 2014, http://www.telegraph.co.uk/technology/google/10832179/Google-gets-right-to-be-forgotten-requests-hours-after-EU-ruling.html

504 Kristol/Montulli, Http State Management Mechanism, RFC Editor, 1997.

505 The value of data, 22 September 2017, https://www.weforum.org/agenda/2017/09/the-value-of-data/

Companies will typically attempt to place trackers on as many websites as possible to optimise data inflow. Once in-page, they store a unique identifier (a code string) in the user's browser so they can record user behaviours, such as:

- Which sites the user visits and for how long
- The speed and pattern of the user's scrolling
- What the user clicks on or hovers over

These behavioural data are combined with other information in order to build detailed profiles of each individual user. Typically, tracking companies will also perform "cookie syncing", which allows them to swap their unique identifier with other ad tech actors, so that the data they hold on users can be crossreferenced and combined, potentially with valuable identifiers like email addresses, social media logins or real names.

While sensitive information about a person's health condition belongs to so-called special category data that is carefully protected under Article 9 of the GDPR, 52% of EU public health service web pages were found to contain commercial trackers.[506]

Across both government and health service websites, a total of 112 companies were identified using trackers that send data to a total of 131 third party tracking domains.

Google performs more than twice as much tracking as any other company. Google owns several of the most dominant ad tracking domains, accounting for three out of the top five trackers on government websites. Both of the top two trackers found on health service landing pages also belong to Google. These results do not include trackers associated with the Google Analytics platform.

Google controls the top three tracking domains found in this study: YouTube.com, DoubleClick.net and Google.com.

- Through the combination of these domains, Google tracks website visits to 82% of the EU's main government websites.
- On each of the 22 main government websites on which YouTube videos have been installed, YouTube has automatically loaded a tracker from DoubleClick.net (Google's primary ad serving domain).
- Using DoubleClick.net and Google.com, Google tracks visits to 43% of the scanned health service landing pages.

Given its control of many of the Internet's top platforms (Google Analytics, Maps, YouTube, etc.), it is no surprise that Google has greater success at gaining tracking access to more webpages than anyone else. It is of special concern that Google is capable of cross-referencing its trackers with its 1st party account details from popular consumer-oriented services such as Google Mail, Search, and

506 Ad Tech Surveillance on the Public Sector Web. A special report on pervasive tracking of EU citizens on government and health service websites, Report by Cookiebot, March 2019, https://www.cookiebot.com/media/1121/cookiebot-report-2019-medium-size.pdf

Android apps (to name a few) to easily associate web activity with the identities of real people.

Google tracks users through "Location History" and "Web & App Activity", which are settings integrated into all Google accounts. For users of mobile phones with Android this tracking is particularly difficult to avoid. Google is processing incredibly detailed and extensive personal data without proper legal grounds, and the data has been acquired through manipulation techniques. When we carry our phones, Google is recording where we go, down to which floor we are on and how we are moving. This can be combined with other information about us, such as what we search for, and what websites we visit. Such information can in turn be used for things such as targeted advertising meant to affect us when we are receptive or vulnerable. TRhe scale in which Google tracks the location of its users breaches the GDPR. Users have not given free, specific, informed and unambiguous consent to the collection and use of location data, particularly considering the scale of tracking going on.[507]

Under the GDPR, companies are allowed, in certain circumstances, to use non-sensitive personal data, without consent. Such circumstances could be e.g. incidental re-use of data for the provision of services. This is called the "legitimate interest" exception of the GDPR. Now, lawmakers are opening up to incorporating this exception in the ePrivacy Regulation as well. However, a "legitimate interest" exception has no place here. A ruling by the Court of Justice, in 2016, stated that communications data must be considered to be sensitive data, and therefore, companies should under no circumstances be allowed, without specific permission, to monetise or otherwise exploit sensitive communications. It would only broaden to an unpredictable extent the way that companies would be allowed to use communications data. Any "legitimate interest" exception would undermine users' control over their own personal data.[508]

Communications data are highly sensitive. This is why every update of the ePrivacy Directive insisted on users' consent for processing of this data. Despite the claims to the contrary, the new Regulation is doing little more than maintaining this principle. Yet, the need for meaningful consent is crucial.[509]

The timeliest example of companies interfering into the public sector against GDPR is Finland's Keal. Public benefits agency Kela has broken the law by not asking users of its website for permission to gather their data under data protection regulations. The data belonging to persons who use the website of the Finnish Social

507 New study: Google manipulates users into constant tracking, 27 November 2018, https://www.forbrukerradet.no/side/google-manipulates-users-into-constant-tracking

508 Ad Tech Surveillance on the Public Sector Web. A special report on pervasive tracking of EU citizens on government and health service websites, Report by Cookiebot, March 2019, https://www.cookiebot.com/media/1121/cookiebot-report-2019-medium-size.pdf

509 Buttarelli G., The urgent case for a new ePrivacy law, October 19, 2018, https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_en

Insurance Institution, Kela, had ended up in the hands of third parties such as Facebook and Google. Kela's site uses technology and data collection tools sourced from private companies.[510]

A vast majority of websites is undermining EU rules for data privacy, a study by researchers from MIT, UCL, and Aarhus University suggests.[511] Fewer than 12% of the top 10,000 websites that were studied met the minimum requirements set out in EU law for the use of cookie consent tools. These illegal practices and configurations result from websites not following the legally prescribed course of action with regards to the use of cookie consent tools to obtain consent from their website visitors. Such consent is required by law for all websites in the EU. This comes as a result of guidelines set out in the GDPR that are designed to govern how companies collect and process the personal data of website users.

However, websites can effectively navigate around the GDPR by tailoring the design of their consent management platforms to provide a misleading veneer of a consent agreement. For example, although the GDPR only recognizes informed and active consent, many websites flag users who close or ignore cookie consent tools as having passed consent.

Some cookie consent tools, for example, give the user no choice between approving and declining the use of cookies. In contrast, others make use of pre-ticked boxes to duplicitously garner user consent. It is in precisely this ambiguous way that many websites can gather user consent without the user ever actually having provided consent in the first place.

A significant majority of cookie consent tools on EU websites either present no option for consent to users, or they manipulate users outright into unwittingly providing consent.[512] Only a significant minority (11.8%) of websites comply fully to the GDPR's standards. For example, the study finds that the familiar banner-style cookie consent tools do not affect users providing consent. As soon as an opt-out button is added to the interface, consent increases by nearly 25 per cent. On the other hand, consent forms which provide a myriad of buttons and choices for users to provide consent ('granular controls') seem to marginally decrease the number of users giving consent to the website.

The Court of Justice delivered its judgment[513] in case C-673/17 Planet49, concerning the requirements for a valid consent to the storage of cookies. The Court

510 Kela website user data ended up with Google, Facebook, February 1, 2020, https://yle.fi/uutiset/osasto/news/paper_kela_website_user_data_ended_up_with_google_facebook/11187895

511 Nouwens M., Liccard I., Veale M., Karger D., Kagal L., Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence, 8 January 2020, https://arxiv.org/pdf/2001.02479.pdf

512 Utz Ch., Degeling M., Fahl S., (Un)informed Consent: Studying GDPR Consent Notices in the Field, 22 October 2019, https://arxiv.org/pdf/1909.02638.pdf

513 Judgement of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801

agreed with the Advocate General that consent referred to in Article 2(f) and in Article 5(3) of Directive 2002/58 cannot validly be obtained by way of a pre-ticked checkbox which the user must deselect to refuse his or her consent. To support this conclusion, the Court referred to the requirements for consent to be 'specific' and 'unambiguous' under Directive 2002/58 as well as the even more detailed wording of the GDPR.

Importantly, the Court did not elaborate on the requirement that consent must be 'freely given', arguing that a corresponding question had not been asked by the referring court. Response to such a question - one of major importance to the digital economy - would involve an assessment whether user's consent to the processing of personal data for advertising purposes constituted a prerequisite to that user's participation in a promotional lottery. As noted in our previous post, the Advocate General elaborated on this matter in a way that was subject to criticism. Against this background, self-restraint showed by the Court is to be welcomed.

As regards the question whether the interpretation set out above should differ, depending on whether or not the information stored or accessed on user's terminal equipment qualifies as personal data, the Court responded with a clear 'no'. This remains in line with the rationale of Directive 2002/58 which aims to protect the user (including natural persons acting for business purposes) from interference with his or her private sphere, regardless of whether or not that interference involves personal data.

Finally, as regards the scope of information to be provided to the user before obtaining his or her consent, the Court opted for a broad reading of Article 5(3) of Directive 2002/58 in conjunction of Article 10(c) of Directive 95/46 and Article 13(1)(e) of the GDPR. In this respect, the Court, once again, sided with the Advocate General, stressing that "clear and comprehensive information implies that a user is in a position to be able to determine easily the consequences of any consent he or she might give and ensure that the consent given is well informed. It must be clearly comprehensible and sufficiently detailed so as to enable the user to comprehend the functioning of the cookies employed" (para. 74). The Court considered that information on both the duration of the operation of cookies and whether or not third parties may have access to them had to be provided to the user.

4. DOMINANT ICT COMPANIES

While people use web sites for reasons, such as obtaining news, answering queries, providing information, staying in touch with friends, making new relations, or organizing events, they are watched in great detail. Profit-oriented web services develop massive systems of user surveillance and store 'literally everything', as a Facebook employee has admitted.[514] Internet users, willingly or unwillingly, provide commercial Internet services with information that is used for monetary exchanges with the advertising industry. The revenues finance the web services but also include profits for the owners of Internet corporations.[515]

Internet firms, particularly large, US -based companies like Google or Facebook, have become the global regulators over information and online behaviour. The firms' regulatory capacity derives in part from their provision of essential services, such as search, web hosting, or payment services, as well as from their global platforms, significant market share, and sophisticated enforcement programs. A key reason that these Internet firms are powerful global regulators is because they operate what security analyst Bruce Schneier calls surveillance-based business models in which they comprehensively track their users and amass users' personal information, often with the intent of selling this information to advertisers.[516]

Interestingly, companies with data-intensive business models like social networking services generally contend that individuals are making an informed choice in disclosing their personal data for better services or free services, or more targeted useful advertising.

The dominant companies have the possibility of regulating through technology. This is far more threatening to the Internet's constitution than traditional governmental regulation backed up by legal institutions.[517]

Henry H. Perritt Jr. predicted[518] that under specific circumstances also exist monopolies in the Internet may be created. Some companies in self-interest started by blocking access to some services or products only offering their own. These typically

514 Wong P., Conversations about the Internet #5: Anonymous Facebook Employee, 2010 http://therumpus.net/2010/01/conversations-about-the-internet-5-anonymousfacebook-employee/3/

515 Sevignani S., The commodification of privacy on the Internet, Science and Public Policy 40 (2013), p. 734

516 Pix A., Surveillance Is the Business Model of the Internet - Interview with Bruce Schneier, July 18, 2017, https://www.schneier.com/news/archives/2017/07/surveillance_is_the_.html

517 Lessig L., CODE: AND OTHER LAWS OF CYBERSPACE, VERSION 2.0 81–82 (2006)

518 Perritt H. H. Jr., The Internet at 20: Evolution of a Constitution for Cyberspace, 20 Wm. & Mary Bill Rts. J. 1115 (2012), https://scholarship.law.wm.edu/wmborj/vol20/iss4/5, p. 37

involve a monopoly position by the one denying access. Monopolies may arise for several reasons. For example, a supplier may have proprietary interconnection technologies protected by intellectual property law offering features that distinguish it from competitors. In such circumstances, suppliers of complementary products may be willing to pay higher-than-market rates for access, so they can incorporate the proprietary features in the integrated offering to consumers.

The law can remove artificial barriers to entry. One such barrier to entry is "predatory pricing" by the monopolist. Predatory pricing signifies that a monopolist, threatened by the prospect of a new entrant, will reduce prices in the short run to a level below that at which the new entrant can earn a profit.[519] A monopolist can afford to do this, either because it can forego some of its monopoly profits in the short run in order to retain its monopoly in the long run, or because it has banked enough excess monopoly profits in the past to allow it to finance a short-term loss as a good investment to increase prices later and reinstate its monopoly profits. Antitrust law developed a complex set of rules to determine when predatory pricing exists and when it should be illegal.[520]

Empires are emerging that control backbone connectivity, but that is not all. Empires are also developing with respect to content distribution. Whether these empires pose threats to the Internet's constitution depends on imperial business policies. One can speculate on adverse directions for evolution. For example, Google dominates the market for Internet search and for search-related advertising. Its email service, Gmail, represents a rapidly growing share of the market.[521]

Android software for smartphones has displaced Apple's dominance of this market. Google has also entered the hardware market. It has launched Google+, a social networking service aimed at Facebook's market. Google+ did not succeed[522], but Google's Gmail remains the most popular e-mail service.

The result would be a market structure in which Internet users obtain a larger and larger portion of their Cyberspace resources through Google rather than its competitors.

Today, companies aggregate, trade, and utilize personal information at unprecedented levels. Their unilateral and extensive access to data about the characteristics, behaviours, and lives of billions allows them to constantly monitor, follow, judge, sort, rate, and rank people as they see fit. Since the rise of social networks, smartphones, and online advertising, a wide range of companies has started

519 Brocke Grp. v. Brown & Williamson Tobacco Corp., 509 U.S. 209, 221–28 (1993).

520 Section 2 of the Sherman Act, at 15 U.S.C. § 2. Article 102 of the TFEU - Predatory pricing is one of the forms of the abuse of dominant position.

521 Perritt H. H. Jr., The Internet at 20: Evolution of a Constitution for Cyberspace, 20 Wm. & Mary Bill Rts. J. 1115 (2012), https://scholarship.law.wm.edu/wmborj/vol20/iss4/5, p. 42

522 Fox Ch., Google shuts failed social network Google+, April 2, 2019, https://www.bbc.com/news/technology-47771927

to monitor, track, and follow people across virtually all aspects of their lives. Today, the behaviours, movements, social relationships, interests, weaknesses, and most private moments of billions are constantly recorded, evaluated, and analyzed in real-time.[523]

When surfing the web, hidden pieces embedded of software transmit information about the websites visited, navigation patterns, and sometimes even keystrokes, scrolls and mouse movements to hundreds of third-party companies. Similarly, when carrying a smartphone, rich information about the user's everyday life not only flows to Google, Apple, and a variety of app providers but also to a significant number of third-party companies, again based on hidden software embedded by app providers. Such information may include a person's contacts, information about real-time app usage and movements, as well as data from all kinds of sensors recording motion, audio, video, and more. Furthermore, as a rapidly increasing number of devices connects to the internet – from wearables, e-readers, TVs, game consoles, toys, baby monitors, printers, and voice-controlled speakers to thermostats, smoke alarms, energy meters, door locks, and vehicles –personal data collection threatens to become ubiquitous and totalizing. Already now, though, individuals can see only the tip of the data and profiling iceberg. Most of it occurs in the background and remains opaque; as a result, most consumers, as well as civil society, journalists, and policymakers, barely grasp the full extent and forms of corporate digital tracking and profiling. This large-scale and widely unrestrained commercial exploitation of personal data raises major concerns about the future of autonomy, equality, human dignity, and democracy.[524]

4.1. Facebook

Facebook data is for sale all over the world.[525]

In February 2004, Mark Zuckerberg created Facebook (then called "Thefacebook") in his dorm room at Harvard University.[526] Within 1 month of its creation, half of the Harvard student population had signed up.[527] Facebook quickly expanded

523 Christl W., Corporate Surveillance in Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions, June 2017, http://crackedlabs.org/en/corporatesurveillance

524 Christl W., How Companies Use Personal Data Against People. Automated Disadvantage, Personalized Persiasion, and the Societal Ramifications of Commercial Use of Personal Information, 2017, https://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf

525 Steve Bannon on Cambridge Analytica: 'Facebook data is for sale all over the world', March 2018, https://www.theguardian.com/us-news/2018/mar/22/steve-bannon-on-cambridge-analytica-facebook-data-is-for-sale-all-over-the-world

526 Markoff J., The tangled history of Facebook, New York Times 2007, http://www.nytimes.com/2007/08/31/business/worldbusiness/31iht-facebook.5.7340806.html

527 Phillips S., A brief history of Facebook, Guardian, 2007,www.guardian.co.uk/technology/2007/jul/25/media.newmedia

the list of approved networks, allowing it to reach a wider range of users. By 2005, Facebook allowed access to over 800 college and university networks as well as high-school networks.[528] In 2006, Facebook continued to expand its network base, allowing access to over 22,000 commercial organization networks.[529] The last major network expansion occurred in 2006, which allowed access to anyone over the age of 13 with a valid e-mail address.[530]

By expanding globally as well as attracting a wider range of age groups, Facebook has been able to continue its rapid growth. Facebook originated in the United States, but more than 80% of current Facebook users now live outside the United States, and the majority of new growth is occurring internationally, with Facebook available in over 70 languages.[531] In addition to the growing global diversity of users, the typical age of Facebook users has also shifted over the course of the network's growth. For example, Facebook originally targeted college-aged students, but in 2010 the fastest growing demographic group was users over the age of 34, representing 28% of users.[532]

Facebook is the world's largest social network - when Senator Lindsey Graham asked Zuckerberg to name his biggest competitor, Zuckerberg couldn't name one.[533] Facebook itself has 2.1 billion active monthly users, WhatsApp hit 1.5 billion earlier this year. In 2017 Facebook Messenger had 1.3 billion and Instagram had 800 million monthly active users.[534]

The original idea for the term Facebook came from Zuckerberg's high school (Phillips Exeter Academy). The Exeter Face Book was passed around to every student as a way for students to get to know their classmates for the following year. It was a physical paper book until Zuckerberg brought it to the internet.

---

528 Arrington M., 85% of college students use Facebook, TechCrunch, 2005, http://www.techcrunch.com/2005/09/07/85-of-college-students-use-facebook

529 Zywica J., Danowski J., The faces of Facebookers: Investigating social enhancement and social compensation hypotheses; predicting Facebook™ and offline popularity from sociability and self-esteem, and mapping the meanings of popularity with semantic networks, Journal of Computer-Mediated Communication, 2005, 14, 1–34.

530 Brown J. J., From Friday to Sunday: The hacker ethic and shifting notions of labour, leisure and intellectual property, Leisure Studies, 27, 2008, 395–409.

531 Facebook, Statistics of Facebook, Palo Alto, CA, 2012, http://newsroom.fb.com/content/default.aspx?NewsAreaId=22, Schonfeld, E. (2010). Facebook closing in on 500 million visitors a month. TechCrunch. Retrieved from http://techcrunch.com/2010/04/21/facebook-500-million-visitors-comscore/

532 Fletcher D., Friends (and moms) without borders, Time 2010, from http://www.time.com/time/video/player/0,32068,86888223001_1990764,00.html

533 Jeong S., Zuckerberg struggles to name a single Facebook competitor, April 2018, https://www.theverge.com/2018/4/10/17220934/facebook-monopoly-competitor-mark-zuckerberg-senate-hearing-lindsey-graham

534 Meyer D., What to Know About 'Freedom From Facebook,' the New Progressive Campaign to Break Up the Social Media Giant, May 2018, http://fortune.com/2018/05/21/facebook-monopoly-breakup-progressive-campaign-ftc/

Facebook is a phenomenon. In case of my work Facebook gives me a series of examples, how many abuses can be made in area of data security and data protection. Facebook is probably the first place in Internet where people freely and without proper understanding give details about almost every single information of their life. Names, photos, addresses, e-mail addresses, phone numbers and possibly many, many other. What is even more important Facebook works in the way that makes its users to give even more details. Details, which have commercial value. Every single time we "like" something, we look for profiles of our favourite band, or actor we create a kind of profile of ourselves. That can be used for directing specific adds to us. Above I have already written about selling this kind of information to Google or Yahoo.[535]

I already have mentioned problem of collecting data by Google for too long. Apparently, Facebook struggles with the same accusations. European Commission is trying to force Facebook into giving "Right to Oblivion" to its users. This will be regulations to force sites to remove content from the network, which you do not want there. Pilot project for the "Right to Oblivion" is already in place outside the EU, Norway. Its citizens may apply to the Advocate protection of personal data and ask for help in wiping inadvertently thrown from the network information.[536]

Not so long ago it was proved how easy Facebook logging details could be stolen. Eric Butler[537], a freelance web application and software developer, created Firesheep just to prove this point. When logging into a website, users usually start by submitting username and password. The server then checks to see if an account matching this information exists and if so, replies back to you with a "cookie" which is used by your browser for all subsequent requests. Firesheep, a Firefox[538] extension designed to demonstrate that apparently this is serious problem. Creator of the application did point out that websites have a responsibility to protect the people who depend on their services. They have been ignoring this responsibility for too long, and it is time for everyone to demand a more secure web. In his opinion, Firesheep will help the users win.[539]

At the beginning of 2010 EU Data Protection Group complained about privacy policies at the social networking site Facebook. Organization's complaints included concerns over the default Facebook privacy settings that leave most of the information users provide open to the public. The group is urging Facebook to

535 Czy dostrzegasz związek między prywatnością i zarobkami?, http://like-a-geek.jogger.pl/2010/09/15/czy-dostrzegasz-zwiazek-miedzy-prywatnoscia-i-zarobkami/

536 Czy KE nauczy Facebooka „zapominać" informacje użytkowników?, http://wyborcza.biz/biznes/1,100896,8622445,Czy_KE_nauczy_Facebooka__zapominac__informacje_uzytkownikow_.html

537 https://codebutler.com/

538 Internet browser - https://www.mozilla.org/en-US/firefox/new/

539 Firesheep - http://codebutler.com/firesheep

change its policy so that user's profile information is visible only to the people they choose, and to make their information visible to Internet search engines only on request.[540] It is not the first time when it is alleged that privacy policies in Facebook are too complicated for users.[541]

One of the biggest, if not the biggest abuses of all was when it appeared that Microsoft and Facebook are partnering on Bing, folding in information from 500 million Facebookers into Microsoft's search engine.[542] That caused other issues when over 100 million Facebook accounts were stolen and could be downloaded from BitTorrent network.[543]

In its 2012 IPO filing, Facebook announced that it intends to grow in the near future by expanding its global user base, increasing engagement by developing new social tools, improving the mobile experience, and creating more value for advertisers and users.[544]

Facebook's purchase of Whatsapp allows it to tap into a deluge of new user data. The merger could result in a new form of market dominance: 'data monopoly'. Now the EU Commission is set to examine the takeover. Facebook was prepared to fork out $19 billion (14 billion euros) for the comparatively small company Whatsapp. However, the text messaging service is only small in terms of staff. If you look at the user figures, Whatsapp resembles quite a giant: 30 million users in Germany and 450 million worldwide. They all volunteer a significant amount of personal data - information that Facebook is keen to harvest given that this is what their business is based on.

It is the first time the EU is examining the merger of two social networks and it is faced with the challenge of determining whether Facebook has become a "data monopolist" with the Whatsapp takeover - a key issue for data privacy activists.

It is also about answering the basic question of how you determine a monopoly in a market offering free "products". In the past a monopoly was defined by whether a company was able to set prices that are far higher than its own costs.[545] This procedure is void in markets where services are offered free of charge.

However, it is not just the sheer numbers that raise the price but also the advertising effectiveness. - Advertising customers favour websites that cater for

---

540 EU Data Protection Group to Facebook: Change Your Privacy Policies, http://www.macobserver.com/tmo/article/eu_data_protection_group_to_facebook_change_your_privacy_policies/

541 Facebook poprawia się pod presją krytyki, http://wyborcza.biz/biznes/1,101562,7949869,Facebook_poprawia_sie_pod_presja_krytyki.html, Facebook unveils changes to enhance privacy, http://www.theregister.co.uk/2010/10/06/facebook_groups/

542 Microsoft's Bing to slurp Facebook users' data and likes, Scrappy upstart teams with incumbent, http://www.theregister.co.uk/2010/10/13/bing_microsoft_facebook/

543 100 milionów facebookowych kont krąży w Sieci, http://gizmodo.pl/gadgets/7753/100_milionow_facebookowych_kont_krazy_w_sieci.html

544 http://www.vbprofiles.com/companies/3e122f809e597c10032cd724

545 Head of the Institute for Commercial and Business Law at Bonn University

targeted advertising because this increases the likelihood that customers will indeed make a purchase. Companies such as Facebook, which collect and evaluate a deluge of data that includes the interests and preferences of their users, have a clear bonus in this context. - Excessive advantage allows a company to set monopoly prices for its advertising space offerings. - If a user feels he must be part of a certain social network, the company can effectively dictate the conditions for accessing it.

However, do the anti-trust authorities have to look into this particular case? After all, nobody is forced to sign up to Facebook or Whatsapp. Apparently, these networks are so successful because they offer the greatest benefit. It is hard to probe it as does not create enough turnover here for the authorities to launch a probe.[546]

Facebook's chief executive Mark Zuckerberg said the WhatsApp acquisition supported the two companies' shared mission to better connect the world.[547] Though WhatsApp is not very popular in the United States, it is a key player in European countries, as well as in several major developing markets such as India and Brazil where the messaging service is extremely popular, especially among teenagers. The mobile-messaging service could help Facebook generate more growth from younger users that are no longer choosing the social network to communicate.

This acquisition will substantially increase the data pool for Facebook, which makes its money by mining and harvesting information.[548] It shows just how much our data is worth if Facebook is willing to pay $19 billion for it. Access to this data also improves insight into how people communicate.[549]

Zuckerberg did not make any statements on what Facebook planned to do with WhatsApp in terms of security. WhatsApp's servers will become Facebook's servers and there is nothing that prohibits them from combining and using this data.[550]

WhatsApp has said in the past that it places a lot of value on privacy. WhatsApp has been criticized for storing the address books from people's smartphones, but supposedly does not collect personal information such as name, gender, or age. Messages are deleted from servers once delivered.

While Facebook may be stressing privacy, what they can do is analyze the feed of information, for example intensity, number of pictures, emotionality and so on. Maybe they're not storing messages, but on a meta-level, you can tell a lot about someone from communication patterns. Even a minimum amount of data can reveal a lot about a person. Researchers at Cambridge University, for example, had determined with surprising accuracy that an analysis only of a person's Facebook

546 Facebook, a 'data monopolist'?, http://www.dw.com/en/facebook-a-data-monopolist/a-17788350

547 http://newsroom.fb.com/news/2014/02/facebook-to-acquire-whatsapp/

548 https://www.accessnow.org/

549 Slöetjes J., advisor to Dutch digital rights group Bits of Freedom. - https://www.bof.nl/home/english-bits-of-freedom/

550 Casagrande S., WhatsApp with your Facebook data?, February 20, 2014, https://www.dw.com/en/whatsapp-with-your-facebook-data/a-17446624

"likes" could determine a users' race, age, IQ, sexuality, substance use and political leaning. There will be a situation where Facebook knows who you are, how you communicate, what you do and who you do it with. This creates a big advantage for Facebook. They know things about you and you don't know what they know.[551]

Facebook appears to be following a strategy of acquiring or building a family of applications instead of simply strengthening its core social network with its purchase of WhatsApp, as well as its $1 billion acquisition of Instagram in 2012. It faces a smaller yet also significant counterpart with Google, Google+ and Picasa.[552]

However, in this day and age, it is impossible to avoid social networks. The point is: if we are to be engaged in society, there are social networks which weave their way into the fabric of our lives. But in order for consumers to avoid becoming the product that companies like Facebook are selling, individuals have to be more aware of what they are doing online. In addition, there needed to be sufficient privacy laws in place, which are strictly enforced.[553]

4.1.1. Abuses

As with any social networking site, Facebook is only as good as the content that users share. Therefore, a design that encourages content contribution improves the overall user experience.[554] But the sharing of content and personal information on Facebook comes with certain potential privacy risks, including unintentional disclosure of personal information, damaged reputation due to rumours and gossip, unwanted contact and harassment, vulnerability to stalkers or pedophiles, use of private data by a third party, hacking, and identity theft.[555] The tradeoff between potential benefits and risks that accompany privacy settings presents a dilemma, both for Facebook administrators and Facebook users. Facebook administrators have the incentive to keep security and access controls weak by design in order to encourage information exchange and increase their company's value to advertisers. Since

551 Casagrande S., WhatsApp with your Facebook data?, February 20, 2014, https://www.dw.com/en/whatsapp-with-your-facebook-data/a-17446624

552 Warzel Ch., These Confidential Charts Show Why Facebook Bought WhatsApp, Mac R., December 5, 2018, https://www.buzzfeednews.com/article/charliewarzel/why-facebook-bought-whatsapp

553 Casagrande S., WhatsApp with your Facebook data?, February 20, 2014, https://www.dw.com/en/whatsapp-with-your-facebook-data/a-17446624

554 Burke M., Marlow C., Lento T., Feed me: Motivating newcomer contribution in social network sites, [in:] Proceedings of the 27th International Conference on Human Factors in Computing Systems, New York, NY: ACM, 2009, p. 945-995

555 Boyd D. M., Facebook's privacy trainwreck: Exposure, invasion, and social convergence. International Journal of Research Into New Media Technologies, 14, 2008, 13–20, Debatin B., Lovejoy J. P., Horn A., Hughes B. N., Facebook and online privacy: Attitudes, behaviors, and unintended consequences. Journal of Computer-Mediated Communication, 15, 2009, 83–108, Taraszow T., Arsoy A., Shitta G., Laoris Y., How much personal and sensitive information do Cypriot teenagers reveal in Facebook?, [in:] Proceedings From 7th European Conference on E-Learning, Reading, England: ACI, 2008, p. 871-876

Facebook is currently by far the most popular social network site, his words come with significant effects for Internet users.

In the early years, the platform pushed users towards making more and more information about them publicly accessible by default.[556] In recent years, however, the company mostly stopped doing so and has respectably improved the ways users can control their privacy on Facebook at an interpersonal level.[557]

A 2012 secret experiment in which Facebook manipulated users' news feed to see whether certain kinds of content made users happy or sad, violated basic research ethics. There is a longstanding rule that research involving human subjects requires informed consent. The researchers clearly didn't get it. Facebook's TOS — like those of most Internet companies — are cleverly crafted so as to be virtually indecipherable to the average user but allow Facebook to do essentially whatever it wants commercially. It protects Facebook and its business practices, but it in no way provides the level of informed consent that is expected and required when doing research with human subjects. They do what they want and what is expedient. Like the rest of the tech giants, they then apologize, wait a bit and then try something new that's likely to be even more outrageous and intrusive. Silicon Valley calls this innovation, but it is simply a compete disrespect for societal norms and customs.[558]

It has come to light that Facebook ran an experiment with nearly 700,000 users in 2012, showing how it could manipulate emotions by showing users more positive or negative content in their News Feeds. Forbes points out[559] that Facebook made changes to its data use policy four months after the experiment, and yes, that bit about research was one of those changes. Yes, the current outrage will no doubt die down within the week, and Facebook will carry on being Facebook. And Facebook users will carry on using Facebook.[560]

It's no secret that Facebook shared user data[561] with device and software makers as part of its partnerships. Now, however, the scope of those deals is clearer. Facebook in the response to a House Energy & Commerce Committee request for data with a 747-page document detailing the social network's data sharing deals with other

556 The Evolution of Privacy on Facebook, http://mattmckeon.com/facebook-privacy/

557 Constine J., Facebook Stops Irresponsibly Defaulting Privacy Of New Users' Posts To "Public", Changes To "Friends", 2014, https://techcrunch.com/2014/05/22/sometimes-less-open-is-more/

558 Facebook Secret Research On Users' Emotions Is Unethical, Consumer Watchdog Says, https://www.consumerwatchdog.org/newsrelease/facebook-secret-research-usersâ€™-emotions-unethical-consumer-watchdog-says

559 http://www.forbes.com/sites/kashmirhill/2014/06/30/facebook-only-got-permission-to-do-research-on-users-after-emotion-manipulation-study/

560 Actually, Facebook Changed Its Terms To Cover That Experiment After It Was Over, http://www.consumerwatchdog.org/story/actually-facebook-changed-its-terms-cover-experiment-after-it-was-over

561 Lawler R., Facebook's on-device data sharing program included Huawei, Lenovo. The social network insists any data shared did not go to those companies' servers, June 2018, https://www.engadget.com/2018/06/06/facebook-huawei-lenovo/

companies. Facebook has shared user info with 52 firms, including Chinese firms like Alibaba, Huawei, Lenovo and Oppo. According to what Facebook shared, most of agreements involving sharing data ended at this point.[562]

Facebook had inadvertently allowed the profiles of up to 87 million people to be collected by the political data-mining firm Cambridge Analytica. The Federal Trade Commission has opened an investigation into Facebook following reports that a data analytics firm that had worked with the Trump campaign had improperly accessed names, "likes" and other personal information about tens of millions of the social site's users without their knowledge.[563]

One of the biggest issues here is a settlement Facebook reached with FTC in November 2011, ending an investigation that Facebook deceived users about the privacy protections they are afforded on the site. Among other requirements, the resulting consent decree mandated that Facebook must notify users and obtain their permission before data about them is shared beyond the privacy settings they have established. It also subjected Facebook to 20 years of privacy checkups to ensure its compliance.[564]

Entanglement with Cambridge Analytica may have violated the company's legal agreement with the federal watchdog agency. Whistleblowers in recent days contend that Cambridge Analytica collected information about users and their friends under a since-ceased policy governing third-party apps on Facebook – then kept that data even after Facebook asked that it be deleted.

In March 2018 it was reported by some newspapers that the UK-based political consulting firm, Cambridge Analytica had, in 2014, improperly obtained information on 87 million Facebook users without their consent. The number includes 2.7 million Europeans. According to Christopher Wylie, whistleblower and former Cambridge Analytica employee, the collection of data was initially made via a third-party App that 270 000 Facebook users had installed for a psychology test. A researcher in the UK, who obtained the permission of these initial users for research purposes, developed the App. Data of these users and of the friends of their friends were collected and passed to Cambridge Analytica, which used that data to target online voters/users with personalized political advertisements. The purpose was to manipulate their behaviour with the aim of helping Donald Trump win the

562 Fingas J., Facebook shared user data with 52 tech companies, June 2018, https://www.engadget.com/2018/06/30/facebook-shared-user-data-with-52-tech-companies/?sr_source=Twitter&guccounter=1

563 Romm T., Timberg C., FTC opens investigation into Facebook after Cambridge Analytica scrapes millions of users' personal information, March 2018, https://www.washingtonpost.com/news/the-switch/wp/2018/03/20/ftc-opens-investigation-into-facebook-after-cambridge-analytica-scrapes-millions-of-users-personal-information/?noredirect=on&utm_term=.7f2e14cdafeb

564 Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises, November 2011, https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep

US presidential election in 2016. It happened despite Facebook announcing in 2014 that they had made changes to restrict app developers' access to data.[565]

In reaction to this news, in Europe, first the European Parliament President Antonio Tajani released a statement on 19th of March 2018. With this, he confirmed the commitment of the EP to investigate fully on allegations of misuse of data considered as an unacceptable violation of citizens' privacy rights.[566] On 12th of April, the EP invited Facebook's CEO Zuckerberg to explain himself.[567] After the explanations received by Commissioner Jourova were unsatisfactory, it was promised that all possible legal measures and stronger enforcement granted by the GDPR will be taken.[568] In addition, the WP29 issued a statement in which Facebook's apologies are said to be not sufficient, and the establishment of a Social Media Working Group was announced.[569] European Data Protection Supervisor Giovanni Buttarelli, in Opinion from 19th of March 2018, affirmed that what had happened with Cambridge Analytica was not a mistake, but a symptom of a predominant business model, and thus relying on the goodwill of tech companies to regulate themselves is not enough.[570]

As a result, a non-binding EP's resolution was adopted in plenary 5th of July 2018 and it deemed the Privacy Shield not adequate to protect individuals' rights.[571]

The possibility to suspend the data-exchange deal was provided for in Directive 95/46 and is set out now in the GDPR which states that if there is not adequate protection, data transfers should be suspended. EU data protection authorities are also called on to take enforcement actions and to suspend transfers when they are informed of non-compliant companies.[572]

---

565 Puccio L., Monteleone S., The Privacy Shield: Update on the state of play of the EU-US data transfer rules, https://www.academia.edu/37345183/The_Privacy_Shield_Update_on_the_state_of_play_of_the_EU-US_d, p. 27

566 Statement by Antonio TAJANI, EP President on the Facebook data crisis, 21/03/2018, https://multimedia.europarl.europa.eu/en/statement-tajani-cambridge-analytica-issue_I152975-V_v

567 Bodoni S., Stearns J., Zuckerberg Asked to Explain Himself in European Parliament, April 12, 2018, https://www.bloomberg.com/news/articles/2018-04-12/zuckerberg-asked-to-explain-himself-in-european-parliament

568 Stupp C., Cambridge Analytica harvested 2.7 million Facebook users' data in the EU, Apr 6, 2018, https://www.euractiv.com/section/data-protection/news/cambridge-analytica-harvested-2-7-million-facebook-user

569 WP29 Press Release, "Sorry is not enough": WP29 establishes a Social Media Working Group, Brussels, 11 April 2019, https://edps.europa.eu/sites/edp/files/publication/18-04-11_wp29_press_release_en.pdf

570 European Data Protection Supervisor, Opinion 3/2018, EDPS Opinion on online manipulation and personal data, https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf

571 EP resolution of 5 July 2018, Adequacy of the protection afforded by the EU-US Privacy Shield, http://www.europarl.europa.eu/doceo/document/TA-8-2018-0315_EN.html?redirect

572 Puccio L., Monteleone S., The Privacy Shield: Update on the state of play of the EU-US data transfer rules, https://www.academia.edu/37345183/The_Privacy_Shield_Update_on_the_state_of_play_of_the_EU-US_d, p. 29

A study[573] commissioned by the Belgian Privacy Commission (BPC) has found that Facebook is tracking all users of its social networking site, even if they've opted out of tracking. The research also found that logged out users, and people who don't have an account at all, were having their Web movements tracked by Facebook through its use of social plugins, primarily the 'Like' button.

Under EU law, any website must get the user's permission before placing any cookies on their computer. Among other practices, it's the automatic placement of tracking cookies that interact with its social plugins found on millions of different websites, that puts Facebook "violation of European law," the study said. Facebook disputes the accusations.

To be accurate Facebook has a different view on this matter. They opposed this report stating that it contains factual inaccuracies. Apparently, the authors have never contacted Facebook, nor sought to clarify any assumptions upon which their report is based. Neither did they invite the companies' comment on the report before making it public. Facebook have explained in detail the inaccuracies in the earlier draft report (after it was published) directly to the Belgian DPA and have offered to meet with them to explain why it is incorrect, but they have declined to meet or engage with them.[574]

Advertising revenue is Facebook's biggest source of income, jumping 45% already in 2015, with mobile ad sales accounting for 78% of that. Being able to track web-browsing habits, even anonymised ones, allows it to better target that advertising.

The internet has always been offered for free and, the argument goes, people would not be prepared to pay cold, hard cash for services from the likes of Facebook and Google[575], preferring instead to pay with their data.

Facebook has learnt from past mistakes that it has to treat user data with kid gloves, understanding that privacy is hugely important to its members. It allows users to opt out of having ads targeted at them by going to Settings, Adverts and then Advert Preferences but this does not stop Facebook collecting the information.

Cookies which track browsing habits have always been controversial and, in 2011, all EU websites were forced to get consent from visitors to store or retrieve any information on a computer, smartphone or tablet.[576]

---

573 Van Alsenoy B., Verdoodt V., Heyman R., Ausloos J., Wauters E., Acar G., From social media service to advertising network. A critical analysis of Facebook's Revised Policies and Terms, March 31, 2015, https://www.law.kuleuven.be/citip/en/news/facebook-1/facebooks-revised-policies-and-terms-v1-2.pdf

574 Facebook tracks logged-out users in 'violation' of EU law, study says, http://thenextweb.com/facebook/2015/03/31/facebook-tracks-logged-out-users-in-violation-of-eu-law-belgian-privacy-commission-says/

575 Also confirmed by Taj Montezano

576 What is Facebook doing with my data?, http://www.bbc.com/news/magazine-34776191

Another abuse is the fact that Facebook reads and in fact analysis private messages for advertising purposes.

Facebook was accused of violating state and US federal privacy laws by scanning the content of users' private messages in order to obtain advertising data. The facts are likely less sensational. While the security research, first reported in the Wall Street Journal, suggests that Facebook was indeed scanning messages to in order to slap new "Likes" on webpages, the process doesn't amount to what most people think of as "reading." Instead, the process is similar to Google's automated practice of scanning Gmail messages in order to serve relevant ads — a practice that a federal judge appeared to consider a violation of the Wiretap Act. Yahoo was also hit with a similar lawsuit. The Facebook case is based on the same law and amounts to the same accusation: that the company violated the Electronic Communications Privacy Act (a sub-section of the Wiretap Act) by tapping into private messages without permission.[577]

Facebook's privacy policies are constructed so that users agree to hand over more personal information in exchange for the right to use the service for free. Users still don't really get a say in how that data is used. Also, Facebook users have very little control over how their information is used in advertising. The company asserts the right to use anything you do on Facebook to help it target ads to you, both on and off the service. Facebook even tracks what you do on other websites and will use that information for advertising, too, unless you explicitly opt out of the extra tracking — an option that requires a trip to a third-party website or soon, the tweak of a setting on your mobile phone.

If you don't like the new arrangement, your option is the same as it has always been: don't use Facebook. And, yes, in fact it is a solution. Harsh one, primitive even, but even if Facebook is in my way of understanding one of the companies we cannot avoid, it is still a valid solution.

Facebook is in fact openly discussing its privacy policies and reminding consumers that many of its new features will also require more data disclosures. Still, there's also the reality that all of the messages about "privacy check-ups" and "you're in charge" serve to obscure the basic bargain at work here: consumers must pay in data to use Facebook's service.

A better solution, then, would be to give Facebook users the choice to pay with money instead of data. In practice, this could mean that Facebook users could pay a monthly subscription fee, and, in return, the company would agree not to share information about their likes, location or history with advertisers. The fee might be set at $5 a month — which seems reasonable given that some estimates set the ad

577 Facebook reads private messages to boost "Likes," lawsuit claims, https://gigaom.com/2014/01/02/facebook-reads-private-messages-to-boost-likes-lawsuit-claims/

value of each Facebook user at $128[578] — and could be adjusted lower for users who agreed to give up more data.[579]

There is a question whether Facebook could truly protect users' privacy given that it relies so heavily on collecting data about their lives and behavior.[580] Facebook makes money by profiling us and then selling our attention to advertisers, political actors and others. These are Facebook's true customers, whom it works hard to please. Facebook doesn't just record every click and "like" on the site. It also collects browsing histories. It also purchases "external" data like financial information about users (though European nations have some regulations that block some of this). Facebook recently announced its intent to merge "offline" data — things you do in the physical world, such as making purchases in a brick-and-mortar store — with its vast online databases. Facebook even creates "shadow profiles" of nonusers. That is, even if you are not on Facebook, the company may well have compiled a profile of you, inferred from data provided by your friends or from other data.

Everyone involved in the Cambridge Analytica data-siphoning incident did not give his or her "consent" — at least not in any meaningful sense of the word. It is true that if you found and read all the fine print on the site, you might have noticed that in 2014, your Facebook friends had the right to turn over all your data through such apps. (Facebook has since turned off this feature.)[581] If you had managed to make your way through a bewildering array of options, you might have even discovered how to turn the feature off. This wasn't informed consent. This was the exploitation of user data and user trust.

The group Europe-v-Facebook argued that it has to be taken into account the fact that Facebook has become a standard form of communication and that consent to a monopoly is hardly free.[582] There is the power asymmetry between individuals and Facebook that invalidates the consent, or at least should. Also, Irish Data Protection Commissioner questioned whether individual consent to Facebook privacy policies are informed as the user must read a multitude of documents in order to fully understand the use of their information and the options available to them.[583]

---

578 http://www.forbes.com/sites/georgeanders/2014/02/07/youre-worth-128-on-facebook-sorry-about-that-linkedin-drop/

579 Why it's time for Facebook to offer a "pay for privacy" feature, https://gigaom.com/2014/11/13/why-its-time-for-facebook-to-offer-a-pay-for-privacy-feature/

580 Newton C., The 5 biggest takeaways from Mark Zuckerberg's appearance before the Senate. Congress doesn't understand Facebook — does anyone?, April 2018, https://www.theverge.com/2018/4/10/17222444/mark-zuckerberg-senate-hearing-highlights-cambridge-analytica

581 Tufekci Z., Facebook's Surveillance Machine, https://www.nytimes.com/2018/03/19/opinion/facebook-cambridge-analytica.html

582 Europe-v-Facebook, Response to Audit by the Irish Office of the Data Protection Commissioner on Facebook Ireland Ltd., Vienna, 4 December 2012, 42: http://www.europe-v-facebook.org/report.pdf

583 Data Protection Commissioner, Facebook Ireland Ltd: Report of Audit, 21 December 2011, 39: http://www.dataprotection.ie/documents.facebook%20report/final%20report/report.pdf

In September 2019 it was revealed that Facebook has suspended tens of thousands of apps for a variety of violations, including improperly sharing private data. Facebook VP of Product Partnerships Ime Archibong said the move was part of an ongoing review that began in March 2018, following revelations that, two years earlier, Cambridge Analytica used the personal information of as many as 87 million Facebook users to build voter profiles for President Donald Trump's presidential campaign.[584]

The tens of thousands of apps were associated with about 400 developers. While some of the apps were suspended, in a few cases others were banned completely. Offenses that led to banning included inappropriately sharing data obtained from the Facebook platform, making data available without protecting user's identities, or clear violations of the social network's terms of service. One of the few apps Facebook identified was called myPersonality. Company claims that it shared information with researchers and companies with only limited protections in place, and then refused our request to participate in an audit.[585]

Finally, there are news from April 2021. We learned that 533 million (533,313,128 to be more exact) Facebook users' mobile number, Facebook ID, name, gender, location, relationship status, occupation, date of birth, and email addresses.[586] This Facebook data leak has been released for free on the same hacker forum for eight site "credits", a form of currency on the hacker forum, equal to approximately $2.19.[587] Here are some problems with this leak and some inconsistencies in what Facebook claims.

First Facebook has told the Irish Data Protection Commission that a breach took place prior to the entry into force of the EU's General Data Protection Regulation in 2018, and the company therefore chose not to notify the violation to the authorities.[588] Later the response was that the data leak was reported in 2019 and that the company patched the underlying vulnerability in August of that year.[589]

584 An Update on Our App Developer Investigation, 20 September, 2019, https://newsroom.fb.com/news/2019/09/an-update-on-our-app-developer-investigation/

585 Goodin D., Facebook suspends tens of thousands of apps in ongoing privacy investigation, 21 September, 2019, https://arstechnica.com/information-technology/2019/09/facebook-suspends-tens-of-thousands-of-apps-in-ongoing-privacy-investigation/

586 Holmes A., 533 million Facebook users' phone numbers and personal data have been leaked online, April 3, 2021, https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4?r=US&IR=T

587 Abrams L., 533 million Facebook users' phone numbers leaked on hacker forum, April 3, 2021, https://www.bleepingcomputer.com/news/security/533-million-facebook-users-phone-numbers-leaked-on-hacker-forum/

588 Stolton S., Facebook to Irish data body: 533 million user breach took place before GDPR, April 6, 2021, https://www.euractiv.com/section/data-protection/news/facebook-to-irish-data-body-533-million-user-breach-took-place-before-gdpr/

589 Newman L., What Really Caused Facebook's 500M-User Data Leak?, April 6, 2021, https://www.wired.com/story/facebook-data-leak-500-million-users-phone-numbers/

However, in fact, the data, which first appeared on the dark web in 2019, came from a breach that Facebook did not disclose in any significant detail at the time.[590] Ireland's Data Protection Commission confirmed it is working with the tech firm to establish if the dataset referred to is indeed the same as that reported in 2019.[591]

The list of abuses against privacy and data protection is long and literally every month is getting longer or we are learning about those from the past.

4.2. Google

If you think Americans google a lot, try Europe. Their Google controls more than 90 percent of the online search market. Portal to the internet, the internet in itself for some.[592]

So big and influential that when accused of abusing its dominant position on the EU market of search engines, first negotiations started, but when they failed in opinion of EU and EU commentators, the idea to break up the company followed. Along with that Google is facing possibility of being fined with the highest fine in the history of EU competition law – 5 billion dollars.

Google, which is based in Mountain View, Calif., has since morphed into a multi-faceted juggernaut relentlessly trying to muscle into new markets. The company now runs the world's most watched online video service in YouTube, the largest email service in Gmail and the most widely used operating system for mobile devices in Android. All of those services provide more opportunities to show the ads that generate the bulk of Google's revenue. Google is now the company facing the scrutiny of regulators – and Microsoft has been active in making those complaints. Google is certainly the biggest challenge that Microsoft has ever had to deal with.[593]

4.2.1. Abuses

Google is best known for its search engine. On this market it has undeniable domination with over 64 percent share.[594] Since 2004, Google's e-mail service called Gmail has gained market rapidly.[595] Another popular service is AdWords which

590 Clark M., The Facts on News Reports About Facebook Data, April 6, 2021, https://about.fb.com/news/2021/04/facts-on-news-reports-about-facebook-data/

591 Facebook leak: Irish regulator probes 'old' data dump, April 6, 2021, https://www.bbc.com/news/technology-56639081

592 Desjardins J., How Google retains more than 90% of market share, April 23, 2018, https://www.businessinsider.com/how-google-retains-more-than-90-of-market-share-2018-4?r=US&IR=T

593 Microsoft escalates ad assault on Google, April 9, 2013, https://eu.usatoday.com/story/tech/2013/04/09/microsoft-google-advertising/2066991/

594 Bing's Market Share Up 51% In Past 12 Months.

595 Email and webmail statistics, http://www.email-marketing-reports.com/metrics/email-statistics.htm

allows creating and running ads for business.[596] AdWords is in my opinion one of the most controversial Google services. This is the reason for Google to collect personal data of people using search engine and Gmail. Also, to make AdWords more efficient, Google buys this kind of information from, for example Facebook.[597]

Google has dominant position in almost every EU Member State, with a market share of up to 95% in some national search engine markets. The company has a significant role in European citizens' daily lives and company's apparent lack of focus in data retention is concerning for European Union.[598]

In the beginning of 2015, The European Union has accused Google of cheating competitors by distorting internet search results in favour of its own shopping service as it laid formal charges against the US technology company. Dominant companies have a responsibility not to abuse their powerful market position by restricting competition with others in markets where they are dominant or in neighbouring markets. Yet, in general search results, Google artificially favours its own company's shopping service and that this constitutes an abuse - The EU's five-year inquiry found that in Google searches, the US firm gave prominence to its own comparison-shopping services, regardless of their relevance to the search query, which diverted traffic away from competitors.

In a blog post[599], Google argued that internet users had more choice than ever before and could access information in multiple ways. Google respectfully but strongly disagree with the need to issue a statement of objections and look forward to making their case in coming future. It is rather widely believed that without legal action, Google would have continued to ignore European competition rules. Google had 10 weeks to respond to the antitrust charges, with a potential fine of up to 10% of its annual turnover – or $6bn (£4bn) – now hanging over its head. A separate EU investigation has been launched into incentives offered by the internet search giant to smartphone manufacturers to pre-install and bundle apps and services on its Android operating system, used by manufacturers such as Samsung, HTC and Sony. Additionally, EU would investigate whether Google was hindering smartphone and tablet manufacturers from "forking" Android, using the free codebase that underpins the operating system to develop competing software free of Google's influence. Android is the world's largest operating system, with an 81%

596 What is Google AdWords?, http://adwords.google.com/support/aw/bin/answer.py?hl=en&lev=+index&cbid=1gwv7dnfyp5n4&answer=6084&src=cb

597 Facebook is 'killing privacy for commercial gain', http://www.theregister.co.uk/2010/10/12/schneier_rsa_keynote_facebook/, WSJ: Facebook i MySpace łamały własne zasady prywatności, http://wyborcza.biz/biznes/1,101562,7915409,WSJ__Facebook_i_MySpace_lamaly_wlasne_zasady_prywatnosci.html

598 EU says Google and Microhoo still violate data protection law, 'Your anonymization doesn't anonymize', http://www.theregister.co.uk/2010/05/26/eu_says_google_microsoft_and_yahoo_still_do_not_comply_with_data_retention_laws/

599 The Search for Harm, https://googleblog.blogspot.co.uk/2015/04/the-search-for-harm.html

share[600] of the smartphone market, according to some estimates, giving rise to fears about market dominance. Google's web search market share is over 90% in Europe, and Microsoft, TripAdvisor, Streetmap and others, brought the complaint against it in Europe.

There are some concerns, though. The European commission should take care to ensure that its investigation focuses on substantive breaches of EU competition law and not be dragged into a politically motivated protectionist battle with the US. In addition, the European consumer organisation BEUC welcomed what it saw as EU enforcement of a non-discrimination principle that would allow citizens to get fair and neutral search results. It is important to remember that manipulating search results leads to broader problems for Europe's digital economy, as Google's market share means it essentially decides which companies are placed in the shop window. Such control restricts access, thereby reducing competition and resulting in less consumer choice.

Google is not resting in criticizing EU legal actions in the area of competition law and has described the European commission's antitrust case against its search engine business as "wrong as a matter of fact, law and economics" in a lengthy counter submitted to the regulator. Google's response, which runs to more than 100 pages, is confidential. However, the company's general counsel Kent Walker outlined his defence in a blog post[601], saying that far from harming rival shopping price comparison services, the Google had increased traffic to their sites. He said that over the last decade, the company had delivered 20bn free clicks to rival price comparison sites, with free traffic – as opposed to traffic acquired by paying for adverts on Google – increasing by 227%. Google claims the commission has defined its competitors too narrowly and says Google shopping should be seen as operating in a field that includes big retailers like Amazon and marketplaces like eBay, where shoppers frequently go to compare prices. Far from being harmed by Google, these retail businesses are growing fast. He also rejected the commission's proposed remedy. EU wants Google to use the advertising box at the top of its results page to show products sourced and ranked by other price comparison services, not just Google shopping. The company argues that implementing this would be technically difficult, produce poor quality search results, and that the solution is not legally justified. If Google's defence is unsuccessful, it could in theory be fined up to 10% of the previous year's turnover. Google revenues were $66bn (£43bn) in 2014.[602]

600 Android dominates 81 percent of world smartphone market, http://www.cnet.com/uk/news/android-dominates-81-percent-of-world-smartphone-market/

601 Improving quality isn't anti-competitive, http://googlepolicyeurope.blogspot.co.uk/2015/08/improving-quality-isnt-anti-competitive.html

602 Google attacks Brussels antitrust case in 100-page response, http://www.theguardian.com/technology/2015/aug/27/google-attacks-brussels-antitrust-case-european-commission-shopping-price-comparison

The European Commission has decided to open an antitrust investigation into allegations that Google Inc. has abused a dominant position in online search, in violation of European Union rules (Article 102 TFEU). The opening of formal proceedings follows complaints by search service providers about unfavourable treatment of their services in Google's unpaid and sponsored search results coupled with an alleged preferential placement of Google's own services. This initiation of proceedings did not imply that the Commission has had proof of any infringements at the time. It only signifies that the Commission will conduct an in-depth investigation of the case as a matter of priority.

The Commission will investigate whether Google has abused a dominant market position in online search by allegedly lowering the ranking of unpaid search results of competing services which are specialised in providing users with specific online content such as price comparisons (so-called vertical search services) and by according preferential placement to the results of its own vertical search services in order to shut out competing services. The Commission will also look into allegations that Google lowered the 'Quality Score' for sponsored links of competing vertical search services. The Quality Score is one of the factors that determine the price paid to Google by advertisers.[603]

European Parliament took a vote that could encourage a breakup of Google. The action related to Google was part of a broader resolution from the Parliament, which represents the European Union, having to do with the digital economy.[604]

Google is estimated to have a larger market share on the continent than in the United States, China, and many other big countries. But partly because Google holds such a dominant position, regulators and lawmakers in Europe have scrutinized it intensely, especially in recent years. – Which is quite similar to what EU Commission did over years against Microsoft.[605]

In the US, a two-year investigation by the Federal Trade Commission into similar issues ended in 2013 with the commissioners deciding that Google hadn't broken the law.[606] Google's competitors have objected to the company's proposals for settlements, which included ideas like letting competitors pay to have their results shown alongside Google's own.

---

603 Antitrust: Commission probes allegations of antitrust violations by Google, http://europa.eu/rapid/press-release_IP-10-1624_en.htm

604 Vara V., Europe versus Google, November 29, 2014, https://www.newyorker.com/business/currency/europe-versus-google

605 Rosoff M., Here's How Dominant Google Is In Europe, November 29, 2014, https://www.businessinsider.com/heres-how-dominant-google-is-in-europe-2014-11?r=US&IR=T

606 Wyatt E., A Victory for Google as F.T.C. Takes No Formal Steps, January 3, 2013, https://www.nytimes.com/2013/01/04/technology/google-agrees-to-changes-in-search-ending-us-antitrust-inquiry.html

Europeans are picking on Google and even on other US companies: There have also been signs of tension with other U.S. companies—for instance, antitrust settlements with Microsoft, cabbies in London and Madrid protesting against Uber, and scrutiny of Amazon and Apple's tax policies. The vote, once complete, was covered widely in the U.S. as a potential sign of trouble for Google.[607]

In a letter to European Parliament leaders in the run-up to the vote, twelve American members of Congress wrote that the resolution "would deter continued innovation and investment from U.S. based Internet companies."

For one thing, the vote is nonbinding. It's up to the European Commission, which is separate from the Parliament, to decide how to handle the ongoing antitrust case against Google. A spokesman for Margrethe Vestager, said that the vote wouldn't influence the commissioner, and that antitrust matters should be independent from politics.

And, while the resolution is seen in the U.S. as targeting Google in particular and American companies in general, the language itself reflects a preoccupation not with the U.S. but with Europe's own difficulties: laying out the policies that Parliament supports and covering topics ranging from net neutrality to online privacy. It focusses on what E.U. lawmakers have called the "digital single market"—a strong, homegrown, transcontinental digital economy that could hasten Europe's recovery from recession. The phrase "digital single market" appears almost thirty times in the text.[608]

European lawmakers may seem at times to be targeting US companies out of some sense of cultural spite, but it probably just looks like that because the US happens to be the home of many of the powerful Internet companies against which Europe's smaller digital firms are competing, often without much success. In the Internet industry, it can be very difficult for newcomers to fight effectively against large, entrenched incumbents with well-established user bases. If Europe wants to pursue policies to help its homegrown companies, which seems to be one of the Parliament's goals, it's only natural that big US companies will bear the brunt of many of those policies. But this may have little to do with anti-Americanism; Europe is concerned mostly with saving itself.[609]

607 Vara V., Europe versus Google, November 29, 2014, https://www.newyorker.com/business/currency/europe-versus-google

608 Scott M., Larger T., To take on Big Tech, US can learn antitrust lessons from Europe, August 25, 2019, https://www.politico.eu/article/europe-us-big-tech-competition-antitrust-apple-google-facebook-amazon/

609 Vara V., Europe versus Google, November 29, 2014, https://www.newyorker.com/business/currency/europe-versus-google

Although merely symbolic — the resolution carries no legal weight — the move came the day after a separate European body sought to further expand citizens' "right to be forgotten" privacy protections against Google.[610]

Policy-making activity being devoted to the company signifies the growing antipathy to American technological dominance in the European Union even as its citizens grow ever more reliant on its gadgetry and conveniences.

Breaking up Google would be unprecedented in all kinds of ways and seems hugely unlikely in absence of massive, proven consumer harm — and it's very unclear to me whether the commission is going to find that harm. The power of the commission to break up companies was made explicit in 2003. In a landmark case in 2008, the German energy utility E.ON agreed to sell its extra-high-voltage network as part of a settlement, not something unilaterally imposed on the company.

The largest single fine yet levied in such a case was 1.1 billion euros, or $1.37 billion, in 2009 against Intel for abusing its dominance in the computer chip market. But Microsoft underwent a series of investigations and settlements, racking up a total of more $3 billion in European fines over the course of a decade, including a penalty in 2013 for failing to adhere to an earlier settlement.[611]

In 2017, Google was hit with a €2.42 billion ($2.7 billion) fine by the European Union for breaking Eu competition laws. The decision[612] follows a seven-year investigation into the US company's search algorithms, which ended with the judgement that Google had "abused its dominant position by systematically favoring" its own shopping comparison service. Today's fine is the largest antitrust judgement handed out by the executive body of the EU, the European Commission, topping a €1 billion penalty given to Intel in 2009.

The primary target of the case was Google Shopping, a price-comparison feature built into the company's search engine. The commission's antitrust filing states that Google showed users results from Google Shopping irrespective of their merits, depriving rival price comparison sites of traffic. The EU argues that because Google is so overwhelmingly dominant in Europe, it should not be allowed to actively undermine competitors.[613]

---

610 Kanter J., E.U. Parliament Passes Measure to Break Up Google in Symbolic Vote, November 27, 2014, https://www.nytimes.com/2014/11/28/business/international/google-european-union.html

611 European Union Parliament Backs Break Up of Google, November 28, 2014, https://www.medianews4u.com/european-union-parliament-passes-measure-to-break-up-google-in-symbolic-vote/

612 European Commission - Press release, Antitrust: Commission sends Statement of Objections to Google on comparison shopping service; opens separate formal investigation on Android, Brussels, 15 April 2015, https://europa.eu/rapid/press-release_IP-15-4780_en.htm

613 Vincent J., Google fined a record €2.4 billion by the EU for manipulating search results, 27 June, 2017, https://www.theverge.com/2017/6/27/15872354/google-eu-fine-antitrust-shopping

In a press statement[614], EU competition commissioner Margrethe Vestager praised Google for coming up with *many innovative products and services that have made a difference to our lives*. But added that the company also *abused its market dominance as a search engine by promoting its own comparison-shopping service in its search results and demoting those of competitors*.

In 2018, Google has been hit with a record-breaking €4.3 billion ($5 billion) fine by EU regulators for breaking EU competition laws. The European Commission concluded[615] that Google has abused its Android market dominance in three key areas:

1. Google has been bundling its search engine and Chrome apps into the operating system,
2. Google has blocked phone makers from creating devices that run forked versions of Android,
3. Google "made payments to certain large manufacturers and mobile network operators" to exclusively bundle the Google search app on handsets.

That means Google will need to stop forcing manufacturers to preinstall Chrome and Google search in order to offer the Google Play Store on handsets. Google will also need to stop preventing phone makers from using forked versions of Android, as the commission says Google "did not provide any credible evidence that Android forks would be affected by technical failures or fail to support apps." Google's illegal payments for app bundling ceased in 2014 after the EU started to look into the issue. The $5 billion fine decisively exceeds Google's previous $2.7 billion record-breaking fine from the EU last year over manipulated search results.

In 2019, Google has been hit with a new antitrust fine from the European Union totaling €1.5 billion.[616] The tech giant had abused its dominant position by forcing customers of its AdSense business to sign contracts stating they would not accept advertising from rival search engines. According to Commissioner Vestager the misconduct lasted over 10 years and denied other companies the possibility to compete on the merits and to innovate.

The fine is the third major penalty the EU has levied against the tech giant in as many years and closes its last open probe of the firm. Google was fined a record €4.3 billion in 2018 for abusing its market dominance in mobile, and €2.4 billion in

614 European Commission - Press release, Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service, Brussels, 27 June 2017, https://europa.eu/rapid/press-release_IP-17-1784_en.htm

615 Antitrust: Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google's search engine, Brussels, 18 July, 2018, https://europa.eu/rapid/press-release_IP-18-4581_en.htm

616 European Commission - Press release, Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising, Brussels, 20 March 2019, https://europa.eu/rapid/press-release_IP-19-1770_en.htm

2017 that for manipulating shopping search results. Google is currently appealing both cases.

The policy under scrutiny dates back to 2006. Then, Google started selling customers its AdSense for Search product. This let companies like retailers and newspapers place a Google search box on their website. When visitors used the search box, Google showed them ads and split the commission with the website's owners. Google also made customers sign contracts forbidding them from including rival search engines on their sites alongside Google's own. In 2009, Google allowed the inclusion of rival search engines as long as Google's was more prominent. In 2016, around the time the EU announced its case, the company removed these terms altogether.[617]

Google is absolutely doing that in the US as well. But in the US you've got your First Amendment. And basically, search results have been classified as speech. A lot of people think that Google search results are neutral - that they are just showing what is most relevant to the user. In many cases, that's simply not true. But because of free speech laws in the US, nobody can change those practices in that country.[618]

Google's been trying to make concessions to the European Commissions, but it keeps finding itself up against the complainants, which have largely been backed by Microsoft - has been a very important player in that. Yelp has piled in. And you've also got the big European press publishers who are also pushing back. So every time Google tries to make concessions, these people go no, that's not good enough.[619]

While Google did not comment on the matter, the Computer & Communications Industry Association lobbying group, whose members include Google, Facebook, Microsoft, eBay and Samsung, said the proposal of dividing Google is extreme and unworkable.[620]

The European Consumer Organisation has stepped up its involvement in the European Commission's antitrust investigation into how Google Inc. puts its preferred services atop search results while demoting rivals, particularly in price comparison searches. Currently an 'interested party', essentially having observer status, BEUC has today applied to be a formal complainant.[621]

Adequate answers have not been found to the problem of Google stacking its search results as suits itself. Users are given the impression their searches are

617 Vincent J., Google hit with €1.5 billion antitrust fine by EU, 20 March, 2019, https://www.theverge.com/2019/3/20/18270891/google-eu-antitrust-fine-adsense-advertising

618 Shapiro A., A Closer Look At EU Parliament's Vote To Break Up Google, November 28, 2014, https://www.kgou.org/post/closer-look-eu-parliaments-vote-break-google

619 A Closer Look At EU Parliament's Vote To Break Up Google, http://www.npr.org/2014/11/28/367244283/a-closer-look-at-eu-parliaments-vote-to-break-up-google

620 EU wants to divide and conquer Google, http://bgr.com/2014/11/28/eu-vs-google-search/

621 EU Google investigation: Adequate answers still not found. BEUC files complaint asserting consumer interest, http://blog.digitalmedialicensing.org/?p=1854

neutrally decided, and this problem is exacerbated in price comparison searches. That is why we are becoming formally involved in this process. European consumers deserve a better outcome, the remedies currently proposed by Google do not meet users' legitimate expectations. EU antitrust rules are there to protect fairness within the European Single Market. It is critical that a solution recognises a 'non-discrimination principle' and does its utmost to allow users to get back to searching, not being led.[622]

The proposals will do nothing to prevent Google from using universal search to squeeze out competitive vertical services. On the contrary, Google will now be able to profit not only from the traffic it diverts from competitors, but also from new possibilities to charge for inclusion among Rival Links. By requiring Google rivals to pay a price for their links, Google will be enabled to monetise its anticompetitive behaviour.

The European Commission's specific allegation is relatively benign; that the search giant has broken the law by giving Google Shopping a more favourable position in search results than its various rivals. Google doesn't just make Google Shopping results more likely to appear on top. It also monopolizes its own searches for Google Images, Google Maps, and Google News. All these regularly show up in special boxes near the top of Google search results. If it's illegal to place Google Shopping results above other search results, it should also be just as illegal to give special treatment to Google's other specialized search products for maps, news, or images.[623]

The European Commission complains that "Google systematically positions and prominently displays its comparison-shopping service in its general search results pages, irrespective of its merits," and that it has done so since 2008.[624]

The similarities of this case with the Microsoft Internet Explorer case are as disturbing as they are remarkable. Google is similar to Microsoft in using its dominance to leverage its market power from one market to another. In Microsoft the dominance in desktop operating systems was abused to push Internet Explorer; with Google the dominance in the online search is being used to push vertical services. However, the handling of the case by the European Commission is diametrically different. It is crucial that the European Commission uses its powers conferred by the Treaties to sanction Google for infringing EU competition rules.[625]

---

622 EU Google investigation: Adequate answers still not found. BEUC files complaint asserting consumer interest, http://www.beuc.org/publications/beuc-pr-2014-010_eu_google_investigation-beuc_complaint.pdf

623 Google vs the EU: Will Google Shut Down It's Search Engine Services in EU?, April 21, 2015, https://anonhq.com/dont-evil-eu-attempts-make-google-accountable-filling-statement-objections/

624 Google vs the EU: Will Google Shut Down It's Search Engine Services in EU?, http://anonhq.com/dont-evil-eu-attempts-make-google-accountable-filling-statement-objections/

625 Google case. Questions and Answers, http://www.beuc.org/publications/beuc-x-2014-025_ama_google_questions_and_answers_april_2014.pdf

The European Commission's Competition Commissioner said that Google's proposed antitrust settlement is inadequate and added he would seek further concessions from the Internet giant. Commissioner Joaquin Almunia's decision came in response to objections raised to the third proposed settlement deal released last February. Indeed, Consumer Watchdog, as well as our colleagues at BEUC (The European Consumer Organization) were among those objecting. [626]

Commission will open a formal investigation into Google's Android mobile operating system if regulators don't get "adequate" answers from the company to complaints. In the replies to Consumer's Watchdog letters the complainants have submitted new arguments and data, some of which should be taken in consideration.[627]

Each of three settlement proposals has taken months to negotiate and then each has proved inadequate. Google executives will only drag their feet again, while claiming to be "working with the European Commission." - Same what Microsoft was doing over years![628]

Consumers' Watchdogs called for breaking up Google in 2010. They called on the U.S. Department of Justice to launch a broad antitrust action against Google seeking remedial action that could include breaking the Internet giant into separate companies. The group said it is time to move beyond a reactive approach and actively restrain Google's broader ability to abuse both users and advertisers. Such action could include breaking Google Inc. into multiple separate companies or regulating it as a public utility. Google exerts monopoly power over Internet searches, controlling 70 percent of the US market. For most Americans – indeed, for most people in the world – Google is the gateway to the Internet. How it tweaks its proprietary search algorithms can ensure a business's success or doom it to failure.

Consumer watchdog suggested that the Justice Department could seek a variety of remedies:

- One possibility would be to break Google into different companies devoted to different lines of business.
- Google's importance as a gateway to cyberspace requires a maximum degree of openness and transparency with the potential for government regulation. Arguably Google's monopoly position and importance to the Internet means that the company should be regarded as a public utility and regulated.
- Another remedy would be to force Google to disgorge its monopolistic gains through the imposition of financial penalties. The payment would have

626 EU Rejects 3rd Google Antitrust Deal; It's Time For Formal Complaint, https://www.consumerwatchdog.org/blog/eu-rejects-3rd-google-antitrust-deal-itâ€™s-time-formal-complaint

627 Ibidem.

628 EU Rejects 3rd Google Antitrust Deal; It's Time For Formal Complaint, http://www.consumerwatchdog.org/blog/eu-rejects-3rd-google-antitrust-deal-it's-time-formal-complaint

> to be significant enough to impact Google's future behavior. Perhaps the amount could be tied to paying back consumers for monetizing their private information and content without compensating them.[629]

Consumer Watchdog urged the European Parliament to pass a resolution calling for the break-up of Google to end the Internet giant's monopolistic dominance, a remedy that the US public interest group proposed more than 8 years ago. It's long been clear that Google uses its search results to unfairly advantage its own services. John M. Simpson, Director of Consumer Watchdog's Privacy Project, proposed the break-up remedy to the US Department of Justice in April 2010.

While the European Parliament does not have the power to break up Google, Consumer Watchdog said passage of the resolution in US would increase pressure on the European Commission.

Google got itself into this jam by its arrogant abuse of its tremendous power. US consumers would be better served if senators and congressmen did so notice that, instead of standing on Google's side.[630]

So why "everyone" uses Google all the time, but it is not normal, or should not be considered normal. Try to change the search engine on your iPhone. There are three options and none of the other alternatives is a true alternative in Europe. Therefore, Google is simply the best product and basically with regard to search the only one. The fact is that a market dominating player who has a market share of 90 percent in Germany and in some Eastern European countries 99 percent - which makes it a de facto monopolist - needs to accept certain transparent and clear criteria that apply for all listings. At the moment Google downgrades certain products of competitors and upgrades their own products in the listing without disclosing it, so the costumer doesn't get the product with the highest traffic figures. Instead, the costumer gets the product that is a Google product perhaps on the first rank of the listing.[631]

The tech giant admitted that privacy is not a consideration when it comes to sending e-mail messages to or from a Gmail account. The brief was written in response to a class-action lawsuit in which Google was being sued for violating user privacy by reading e-mails in order to come up with targeted advertising. Just as a sender of a letter to a business colleague cannot be surprised that the recipient's assistant opens the letter, people who use web-based email today cannot be surprised if their emails

---

629 Consumer Watchdog Calls on Justice Department to Launch Antitrust Action Against Google, Including Possible Breakup, http://www.consumerwatchdog.org/newsrelease/consumer-watchdog-calls-justice-department-launch-antitrust-action-against-google-includ

630 Consumer Watchdog Urges European Parliament To Approve Call To Break Up Google, http://www.consumerwatchdog.org/newsrelease/consumer-watchdog-urges-european-parliament-approve-call-break-google

631 'Google is not like any other average company', http://www.dw.com/en/google-is-not-like-any-other-average-company/a-17753047

are processed by the recipient's (e-mail provider) in the course of delivery. Google's brief uses a wrong-headed analogy; sending an email is like giving a letter to the Post Office. Post Office is expected to deliver the letter based on the address written on the envelope and not the mail carrier to open the letter and read it.[632]

Meanwhile Microsoft has been executing an ad campaign that has compared its Outlook e-mail client to Gmail - making claims that Gmail was not protecting user privacy, while Microsoft had claimed that Outlook protected user privacy. From WikiLeaks founder Julian Assange report, we know that Google disrespects privacy. Something that Google had denied up for a long time.[633]

Google is making some impressions of carrying for privacy and data protection. When George Hotz dismantled the defences of Google's Chrome operating system, the company paid him a $150,000 reward – as a contrast to Sony who sued him and Apple that ignored him – for helping fix the flaws he'd uncovered. Two months later Chris Evans, a Google security engineer, followed up by email with an offer: How would Hotz like to join an elite team of full-time hackers paid to hunt security vulnerabilities in every popular piece of software that touches the internet?

Project Zero

Additionally, there is a Project Zero, a group of top Google security researchers with the sole mission of tracking down and neutering the most insidious security flaws in the world's software. Those secret hackable bugs, known in the security industry as "zero-day" vulnerabilities, are exploited by criminals, state-sponsored hackers and intelligence agencies in their spying operations. By tasking its researchers to drag them into the light, Google hopes to get those spy-friendly flaws fixed. And Project Zero's hackers won't be exposing bugs only in Google's products. They'll be given free rein to attack any software whose zero-days can be dug up and demonstrated with the aim of pressuring other companies to better protect Google's users. – but they already use it against other companies, i.e. Microsoft, however, not really showing them vulnerabilities.[634]

Project Zero has already recruited the seeds of a hacker dream team from within Google: New Zealander Ben Hawkes has been credited with discovering dozens of bugs in software like Adobe Flash and Microsoft Office apps in 2013 alone. Tavis Ormandy, an English researcher who has a reputation as one of the industry's most prolific bug hunters most recently focused on showing how antivirus software can include zero-day flaws that actually make users less secure. American hacker prodigy

632 Gibbs S., Gmail does scan all emails, new Google terms clarify, April 15, 2014, https://www.theguardian.com/technology/2014/apr/15/gmail-scans-all-emails-new-google-terms-clarify

633 Google Inc.: Is Microsoft Corporation Right, and Will This Affect Gmail Use?, http://www.consumerwatchdog.org/story/google-inc-microsoft-corporation-right-and-will-affect-gmail-use

634 Russel A., Meet 'Project Zero,' Google's Secret Team of Bug-Hunting Hackers, July 15, 2014, https://www.wired.com/2014/07/google-project-zero/

George Hotz, who hacked Google's Chrome OS defences to win its Pwnium hacking competition last March, will be the team's intern. And Switzerland-based Brit Ian Beer created an air of mystery around Google's secret security group in recent months when he was credited under the "Project Zero" name for six bug finds in Apple's iOS, OSX and Safari.

And what does Google get out of paying top-notch salaries to fix flaws in other companies' code?

- According to Google Project Zero is "primarily altruistic."
- also serve as a recruiting tool that brings top talent into Google's fold, where they may later move on to other teams.
- the company also argues that what benefits the internet benefits Google, because safe and happy users click on more ads. If the company increases user confidence in the internet in general, then in a hard-to-measure and indirect way, that helps Google too.
- Google's counter-surveillance measures have intensified in the wake of Edward Snowden's spying revelations. Google rushed to encrypt those links. More recently, it revealed its work on a Chrome plug-in that would encrypt users' email, and launched a campaign to name which email providers do and don't allow for default encryption when receiving messages from Gmail users.
- Project Zero is the logical next step in Google's anti-spying efforts.[635]

Google has for years paid "bug bounties"– rewards for friendly hackers who tell the company about flaws in its code. But hunting vulnerabilities in its own software hasn't been enough: The security of Google programs like its Chrome browser often depend on third-party code like Adobe's Flash or elements of the underlying Windows, Mac, or Linux operating systems.

When Project Zero's hacker-hunters find a bug, they say they'll alert the company responsible for a fix and give it between 60 and 90 days to issue a patch before publicly revealing the flaw on the Google Project Zero blog. In cases where the bug is being actively exploited by hackers, Google says it will move much faster, pressuring the vulnerable software's creator to fix the problem or find a workaround in as little as seven days.

Project Zero will choose its targets strategically to maximize so-called "bug collisions," the cases in which a bug it finds is the same as one being secretly exploited by spies. Modern hacker exploits often chain together a series of hackable flaws to defeat a computer's defences. Kill one of those bugs and the entire exploit fails.

635 Russel A., Meet 'Project Zero,' Google's Secret Team of Bug-Hunting Hackers, July 15, 2014, https://www.wired.com/2014/07/google-project-zero/

When George Hotz revealed his Chrome OS exploit in Google's hacking competition, another competition's contestants had simultaneously come up with the same hack. Google also learned of two other private research efforts that had independently found the same flaw — a four-way bug collision. Instances like that are a hopeful sign that the number of undiscovered zero-day vulnerabilities may be shrinking, and that a team like Project Zero can starve spies of the bugs their intrusions require.[636]

As mentioned, Google uses Project Zero to find vulnerabilities in other companies' products. Microsoft is not happy that Google's security folks are finding bugs in Windows and telling the world about them before Microsoft can fix the problems. Microsoft says it planned to release a fix for the bug as part of its usual monthly Patch Tuesday cycle in January, two days after Google's 90-day deadline. However, Microsoft also told Google that the patch itself was buggy and would be released in February, according to records made public by Google. Microsoft tries to release all patches on a predictable monthly cycle, to make it easier on enterprise customers who need to test each patch before deploying it. Google doesn't just pick on Microsoft. The team frequently finds bugs in Apple's products, and other software too.

Interestingly, these Google security gurus aren't disclosing bugs found in Google's own software in the same way. Their database comes up blank when searching for a list of bugs found in Google software.

It's not likely that many enterprises will be hacked because of Google's decision to release the code before Microsoft could patch it, though that is a risk.[637]

The ads, which have appeared online, on television and in print, as a part of campaign "Scroogled", depict Google as a duplicitous company more interested in increasing profits and power than protecting people's privacy and providing unbiased search results. This time, Microsoft was vilifying Google for sharing some of the personal information that it gathers about people who buy applications designed to run on smartphones and tablet computers powered by Google's Android software. Earlier ads have skewered Google's long-running practice of electronically scanning the contents of people's Gmail accounts to help sell ads and attacked a recently introduced policy that requires retailers to pay to appear in the shopping section of Google's dominant search engine.[638]

Google has evolved from an endearing Internet start-up to an imposing giant running Web and mobile services that vacuum intimate details about people's lives.

---

636 Russel A., Meet 'Project Zero,' Google's Secret Team of Bug-Hunting Hackers, July 15, 2014, https://www.wired.com/2014/07/google-project-zero/

637 Google Is Doing A New Thing To Tick Off Microsoft: Exposing Bugs In Windows 8, http://uk.businessinsider.com/googles-new-way-to-tick-off-microsoft-2015-1?r=US

638 Microsoft fuels advertising assault against Google, April 9, 2013, https://www.cbsnews.com/news/microsoft-fuels-advertising-assault-against-google/

Despite repeated management assurances about respecting personal privacy, Google has experienced several lapses that have resulted in regulatory fines, settlements and scorn around the world.[639]

Microsoft's latest ads revolve around concerns already raised by privacy watchdogs. Critics argue that Google hasn't adequately disclosed that customers' names, email addresses and neighbourhood locations are routinely sent to the makers of apps sold in Google's online Play store. Google says it shares a limited amount of personal information about customers to ensure they get better service and faster responses if any problems arise. The company says the practice is allowed under its terms of service — a document that most people rarely read in its entirety.[640]

Microsoft says it doesn't pass along personal details about customers buying apps for devices running its Windows Phone software. But there aren't as many Windows Phone users or apps for that system as there are for Android.[641]

Microsoft has tried to thwart Google by investing heavily in online services, to little avail. Since Google went public in August 2004, Microsoft's online division has accumulated more than $17.5 billion in operating losses. The losses include an accounting charge of more than $6 billion for Microsoft's acquisition of a Quantive, an online advertising service that didn't pan out. Google, meanwhile, has been steadily increasing profits and share of the Internet search market. Google processes about two out of every three search requests in the U.S. and handles an even larger percentage of queries in many parts of Europe.[642]

Google's market value has come from nearly $25 billion at the time of its initial public offering to over $1 trillion in January 2020.[643] Microsoft's market value has reached over $1.3 trillion in April 2020.[644] Apple Inc., a rival of both Google and Microsoft, has a market value hovering around $1.2 trillion in April 2020.[645]

---

639 Liedtke M., Microsoft Skewers Google For Giving Your Personal Data To App Developers, April 9, 2013, https://www.businessinsider.com/microsoft-skewers-google-for-giving-your-personal-data-to-app-developers-2013-4?r=US&IR=T

640 Liedtke M., Microsoft escalates advertising assault on Google, April 9, 2013, https://news.yahoo.com/microsoft-escalates-advertising-assault-google-131645123--finance.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmZpLw&guce_referrer_sig=AQAAAGD_v63Hkuh55idEUZyaP9mrBfU2e0YtNfUTXe94AB0mBvnOb98DJgzeaA_NrX5sdvEw-w3VyDBfyWciOydrIjlPK2X6o6UpZRgfFkqm3yvyOEFbNhv_9XYRZaCoUdJlg6ACH3ny4p-7WHsL6KKlV5QNt5YkH7nWw0sbwyPJ9hWRel

641 Warren T., Microsoft finally admits Windows Phone is dead, October 9, 2017, https://www.theverge.com/2017/10/9/16446280/microsoft-finally-admits-windows-phone-is-dead

642 Tech giants at war: Changing fortunes of Microsoft and Google, April 10, 2013, https://economictimes.indiatimes.com/corporate-industry/tech-giants-at-war-changing-fortunes-of-microsoft-and-google/slideshow/19470298.cms

643 https://ycharts.com/companies/GOOG/market_cap

644 https://ycharts.com/companies/MSFT/market_cap

645 https://ycharts.com/companies/AAPL/market_cap

The latest abuse comes from US. Google agreed to pay a $170 million fine and make changes to protect children's privacy on YouTube, as regulators said the video site had knowingly and illegally harvested personal information from children and used it to profit by targeting them with ads. The penalty and changes were part of a settlement with the Federal Trade Commission[646] and New York's attorney general[647], which had accused[648] YouTube of violating the federal Children's Online Privacy Protection Act, or COPPA.

Regulators said that YouTube, which is owned by Google, had illegally gathered children's data, including identification codes used to track web browsing over time, without their parents' consent. The site also marketed itself to advertisers as a top destination for young children, even as it told some advertising firms that they did not have to comply with the children's privacy law because YouTube did not have viewers under 13. YouTube then made millions of dollars by using the information harvested from children to target them with ads, regulators said.[649]

Although the settlement prohibits YouTube and Google from using or sharing children's data they have already obtained, Rohit Chopra, a Democratic commissioner, said that it did not hold company executives personally accountable for illegal mining of children's data. Another Democratic commissioner, Rebecca Kelly Slaughter, said that the agreement did not go far enough by requiring YouTube itself to proactively identify children's videos on its platform.[650]

The settlement requires Google to:

1. develop, implement, and maintain a system that permits YouTube channel owners to identify their content as child-directed, and that informs channel owners that child-directed content may be subject to COPPA;
2. provide annual COPPA compliance training to Google personnel responsible for managing the company's relationships with YouTube channel owners;
3. provide notice of its practices with respect to the collection, use, and disclosure of personal information from children, in compliance with the COPPA Rule; and
4. obtain verifiable parental consent before collecting personal information from children.

---

646 Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law. FTC, New York Attorney General allege YouTube channels collected kids' personal information without parental consent, 4 September, 2019, https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations

647 AG James: Google And Youtube To Pay Record Figure For Illegally Tracking And Collecting Personal Information From Children, 4 September, 2019, https://ag.ny.gov/press-release/2019/ag-james-google-and-youtube-pay-record-figure-illegally-tracking-and-collecting

648 Case No.: 1:19-cv-2642, https://www.ftc.gov/system/files/documents/cases/youtube_complaint.pdf

649 Singer N., Conger K., Google Is Fined $170 Million for Violating Children's Privacy on YouTube, 4 September, 2019, https://www.nytimes.com/2019/09/04/technology/google-youtube-fine-ftc.html

650 Singer N., Conger K., Google Is Fined $170 Million for Violating Children's Privacy on YouTube, 4 September, 2019, https://www.nytimes.com/2019/09/04/technology/google-youtube-fine-ftc.html

Google also is prohibited from benefitting from personal information previously collected from visitors to YouTube channels that are identified as having child-directed content. The settlement imposes additional reporting and recordkeeping obligations and permits both the FTC and New York Attorney General to monitor the company's compliance with the terms of the settlement.[651]

Google has announced that starting around January 1, 2020, the company will end behavioral advertising on content identified as child-directed, and will disable certain features, such as comments and notifications, on such channels. The company also voluntarily has committed to applying machine learning to detect content that is directed to children but that may not have been so identified by content creators. Finally, Google announced that it will expand the YouTube Kids platform, which previously was available only as a mobile app, to desktop.[652]

4.3. Microsoft

A decade ago, Microsoft was the world's most powerful technology company, with its Windows operating system and Office productivity software pervasive on personal computers. Microsoft's dominance had grown so extensive that US and European antitrust regulators spent years trying to rein in the Redmond, Wash., software company.[653]

Microsoft Corporation from Redmond in USA is one of the biggest IT companies in the world and the leader in computer applications innovations. Windows operational system by Microsoft is actually a standard accepted by most consumers. Microsoft through providing interoperability and integration of its own application with Windows secured very strong market position. Not only on market of operational system, but also on related markets, such as multimedia players, internet browsers and office applications.[654] Microsoft has also strong influence on markets of gaming consoles (~58 percent of the market[655]) and e-mail service (~28 percent of the market[656]) with a small portion of search engines market(~2.5

651 Case 1:19-cv-02642, https://www.ftc.gov/system/files/documents/cases/172_3083_youtube_coppa_consent_order.pdf

652 An update on kids and data protection on YouTube, 4 September, 2019, https://youtube.googleblog.com/2019/09/an-update-on-kids.html

653 Microsoft Skewers Google For Giving Your Personal Data To App Developers, http://www.consumerwatchdog.org/story/microsoft-skewers-google-giving-your-personal-data-app-developers

654 T. Skoczny, The Microsoft case before the European Commission and Court of First Instance [in:] D. Miąsik, T. Skoczny, M. Surdek (ed.), Microsoft – case study. Competition Law on the New Technology Markets, Warsaw 2008, p. 27.

655 Console Operating System Market Share Worldwide, March 2020, https://gs.statcounter.com/os-market-share/console/worldwide

656 Email Hosting, March 2020, https://www.datanyze.com/market-share/email-hosting--23

percent by Bing[657]). Together that gives a wide and constant access to personal data of literally millions of users.

4.3.1. Not only abuses

For last 10 years there have been numbers of cases before European Commission and the Court of First Instance[658] involving Microsoft abuses. All of those, concerned abuses of dominant position on several European markets, but never there was an issue of data protection or data security. Although, for years Microsoft's Internet Explorer was well known as a browser responsible for leak of information from users' computers. The brightest example is year 2006 when Internet Explorer was unsafe for 284 days. It took nine months to publish a patch by Microsoft to fix all vulnerabilities in IE. Even Microsoft labelled these vulnerabilities as "critical", which is the most severe rating. If the flaws could be exploited to criminal advantage without any action on the part of the user, or by merely convincing an IE user to click on a link, visit a malicious Web site, or open a specially crafted e-mail or e-mail attachment.[659] European Union institutions where focused all that time, not on dangers in data protection area that IE caused, but on danger for the market of internet browsers.

Today, Microsoft is mostly having problems because of its search engine Bing. These are very serious issues which indicates how substantial is role of search engines in area of data protection and data security.[660]

There are obvious benefits for Microsoft in presenting itself as a defender of student privacy through as many channels as possible, observers of the school-tech market say. The company, which offers cloud-computing services in schools and is a major provider of operating systems in K-12 education, is focusing on an issue that has surged in the consciousness of parents and school leaders and could become increasingly complex and problematic in the years ahead.

Microsoft clearly sees this is a good way of distinguishing themselves, mainly from Google mainly. Consumers are becoming more aware of privacy, and they want it.

Over the past year, Microsoft has helped keep student data-privacy issues in the spotlight in several ways. The company financially supported a widely circulated study released late last year by the Center on Law and Information Policy at Fordham University's law school that pointed to "substantial deficiencies" in district policies for protecting student data through cloud-based computing systems. Microsoft also

657 Search Engine Market Share Worldwide, March 2020, https://gs.statcounter.com/search-engine-market-share

658 The General Court (EGC) - From 1 January 1989 to 30 November 2009, it was known as the Court of First Instance (CFI).

659 Internet Explorer Unsafe for 284 Days in 2006, http://blog.washingtonpost.com/securityfix/2007/01/internet_explorer_unsafe_for_2.html

660 More in Facebook and Google section.

sponsored a guide to help school district leaders make decisions about privacy and ask precise questions about companies' practices, published this year by the Consortium for School Networking, or COSN, a Washington-based group representing district technology officials.

While it makes sense for Microsoft to market its privacy brand, having a business reason for doing that doesn't mean they don't believe what they do. The company might also expose itself to blowback if its performance in the fast-changing ed-tech marketplace doesn't keep up with its rhetoric. Privacy is a moving target and consumers keeps expecting more if something that Microsoft is doing doesn't match how they're positioning themselves the result might be very different from expected. According to some commentators Microsoft's interest in data privacy is long-standing.[661] Back in 200 then-company Chairman Bill Gates pledged that the company would improve privacy and security across its products.

Microsoft has a business model that has long compelled it to maintain strict data-privacy practices, several observers said. Much of Microsoft's business is derived from selling to large, protection-conscious companies and organizations in the public and private sectors. The company points out that major organizations, they cooperate with, typically expect data-privacy guarantees to be baked into contracts, and, therefore, for example school districts should expect the same.[662] Microsoft is trying to position itself in a major advertising campaign as a privacy friendly Internet company.

If Microsoft means what it says about protecting users' privacy, it should join Apple and Mozilla and start blocking cookies by default from sites not visited by the user. There is some reason to believe Microsoft will do the right thing. There is another approach to protecting online privacy, the Do Not Track mechanism. Under this method the browser sends a header expressing a user's desire not to be tracked. The FTC advocated this approach in its Protecting Consumer Privacy in an Era of Rapid Change report a year ago. All four major browsers now offer the option to send the message.

Microsoft has decided to send the Do Not Track message by default. Right now it's just a signal with virtually no listeners. Blocking cookies from sites a user never visited would provide meaningful protection right now. Microsoft must not hesitate to take that step in Internet Explorer, if it is actually the privacy protecting company it claims to be.[663]

---

661 http://www.microsoft.com/security/sdl/story/#chapter-1

662 Microsoft Puts Data Privacy on Its Branding Agenda, http://www.edweek.org/ew/articles/2014/07/09/36microsoft_ep.h33.html

663 Microsoft Should Act Now To Protect Online Privacy, http://www.consumerwatchdog.org/blog/microsoft-should-act-now-protect-online-privacy

Microsoft experiences are supposedly unique as they reason over information from work and life and keep a user in control of their privacy. Microsoft is helping put consumers in control in three ways:

1. Building privacy into policies and practices. Putting you in control means offering transparency, starting with company policies that provide simple and easy to understand explanations of how we use your personal information.
2. Building privacy into products. We design and build products with security and privacy in mind, from our software development processes to using best-in-class encryption to protect your data. These steps are critical to keeping your information safe.
3. Advocating laws and legal processes that keep people in control. We require governments around the world use legal process to request customer data. We have challenged laws to make privacy protections stronger. And we advocate for better public policy to balance privacy and public safety.[664]

Whether you know it or not, odds are you have an online reputation culled from what you share in the digital world and what others post about you. Microsoft promotes approach in which individuals of all ages to take charge of their digital reputations by regularly following some important guidance.

That guidance includes these tips:

1. Once posted, always posted: Think twice about posting comments, images or videos that you wouldn't want your employer to see. Share, but don't over-share!
2. Be knowledgeable about security and privacy settings. Control who sees what you post by judiciously using social networks' privacy settings. For example, you may want to limit the people who can see Facebook photos from your cousin's bachelor's party to just a close circle of friends.
3. Keep personal info personal. Don't make cyber-criminals' jobs easier by sharing sensitive information such as your address or other personal data.
4. Correct any inaccuracies. If you see information about yourself that's wrong or that you don't want to share online, take the necessary steps to correct it. If someone posts a photo of you on Facebook that you don't want others to see, untag yourself or ask the original poster to remove the photo altogether.

For more tips on how to nurture the online reputation you want, Micosoft dedicated whole Safety and Security Center[665]. In addition, the National Cyber

664 Data Privacy Day 2015 – Putting people in control, http://blogs.microsoft.com/on-the-issues/2015/01/28/data-privacy-day-2015-putting-people-control/

665 Protect your privacy on the Internet, http://www.microsoft.com/security/online-privacy/prevent.aspx

Security Alliance[666] has some great suggestions on the safest way to use social networks.[667]

Microsoft claims that their greatest asset is customer trust and their technologies are developed with data protection in mind. The priority is to protect personal data in an age where we support ubiquitous connectivity, pervasive online business and social networking, and flows and storage of information all over the world on all kinds of computers and devices. The efforts have a critical role to play in protecting privacy – a role that includes embedding privacy protection into products and services early in and throughout the design cycle and being transparent about how we collect and use data. Microsoft place particular value on transparency, because it is supposed to enable customers to make informed choices about how their data is used.

The challenge before Microsoft is still how to protect Europeans' privacy while also encouraging innovation and facilitating the productivity and cost-efficiency offered by new computing paradigms like the cloud. Microsoft believes that the GDRP adds a number of important measures that will help to achieve these goals, including requirements that companies design technologies with privacy in mind, be transparent about their processing activities, and remain responsible for how they use personal data. The Regulation also helpfully addresses inconsistent rules and interpretations across the EU Member States, reduces the administrative paperwork for companies, and improves mechanisms to transfer data safely outside of the EU. Which is very important point for Microsoft.

The Regulation in some places dictates not only what obligations apply, but also how those obligations should be implemented – moving the Commission beyond creating regulation to support privacy and into designing technology and business processes. According to Microsoft, right to be forgotten, data portability, and consent do not always reflect how the internet is technically structured today, what consumers want and need, or how technology is likely to evolve tomorrow. Obligations that cannot be properly implemented due to technical hurdles, or that frustrate data subjects, or that become obsolete when technology changes, will be of little lasting value.[668]

Microsoft would like the next generation of privacy regulation in the EU to achieve two ends: it must both provide transparency and robust protection to data

666 http://www.staysafeonline.org/

667 Before you post your next Lumia selfie on Facebook or tweet something clever, here are some social-media guidelines to help keep your online reputation safe. http://lumiaconversations.microsoft.com/2015/01/28/stop-think-connect-safeguarding-online-reputation/

668 Gonie J., The EU's Proposed Data Protection Regulation: Microsoft's Position, March 16, 2012, https://blogs.microsoft.com/eupolicy/2012/03/16/the-eus-proposed-data-protection-regulation-microsofts-position/

subjects as well as allow organisations to innovate while holding them accountable to achieving an appropriate level of data protection.[669]

However not everything is so clear and perfect with Microsoft. The $731 million fine European regulators put on Microsoft for failing to abide by an antitrust sanction, reinforces the European Union's longstanding insistence on fair competition. The huge penalty also signalled that Europe won't easily be swayed by Google and Facebook to back down from expanding online privacy rights for individuals.[670]

This puts a spotlight on how important it is for global companies to take into account the laws and customs of the places they do business. If they can't do that, they're almost begging for the sort of consequences the EU has administered to Microsoft.

Microsoft took full responsibility for failing to give European consumers a choice of Web browsers in shipping some 15 million copies of the Windows 7 operating system. That antitrust case began in 2004, and Microsoft paid fines of $357 million in 2006 and $1.3 billion in 2008 for being slow to comply with regulations. Microsoft cut a deal with the EU and failed to live up to it.[671]

The company didn't say whether it would challenge this latest fine but is not expected to do so as they even apologized for it. The $731 million fine represents about 1% of Microsoft's annual revenue. That's large enough to send a signal that Europe will sink its teeth into promoting fair competition. It also sends the message that Europe is likely to stand firm on consensus support for the hot issue of the moment: reinforcing online privacy.

The fine imposed on Microsoft shows that European authorities are serious about enforcement. The EU antitrust enforcers aren't going to roll over like the US Federal Trade Commission did with its investigation of Google. Some commentators expect European data protection authorities to take strong stands to enforce online privacy laws.[672]

669 Gonie J., The EU's Proposed Data Protection Regulation: Microsoft's Position, March 16, 2012, https://blogs.microsoft.com/eupolicy/2012/03/16/the-eus-proposed-data-protection-regulation-microsofts-position/

670 Whittaker Z., Microsoft fined $731m by EU in browser choice screw-up, March 6, 2013, https://www.zdnet.com/article/microsoft-fined-731m-by-eu-in-browser-choice-screw-up/

671 Acohido B., Microsoft apologizes for violating EU antitrust order, March 6, 2013, https://eu.usatoday.com/story/tech/2013/03/06/microsoft-eu-antitrust-fine-731-million/1969007/

672 European Regulators Hit Microsoft With $731 Million Fine, http://www.consumerwatchdog.org/story/european-regulators-hit-microsoft-731-million-fine

4.4. The role of Dominant ICT Companies

4.4.1. Impact on society

Today, companies aggregate and utilize personal information at an unprecedented scale. Powerful commercial parties have seized control of data pertaining to billions of people and built a pervasive, complex, dynamic, and opaque infrastructure that allows them – together with a wide array of other businesses – to constantly monitor, follow, sort, rate, and rank people as they see fit.

The corporate use of personal data can affect individuals, groups of people, and society at large, particularly in the context of automated decisions and data-driven personalization. Systems that make automated decisions about people based on their data produce substantial adverse effects. They are largely opaque, nontransparent, arbitrary, biased, unfair, and unaccountable – even in areas, such as credit scoring, that have long been regulated in some way. Through data-driven personalization, companies and other institutions can easily utilize information asymmetries in order to exploit personal weaknesses with calculated efficiency. Personalized persuasion strategies provide the means to effectively influence behaviour at scale; manipulative, misleading, deceptive, or even coercive strategies can be automated and customized down to the individual level.[673]

In their current state, today's corporate networks of digital tracking and profiling show a massive potential to limit personal agency, autonomy, and human dignity. This is not only a problem for individuals but one that affects society at large.[674]

Admittedly, changing the present tendencies is not an easy task. There are several challenges on a fundamental level. One of them is the need to be able to preserve the distinction between personal data and anonymity. The latter constitutes a basic foundation of all privacy and data protection legislation, but the access to large amounts of personal data, cross-linking between data sets, as well as through inferences and de-identification based on data analytics undermine it.[675]

Today's legal frameworks, not to mention the mechanisms of their enforcement, do not seem adequately prepared for a situation in which companies can control

673 Privacy Internationl, Data Is Power: Profiling and Automated Decision-Making in GDPR, 2017, https://privacyinternational.org/sites/default/files/2018-04/Data%20Is%20Power-Profiling%20and%20Automated%20Decision-Making%20in%20GDPR.pdf

674 Christl W., How Companies Use Personal Data Against People. Automated Disadvantage, Personalized Persiasion, and the Societal Ramifications of Commercial Use of Personal Information, 2017, https://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf

675 Barocas S., Nissenbaum H., Big Data's End Run around Anonymity and Consent, [in:] Lane J., Stodden V., Bender S., Nissenbaum H. (eds.), Privacy, Big Data, and the Public Good: Frameworks for Engagement, Cambridge University Press 2014, https://doi.org/10.1017/CBO9781107590205.004

data, digital environments, and experiences at such extensive levels.[676] The increased power imbalances between companies and consumers inherent to these data-driven environments as they currently exist. What is more, mitigating the pervasive collection, disclosure, trade, and use of personal data that today occurs across companies and largely happens without the subjects' knowledge and expectation.[677]

Stanford researchers have found that computers can judge personality traits more accurately than one's friends and colleagues. In fact, artificial intelligence can draw inferences about a person as accurately as a spouse, according to Stanford postdoctoral fellow Michal Kosinski. According to Kosinski, the findings reveal that by mining a person's Facebook "likes," a computer was able to predict a person's personality more accurately than most of their friends and family. Only a person's spouse came close to matching the computer's results.

It can be useful also to understand interaction between computer and human being: "This is an emphatic demonstration of the ability of a person's psychological traits to be discovered by an analysis of data, not requiring any person-to-person interaction. It shows that machines can get to know us better than we'd previously thought, a crucial step in interactions between people and computers."

"In this context," he added, "the human-computer interactions depicted in science fiction films such as Her seem not to be beyond our reach." He said the research advances previous work from the University of Cambridge in 2013 that showed that a variety of psychological and demographic characteristics could be "predicted with startling accuracy" through Facebook likes.

In the new study, researchers collected personality self-ratings of 86,220 volunteers using a standard, 100-item long personality questionnaire. Human judges, including Facebook friends and family members, expressed their judgment of a subject's personality using a 10-item questionnaire. Computer-based personality judgments, based on their Facebook likes, were obtained for the participants. The results showed that a computer could more accurately predict the subject's personality than a work colleague by analyzing just 10 likes; more than a friend or a roommate with 70; a family member with 150; and a spouse with 300 likes. "Given that an average Facebook user has about 227 likes (and this number is growing steadily), artificial

676 Calo R, Rosenblat A., The Taking Economy: Uber, Information, and Power, Columbia Law Review, Vol. 117, 2017; University of Washington School of Law Research Paper No. 2017-08, https://ssrn.com/abstract=2929643

677 Christl W., How Companies Use Personal Data Against People. Automated Disadvantage, Personalized Persiasion, and the Societal Ramifications of Commercial Use of Personal Information, 2017, https://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf

intelligence has a potential to know us better than our closest companions do," wrote Kosinski and his colleagues.[678]

Online tracking is pervasive and invasive on the Internet. The most insidious is performed by companies that most consumers don't even know exist, so-called 3rd parties on the websites you chose to visit. By putting little bits of computer code known as cookies on your browser, they are able to track your every move as you surf the web. Most people don't realize the extent to which this brazen online tracking is done, but when the practice is described, they want to be able to control it. Why should a company I know nothing about, have no say over and no relationship with be able to collect information about my online activity? On the other hand, though most consumers want some say over whether data is collected by sites they choose to visit, they are less concerned about such data collection by a site they have selected, a so-called first party. As long as we are tracked by the company which service we choose ourselves to use, we are not that much concerned about our privacy. It is the fact that also third-parties are using it, is what worries us. For example - Consider Amazon.com. If you buy a book from them, Amazon records what you've purchased and makes suggestions about other books you might like the next time you visit the site. Many people find that helpful and useful. - Understanding the distinction between tracking by sites you choose to visit (first parties) and sites with which you have no direct relationship (third parties), Apple's Safari browser by default has for a decade honoured the privacy friendly approach by blocking cookies from sites you haven't visited. If you want to allow 3rd party cookies to be set, you can change Safari's preferences. - Apple's approach isn't perfect. If you are committed, it is possible to fool the Safari browser. You'll recall that Google was caught hacking around Safari's privacy settings in violation of a consent agreement with the Federal Trade Commission and fined $22.5 million. Nonetheless, Safari's approach has been the most privacy friendly.[679]

User agreements are long and confusing and that more data is collected by Facebook than many users might realize.[680]

4.4.2. Impact on privacy

Other point of view, where biggest companies have positive impact on privacy by providing high quality encryption: US Attorney General Eric Holder said that

678 Parker C. B., Stanford research finds that computers are better judges of personality than friends and family, January 12, 2015, https://engineering.stanford.edu/magazine/article/stanford-research-finds-computers-are-better-judges-personality-friends-and-family

679 Microsoft Should Act Now To Protect Online Privacy, 2014, https://www.consumerwatchdog.org/blog/microsoft-should-act-now-protect-online-privacy

680 Domonoske C., Mark Zuckerberg Tells Senate: Election Security Is An 'Arms Race', April 2018, https://www.npr.org/sections/thetwo-way/2018/04/10/599808766/i-m-responsible-for-what-happens-at-facebook-mark-zuckerberg-will-tell-senate?t=1549538389858

officers should not be blocked from the information they need to investigate a crime. Apple's new iPhone 6 and Google's Android smartphones have data encryption so sophisticated that only the user may unlock it. Even law enforcement officers with search warrants would not have access. It is fully possible to permit law enforcement to do its job while still adequately protecting personal privacy. What is concerning about this is companies marketing something expressly to allow people to place themselves beyond the law.[681]

Yet another US official has played the "think of the children" card, taking Apple and Google to task for implementing stronger encryption policies in their mobile platforms. Child predators could use the encryption settings in mobile platforms to evade authorities and hide illegal images and content on their devices from law enforcement.[682]

In a new blog post[683], Microsoft president and chief legal officer Brad Smith argues that privacy is a human right and the Safe Harbor decision is an opportunity for stronger privacy regulations.

- The first step is to ensure that people's legal rights move with their data -- something Smith argues could be managed by an agreement that the U.S. would only demand access to personal information that belongs to Europeans in ways that line up with European Union law and vice versa.
- The second step is an expedited process for governments in the U.S. and E.U. to serve lawful requests for data to authorities in a person's home country,
- Third suggests an exception to such a rule that gives the U.S. or E.U. countries authority over people who physically resides within their boundaries.
- The final component of the proposal is an agreement, "except in the most limited circumstances," that governments on both sides to only seek access to data by going through the companies themselves -- implicitly rejecting policies that rely on surreptitious access like spying on or hacking into companies to access information.[684]

The researchers acknowledge that this type of research may conjure up privacy concerns about online data mining and tracking the activities of users. A future

681 U.S. attorney general criticizes Apple, Google data encryption, http://www.reuters.com/article/2014/09/30/us-usa-smartphones-holder-idUSKCN0HP22P20140930

682 US Attorney Gen latest to roast Apple, Google mobe encryption, http://www.theregister.co.uk/2014/10/01/us_attorney_general_piles_on_phone_encryption_criticism/

683 http://blogs.microsoft.com/on-the-issues/2015/10/20/the-collapse-of-the-us-eu-safe-harbor-solving-the-new-privacy-rubiks-cube/

684 Microsoft's plan to avoid a 'return to the digital dark ages' in wake of Safe Harbor decision, https://www.washingtonpost.com/news/the-switch/wp/2015/10/20/microsofts-plan-to-avoid-a-return-to-the-digital-dark-ages-in-wake-of-safe-harbor-decision/

with our habits being an open book may seem dystopian to those who worry about privacy.[685]

You can run predictions for very huge populations in no time whatsoever, with very little cost. The researchers saw no major barriers to scaling up their algorithms to identify personality traits for billions of users, without too much computational heft. It could even be done in near real time, providing a personality profile in milliseconds.[686]

Research shows that intimate personal attributes can be predicted with high levels of accuracy from 'traces' left by seemingly innocuous digital behaviour, in this case Facebook Likes. The study raises important questions about personalised marketing and online privacy.

Microsoft researchers claim the research would contribute to the on-going discussions about user privacy. Consumers rightly expect strong privacy protection to be built into the products and services they use and this research may well serve as a reminder for consumers to take a careful approach to sharing information online, utilizing privacy controls and never sharing content with unfamiliar parties.[687]

It is not about shutting down access to data. Companies should give users the choice if they don't want to give you the digital footprint. Plus phone and credit card companies already know so much more about you than Facebook does.[688]

Even as websites, wearable computers and, increasingly, every piece of technology we touch gathers and analyzes our data, there's still hope that privacy will survive. Making that case, however, might mean working from a different definition of privacy than we're used to. One cold, hard fact about data privacy is that the data-collection ship sailed long ago, never to return. With limited exceptions, consumers can't really stop tech companies from collecting data about them. When we log into web services, make phone calls, play our favourite apps or buy the latest in connected jewellery, we're giving those companies the right to collect just about whatever information they please about who we are and how we use their products. This why the White House, as part of its new consumer privacy push unveiled on Monday morning, is talking about *how* student data is used and smart grid data is secured rather than what's collected. It's why Federal Trade Commission chairperson Edith Ramirez, speaking about the internet of things at last week's Consumer Electronics

685 New Stanford research finds computers are better judges of personality than friends and family, http://news.stanford.edu/news/2015/january/personality-computer-knows-011215.html

686 Computers may soon know you better than your spouse, http://www.pcworld.idg.com.au/article/563737/computers-may-soon-know-better-than-your-spouse/

687 Digital records could expose intimate details and personality traits of millions, http://www.cam.ac.uk/research/news/digital-records-could-expose-intimate-details-and-personality-traits-of-millions#sthash.KgR9ynWT.dpuf

688 Facebook may know you better than your friends and family, study finds, http://www.washingtonpost.com/news/the-intersect/wp/2015/01/12/facebook-may-know-you-better-than-your-friends-and-family-study-finds/

Show, spoke about how long companies should store user data and not whether they should collect it.[689]

In an increasingly interconnected world, American companies are also leaders in protecting privacy, taking unprecedented steps to invest in cybersecurity and provide customers with precise control over the privacy of their online content.[690]

During the past year, Microsoft has supported academic research on privacy and guides for school officials on the subject. Its executives have also kept a steady presence at public forums urging school districts and policymakers, as well as parents and families, to pay attention to the issue. The company moves aggressively to position itself as a protector of student-data privacy. Microsoft's out-front advocacy would appear to offer an opportunity for the company to take a swipe at some of its rivals, most notably Google.

4.4.3. Impact on legislation

It's important to understand just how much money these companies are throwing around in Washington to buy the policies they want.[691]

In 2014, Google spent a record $16.83 million on lobbying in its efforts to influence federal regulators and lawmakers. In 2019 that number went down to $11.8 million. Facebook, Apple and Amazon also set corporate records for the amount they each spent. The 15 companies spent a total of $116.62 million on lobbying in 2014, a 3 percent decrease from a total of $120.28 million in 2013. Six of the 15 companies increased their 2014 spending, while the rest cut back from 2013 levels. 2019 brought following numbers: Facebook: $16.7 million, Amazon: $16.1 million, Apple: $7.4 million.[692]

Facebook, which has substantially increased its Washington presence over the last years, posted another company record in its effort to influence policymakers. Spending soared 45 percent to $9.34 million from $6.43 million in 2013, to reach $16.7 million in 2019.

Yahoo spent $2.94 million in 2014, an increase of 6 percent from $2.78 million in 2013. Fourth quarter spending was $740,000 vs. $720,000, an increase of 3 percent.[693]

---

689 Data privacy isn't dead with the internet of things, just different, https://gigaom.com/2015/01/12/data-privacy-isnt-dead-with-the-internet-of-things-just-different/

690 http://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families

691 John M. Simpson, Consumer Watchdog's Privacy Project Director

692 Feiner L., Google cut its lobbying spending nearly in half in 2019, while Facebook took the lead, January 22, 2020, https://www.cnbc.com/2020/01/22/how-much-google-facebook-amazon-and-apple-spent-on-lobbying-in-2019.html

693 Google Spends Record $16.83 Million On 2014 Lobbying, Topping 15 Tech And Communications Companies; Facebook, Amazon, Apple Also Post Records, http://insidegoogle.com/

Just hours after Facebook officially went public on the New York Stock Exchange on May 18, 2012, Oregon Gov. John Kitzhaber signed a bill that granted the multibillion-dollar company an enormous tax break on its data center in Prineville, Oregon. Facebook has leaned on tried-and-true techniques: lobbying and campaign contributions. Starting in 2012, the company has given $34,000 in direct corporate contributions to the governor and 24 different Oregon state legislative candidates, according to a review of data collected by the National Institute of Money in State Politics.

Over the past decade, Silicon Valley firms have dramatically increased their lobbying expenses and political contributions. Political action committees run by Google and Facebook now dole out hundreds of thousands of dollars at the federal level every year, and their executives are in demand as fundraisers. But increasingly these contributions are also trickling into cheaper state elections. They tend to arrive just as state governments are considering legislation or regulations that could affect the corporate bottom line.

Tax breaks are not Silicon Valley's only goal when its companies pony up donations. As Yahoo noted, the tech industry has many privacy and security issues – from government responses to data breaches by hackers and the intrusions of the National Security Agency, to the implementation of "Do Not Track" regulations, law enforcement actions against online child pornography and the provision of online account information to the relatives of the deceased. Candidates for state attorney general, in particular, have seen a large increase in tech company campaign cash. Attorneys general, of course, enforce many laws and regulations on privacy and antitrust matters.

Among Silicon Valley tech companies, Facebook leads the way in giving to attorneys general. It has contributed $64,200 to 15 different attorney general campaigns since 2011, more than even Microsoft. In Virginia's 2013 election, the social media giant donated to both Democrat Mark Herring, the ultimate winner, and Republican Mark Obenshain. It has also made contributions of $13,600 to Georgia Attorney General Samuel Olens and $10,000 to Utah Attorney General Sean Reyes since 2011.

As Facebook works to achieve its goal of making the world more open and connected, we believe it is important to develop relationships with elected officials and candidates for public office, at both the state and federal levels, who share our vision.[694]

694 Facebook Is Quietly Making Friends With State Lawmakers Across The Country, http://www.consumerwatchdog.org/story/facebook-quietly-making-friends-state-lawmakers-across-country

5. EFFORTS AGAINST THE ABUSES

5.1. Europe vs Dominant ICT Companies

5.1.1. Max Schrems vs Facebook

Some 25,000 users - led by Austrian law graduate Max Schrems - accused Facebook of violating European privacy laws in the way it collects and forwards data. The case has been brought against Facebook's European HQ in Dublin, which handles accounts outside US and Canada.[695]

The first day of hearings began with a four-hour session in which Facebook's lawyers tried to convince the judge not to admit the suit brought by law student Max Schrems, 27, who is claiming 500 euros ($538) in damages for each user.

Schrems also had a case pending at the European Court of Justice, financed by crowdsourcing, which mainly relates to the so-called Safe Harbor agreement governing data transfers from Europe to the United States. There, the European Data Protection Supervisor told the court that Safe Harbor needed to be changed to safeguard European consumers' rights and that corresponding requests for such changes had been made to the United States.[696]

Basically, Schrems was asking Facebook to stop mass surveillance, to have a proper privacy policy that people can understand, but also to stop collecting data of people that are not even Facebook users.

The case has been brought against Facebook's European headquarters in Dublin, which registers all accounts outside the US and Canada, accounting for approximately 80% of Facebook's 1.35 billion users.[697]

The suit has garnered a huge amount of interest from all over the world. Within days of launching the case last August, Schrems was overwhelmed by the thousands of people from Europe, Asia, Latin American and Australia who wanted to take part. In the end, he limited the number to 25,000 participants, but a further 55,000 have already registered to join the proceedings at a later stage.

695 Austria court considers Facebook privacy case, http://www.bbc.com/news/technology-32229285

696 Austrian student's lawsuit vs Facebook bogged down in procedure, http://www.reuters.com/article/2015/04/09/us-facebook-austria-lawsuit-idUSKBN0N019420150409

697 Class action privacy lawsuit filed against Facebook in Austria, http://www.theguardian.com/technology/2015/apr/09/class-action-privacy-lawsuit-filed-against-facebook-in-austria

The case landed in the European Court of Justice (ECJ) after the Irish authorities refused to open a probe into the alleged violations. The ECJ's decision, which was expected in 2016, could have far-reaching implications for American tech companies operating in Europe.

There are two different things that must be separated. There is the idea of asking for information about a specific person, a Mr X, for example. In the EU as well as the US, that is perfectly okay. The big issue is the forwarding of bulk data belonging to masses of people. We have made complaints about five different companies who are forwarding European data. These are European subsidiaries, of Facebook for example, who hand the data on to a US subsidiary - and they hand it on to the NSA. Under European law, the European subsidiaries are not allowed to hand over the data to foreign countries unless they can guarantee that the data is kept private there. This is something that they can't do, according to the reports that we have heard so far. The main aim for these complaints is that we have European authorities look at whether it is legal or illegal.

The biggest issue here was the total ignorance of European fundamental rights by US companies. But you can't just point the finger at the US companies on this; the EU is also at fault. There are almost no penalties. In Austria, for instance, the maximum penalty is 20,000 euros ($26,000).

With GDPR it has changed, but there was major lobbying from US companies as well as the US government to prevent more serious data protection laws in Europe.

Schrems when describing a problem Facebook imposes gave example of his personal account. What was very frightening for him was his 1,200 pages of data stored by Facebook. There was a lot of information in there that he didn't personally enter onto the computer. A lot of people think that if you don't type in certain things online, it's not going to be there. But, what companies are doing increasingly is getting data about you from your friends. Or they try to aggregate data about your usage that you didn't actively put in. In his Facebook file there were about 300 pages of deleted messages.

It's the companies that are not playing by the rules and are misusing their position, especially Facebook, which basically has a monopoly on social networking. In a democratic society the solution cannot be to not communicate with each other. We should be able to use these cool and empowering technologies without the need for constant worry – that should be the aim.

But it's also the European Union, just watching and writing a few letters and not reacting beyond that. That is the biggest problem we have in Europe – we do have fundamental rights on paper, but we do little to enforce them. If I am a company and the US government is demanding I do something, and I know the Europeans won't react, I know what I would do.

We guarantee our citizens fundamental and constitutional rights, but they are not really working in reality. You have to blame the Europeans the most. It's a question of

democracy as well. Do we have the laws and enforce them, or do we just have them on paper?[698]

Max Schrems, an Austrian law student, had collected eventually roughly 60,000 signatures from people around the world as part of the lawsuit — the largest privacy class-action case brought against Facebook.

Vienna Regional Court rejected the effort by Mr. Schrems, saying that his prominent public role in challenging Facebook's use of personal data meant that he could not pursue the civil litigation. The court also said that it did not have jurisdiction for many of the complainants, as they were not based in Austria.

At least five European regulators — Belgium, France, Germany, the Netherlands and Spain — are investigating whether the social network's revamped privacy policy complies with their national data-protection laws.

The new policy, which came into force worldwide in January, gives Facebook more power to use information in users' posts, messages and other online interactions for the company's main business goal: to sell more advertising. European regulators are examining whether such use of online data offers individuals sufficient control over how information about them is used.[699]

It is directed against Facebook's European subsidiary, registered in Ireland, and that makes it open to all adult Facebook users outside of the United States and Canada. Europe-v-Facebook has already brought about change in the way Facebook deals with users' data by lodging complaints through the Irish Data Protection Commission. As a result, facial recognition has been turned off for all countries outside of the US and the time taken for data deletion has been reduced.

The lawsuit cites Facebook's support of the NSA's Prism surveillance programme and six other points including monitoring and analysis of users through big data systems, and the tracking of Internet users on third-party websites. The aim was to make Facebook finally operate lawfully in the area of data protection. The action was only directed against Facebook's obvious violations of the law and those which affect nearly all users.

Facebook gave one response about sharing the collected data. Their design goal is that the sharing of personal data brings delight and value to the individuals who do it, according to Richard Allan, Facebook's Director of Policy in Europe, in an address to the European Parliament this year. He said that the vast majority of Facebook users have "positive experiences" from the sharing of their personal data.[700]

698 Facebook & Co. ignore fundamental rights, http://www.dw.com/en/facebook-co-ignore-fundamental-rights/a-16927866

699 Facebook Wins a Round in Austrian Court Case, http://bits.blogs.nytimes.com/2015/07/01/facebook-wins-a-round-in-austrian-court-case/?smid=fb-share&_r=0

700 What are the odds for Europe-v-Facebook's latest challenge over personal data?, http://www.dw.com/en/what-are-the-odds-for-europe-v-facebooks-latest-challenge-over-personal-data/a-17847438

5.1.2. Safe Harbor / Privacy Shield

According to EU Justice Commissioner Vera Jourová, there will be major changes in US spying on EU citizens. Details of the replacement to the struck-down Safe Harbor framework, which until this month allowed people's personal information to flow across the Atlantic and into American servers, include new agreement that would move away from the previous self-regulatory approach to one that allows for "pro-active" enforcement and sanctions. There will be an annual review of the new framework, including any access to personal information granted to the FBI and other US agencies on national security grounds. Hopefully, there will be sufficient limitations and safeguards to prevent mass surveillance, with judicial control over the process. That will include judicial oversight (approved by the US House of Representatives and soon to be introduced to the Senate) - would extend judicial protection currently enjoyed by US citizens in the Privacy Act to EU citizens. Once approved, that bill would be another important step in guaranteeing protection for data transfers.

Government officials in Europe and America should use the ruling to their advantage – as a way to create better cooperation between agencies. In particular, there should be greater cooperation between Europe's privacy regulators and the Federal Trade Commission, the American agency primarily in charge of data protection issues. Such collaboration could reduce misunderstandings on each region's stance toward privacy, build trust between global regulators and share the best ways to handle new tech trends like cloud computing.

Some American cloud computing companies have contacted European rivals in efforts to reduce their legal risks when providing online services within the EU. That could involve American tech companies transferring legal responsibility and data of their European users to local cloud computing competitors, which already comply with the region's tough privacy rules. Additionally, at the moment, Microsoft is in a fight with the United States government over attempts to seize a customer's data stored in Ireland, filed a letter to the United States Court of Appeals for the Second Circuit, citing the European privacy ruling as grounds for not sharing the user's information with American authorities. And the company is considering additional data centres in Europe to serve its users in the region, in part as a response to the court's recent privacy ruling, according to two people with knowledge of the matter, who spoke on the condition of anonymity because they were not authorized to speak publicly.[701]

701 As U.S. Tech Companies Scramble, Group Sees Opportunity in Safe Harbor Decision, http://www.nytimes.com/2015/10/21/technology/as-us-tech-companies-scramble-group-sees-opportunity-in-safe-harbor-decision.html?smid=fb-share&_r=0

ECJ RULING

a) The ECJ ruling concerns two important and distinct issues. One of the procedure and one of substance;

b) The procedural issue regards the possibility of national DPA investigating the existence of an adequate level of protection in specific personal data transfers from the EU to the US even when a Decision by the Commission pursuant article 25(6) exists. The Court ruled that such an investigating power exists and if doubts arise regarding the existence of an adequate level of protection the DPA should use judicial remedies to allow for a preliminary ruling that could address the existence of an adequate level of protection and thus the validity of such Decisions;

c) The substantive issue regards the validity of the Safe Harbour Decision. The Court ruled it invalid given that the Safe Harbour policy was a regulated self-regulation mechanism in which there were no normative assurances of substantive protection in case of personal data compromise and no legal remedies offered by American authorities aimed specifically at preventing and redressing such breaches.

d) The ECJ ruling thus set new criteria for the Commission to decide on whether a third country offers an adequate level of protection. The Commission must determine the existence of rules that balance the protection of personal data and strict exceptions concerning other values such as national security or public interest and the Commission must determine the existence of legal remedies - both administrative and judicial - that allow a person to have its transferred personal data examined, corrected or erased.

e) The ECJ ruling thus prevents any transfer of personal data from the EU to the US under the Safe Harbour Decision.

f) The ECJ ruling forces the American companies who would want to transfer personal data from the EU to the US to use other mechanisms under EU persona data law, such as general contract clauses, binding corporate rules or derogations, where applicable. Of these, binding corporate rules seem the most promising.

g) The ECJ ruling sees to take into account the proposed Regulation that is meant to substitute the Directive and thus its jurisprudence seems applicable to the new framework therein introduced. Although Commission powers would, according to ECJ ruling, still have to conform to the set of criteria that the Court derived from the Directive and which are present in the proposed Regulation, other alternatives, such as binding corporate rules will be easier to use given its proximity to US legal tradition and practice.

h) The best solution following the ECJ ruling seems, however, to substitute the Safe Harbour with another EU-US cooperative mechanism, but this will imply a serious change in US behaviour towards data protection mechanisms.

5.1.3. Invalidation of Privacy Shield – *Schrems II*

On 16 July 2020, the Court of Justice of the EU issued its judgment[702] in Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (Schrems II). The case is a companion to the Court's 2015 ruling in Maximillian Schrems v. Data Protection, in which the Court invalidated the Commission adequacy decision underlying the EU-US Safe Harbour arrangement. In Schrems II the Court both affirmed the validity of the standard contractual clauses for data transfers under Commission Decision 2010/87/EU[703] (later amended by Commission Decision 2016/2297[704]), and invalidated Commission Decision 2016/1250[705] that was the legal basis of the EU-US Privacy Shield, which was the successor to the Safe Harbour. Beyond its impact on the SCCs and the Privacy Shield, the Schrems II judgment has important implications for the future regulation of international data transfers.

In his opinion[706], Advocate General (AG) Henrik Saugmandsgaard Øe, gave the Court arguments to avoid having to opine on the validity of the Privacy Shield.[707] However, the Court found that it had no choice but to do so.[708] The Court's invalidation of the Privacy Shield was based on several factors:

1) the primacy of US law enforcement requirements over those of the Privacy Shield[709],
2) a lack of necessary limitations and safeguards on the power of the authorities under US law, particularly in light of proportionality requirements[710],
3) the lack of an effective remedy in the US by EU data subjects[711],
4) deficiencies in the Privacy Shield Ombudsman mechanism.[712]

---

702 *Schrems II*, Case C-311/18, ECLI:EU:C:2020:559

703 COMMISSION DECISION of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, C(2010) 593, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32010D0087&from=en

704 COMMISSION IMPLEMENTING DECISION (EU) 2016/2297, of 16 December 2016, amending Decisions 2001/497/EC and 2010/87/EU on standard contractual clauses for the transfer of personal data to third countries and to processors established in such countries, under Directive 95/46/EC of the European Parliament and of the Council, C(2016) 8471, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016D2297&from=EN

705 COMMISSION IMPLEMENTING DECISION (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, C(2016) 4176, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016D1250&from=EN

706 OPINION OF ADVOCATE GENERAL SAUGMANDSGAARD ØE delivered on 19 December 2019 (1), Case C-311/18, ECLI:EU:C:2019:1145.

707 Ibid. paras. 174-186.

708 *Schrems II*, para. 151.

709 *Schrems II*, para 164.

710 *Schrems II*, paras. 168-185.

711 *Schrems II*, paras. 191-192.

712 *Schrems II*, paras. 193-197.

Considering these deficiencies, the Court found that the Privacy Shield Decision was invalid[713] with immediate effect[714]. The judgement influences more than 5300 companies[715] that used Privacy shield as a data transfer framework. Interestingly, U.S. secretary of commerce, Wilbur Ross said the department would continue to administer the Privacy Shield program, including processing submissions for self-certification and re-certification and to maintain the current list.[716]

The holdings of the Schrems II judgment are not unexpected: strengthening the standard of protection for data transfers and the role of DPAs fits with the Court's strong affirmation of data protection rights in recent years, and the Privacy Shield was already strongly criticized in the past[717]. Therefore, the judgment represents a continuation of the Court's approach to the regulation of international data transfers rather than a radical departure from it.

The Court in its judgement followed the AG in upholding Standard Contractual Clauses (SCCs) use, and also affirmed that the Commission has no obligation to evaluate the level of data protection in countries to which data are transferred under them[718]. The Court states that data controllers transferring data under the SCCs must verify whether the law of the third country of destination ensures adequate protection under EU law[719], and that they are required to verify, prior to any transfer, whether the level of protection required by EU law is respected in the third country concerned[720]. This will require data controllers to become experts in third country and raises questions in particular about data transfers to third countries that are non-democratic or where the rule of law does not apply. The judgment will also put DPAs under pressure to take enforcement actions against companies that rely on the SCCs, even though under the GDPR the DPAs do not approve the SCCs and generally will not even know that they are being used.

The Schrems II case directly concerns Facebook as well as any other dominant ICT company, while having much broader implications for how large-scale data processing of EU citizens data can be done. This is about the bulk outsourcing

713 *Schrems II*, para. 201.

714 *Schrems II*, para. 202.

715 Privacy Shield List, https://www.privacyshield.gov/list

716 Lomas N., Europe's top court strikes down flagship EU-US data transfer mechanism, July 16, 2020, https://techcrunch.com/2020/07/16/europes-top-court-strikes-down-flagship-eu-us-data-transfer-mechanism/?guccounter=1&gucereferrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAACMjgCXv6mtVr5teCNwNexxrmXPhenHwjs9O4GRUtaMnektTY7jDcaY6E5sLgMSZOsjrsJBamXZqib-KdkdPQ6blpuLEptpE7p0Ue3IssxcIEBRrow0rvvdmTcd5fMEjK9Msu1b7QxMU-GU6mrK9IlKAx8yR3dWXjYt1RtRiVjLc

717 EU - U.S. Privacy Shield - Second Annual Joint Review, Adopted on 22 January 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/20190122edpb_2ndprivacyshieldreviewreport_final_en.pdf?, p. 20.

718 *Schrems II*, para. 130.

719 *Schrems II*, para. 134.

720 *Schrems II*, para. 142.

of data processing from the EU to the US, typically undertaken for cost reasons. Therefore, one of the consequences of today's ruling might be that more companies switch to regional data processing for European users. The original case raised specific questions of legality around Standard Contractual Clauses used dominant ICT companies for processing regional users' data in the US. On SCCs, the CJEU has not taken issue with the mechanism itself. Unlike Privacy Shield, SCCs do not contain an assessment on the quality of the protections offered by any third country. They are merely tools which may be available to use if the right legal conditions exist to guarantee EU citizens' data rights. If the level is not equivalent to that offered by EU law, then the controller has a legal obligation to suspend the data transfers. This also means that EU regulators have a clear obligation to act on complaints and suspend data transfers which are taking place via SCCs to third countries where data protections are not adequate.

It's not immediately clear what alternative exists for dominant ICT companies, which fall under US surveillance laws and are using SCCs to take EU citizens' data to the US, given judges have invalidated Privacy Shield on the grounds of the lack of protections afforded to EU citizens data in the country. The CJEU has made it clear in its ruling that even within the SCCs a data flow must be stopped if a US company falls under this surveillance law. This applies to practically all dominant ICT companies.[721]

While the SCCs remain valid, the CJEU underlines the need to ensure that these maintain, in practice, a level of protection that is essentially equivalent to the one guaranteed by the GDPR in light of the EU Charter. The assessment of whether the countries to which data are sent offer adequate protection is primarily the responsibility of the exporter and the importer, when considering whether to enter into SCCs. When performing such prior assessment, the exporter, if necessary, with the assistance of the importer, shall take into consideration the content of the SCCs, the specific circumstances of the transfer, as well as the legal regime applicable in the importer's country. The examination of the latter shall be done in light of the non-exhaustive factors set out under Art 45(2) GDPR.[722]

721 CJEU Judgment - First Statement, Jul 16, 2020, https://noyb.eu/en/cjeu

722 Statement on the Court of Justice of the European Union Judgment in Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, 17 July, 2020, https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_en#:~:text=and%20Maximillian%20Schrems-,Statement%20on%20the%20Court%20of%20Justice%20of%20the%20European%20Union,Facebook%20Ireland%20and%20Maximillian%20Schrems&text=The%20EDPB%20identified%20in%20the,decision%20to%20declare%20it%20invalid.

5.1.4. Right to be Forgotten - Google v. CNIL, C-507/17[723] and Glawischnig-Piesczek, C-18/18[724]

In 2014, the CJEU developed the jurisprudence establishing the European legal right to be forgotten[725] also referred to as the right to de-reference or delist. It allows individuals in the EU to request search engines to remove links containing personal information from web results appearing under searches for their names.[726] In that judgment, the Court also highlighted that the right is not absolute and is granted only when one's personal data protection rights outweigh the public's interest in continued access to the information.[727]

Five years after the development of this legal framework in Google Spain Case, the territorial scope of this right continues to confuse the individuals seeking to enforce it and controllers of processed data receiving requests to de-reference. Notably, national Data Protection Authorities tasked with monitoring the application of the Directive within their territories and national courts have faced serious difficulties in interpretation.[728] The uncertainty of its scope prompted France's Conseil d'État to seek clarifications from the CJEU.

Google Case – Google v. CNIL, C-507/17 - Background

The case concerned a dispute between Google Inc. and CNIL, the French DPA, with regards to the scale on which de-referencing is to be given effect. In 2015, CNIL notified Google that it must apply the removal of links from all versions of its search engine worldwide. It held insufficient both measures implemented by Google to comply with the Directive: 1) de-listing links from all EU and EFTA extensions, and 2) de-listing links from all searches conducted in the French territory.

CNIL argued that internet users located in France are still able to access the other versions outside the EU (e.g. Google.com). Therefore, removing links about an individual residing in France only from the French version (google.fr) or even from versions in the other EU Member States is not enough to protect the individual's right, violating the Directive.

Google refused to comply and continued to limit its de-referencing of links only on search results conducted in the versions of its search engines with domain extensions within the EU and EFTA and used geoblocking, a measure which prevents the links from showing in searches made in France regardless of the version used. Google appealed to the Conseil d'État seeking to annul a 100,000 euro fine imposed by CNIL. The Conseil d'État, noting "several serious difficulties regarding

723 Judgment of 24 September 2019, Google v. CNIL, C-507/17, EU:C:2019:772
724 Judgment of 3 October 2019, Glawischnig-Piesczek, C-18/18, EU:C:2019:821
725 *Google Spain*, C-131/12.
726 *Google Spain*, C-131/12, para. 93.
727 Article 17 of the GDPR.
728 *Google v. CNIL*, C-507/17, para. 39.

the interpretation of the directive,"[729] subsequently referred questions to the Court of Justice for a preliminary ruling concerning the scope of application of Articles 12(b) and 14(a) of the Directive.

The search engine operated by Google is broken down into different domain names by geographical extensions (.fr, .de, .com, etc). Where the search is conducted from 'google.com', Google automatically redirects that search to the domain name corresponding to the State where the search is made. In addition, Google utilizes different factors such as the IP address to determine the location of a user performing a search on Google. The search engine will yield different results depending on the domain name extension and location (e.g. through IP address) of the user.[730]

The Court addressed whether EU data protection law on de-referencing should be interpreted to mean that a search engine operator is required to remove links: 1) on all versions of its search engine (worldwide), or 2) only on the versions corresponding to all Member States (within the EU), or 3) only on the version corresponding to the Member State of residence of the person requesting the de-referencing.[731]

Judgment of 24 September 2019, Google v. CNIL, C-507/17

Importantly, despite the fact that the questions were referred from the point of view of Directive 95/46, the Court also took General Data Protection Regulation 2016/679 into account (by which Directive was replaced in the meantime), in order to ensure that its answers will, in any event, be of use to the referring court. The direction of both judgments generally remains in line with the interpretation proposed in both opinions.[732]

The Court of Justice held that there is no obligation under EU law for Google to apply the European right to be forgotten globally.[733] The decision clarifies that, while EU residents have the legal right to be forgotten, the right only applies within the borders of the bloc's 28 Member States.

The Court referred to the objective of ensuring a high level of protection of personal data in the EU, pursued by both Directive 95/46 and Regulation 2016/679. It further admitted that a de-referencing carried out on all the versions of a search engine would meet that objective in full and argued that the EU legislature enjoys competence to lay down such an obligation.[734] The Court considered that the EU

729 *Google v. CNIL*, C-507/17, para. 39.

730 *Google v. CNIL*, C-507/17, para. 36.

731 *Google v. CNIL*, C-507/17, para. 43.

732 Although the Data Protection Directive was applicable on the date the request for a preliminary ruling was made, it was repealed with effect from 25 May 2018, from which date the GDPR is applicable. Therefore, the Court examined the questions in light of both the Directive and the GDPR to ensure that the decision will be of use to the refering court.

733 *Google v. CNIL*, C-507/17, para. 64.

734 *Google v. CNIL*, C-507/17, para. 58.

lawmakers have not done so, thus far. In consequence, for the time being, EU data protection law does not require search engine operators to carry out a de-referencing on all world-wide versions of a search engine. However, the Court also did not exclude a possibility for a supervisory or judicial authority of a Member State to weigh up, in the light of national standards of protection of fundamental rights, a data subject's right to privacy and the protection of personal data concerning him or her, on the one hand, and the right to freedom of information, on the other, and, where appropriate, to order such de-referencing.[735]

The Court began by observing that, in principle, de-referencing is to be carried out in respect of all Member States[736] and, if necessary, the search engine operator should be obliged to take sufficiently effective measures to ensure the effective protection of the data subject's fundamental rights. Measures of this kind should have the effect of preventing or, at the very least, seriously discouraging internet users in the Member States from gaining access to the links in question while searching on the basis of that data subject's name.[737]

The Court left the question open whether automatic redirecting to a different national version of the search engine's website constitutes such a measure. It would seem that such blocking or redirection would then fall under the exception to customers' right of access to online interfaces, set out in Article 3(3) of Regulation 2018/302 on geo-blocking[738].

The Court accepted that the interest of the public in accessing information may, even within the Union, vary from one Member State to another, meaning that results of the balancing exercise are not necessarily the same for all the Member States. The Court thus emphasized the role of cooperation between supervisory authorities in the Member States as an adequate framework for reconciling the conflicting rights and freedoms. It is through this framework, therefore, that a de-referencing decision, covering all searches conducted from the territory of the Union on the basis of a data subject's name, should be adopted.[739]

Facebook Case - Glawischnig-Piesczek, C-18/18 - Background

The whole case centres around Eva Glawischnig-Piesczek, a chairperson for the Greens party in Austria. A private citizen in Austria shared an article on Facebook about Glawischnig-Piesczek and called her a "lousy traitor of the people" and a member

735 *Google v. CNIL*, C-507/17, para. 72.

736 *Google v. CNIL*, C-507/17, para. 66.

737 *Google v. CNIL*, C-507/17, para. 70.

738 Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC, OJ L 60I.

739 *Google v. CNIL*, C-507/17, para. 69.

of a "fascist party," among other names. The article appeared on the Austrian news website oe24.at and was titled, "Greens: Minimum income for refugees should stay."

The decision stems from a reference for a preliminary ruling made by the 'Oberster Gerichtshof' (Austrian Supreme Court), in a case considering an appeal by both Eva Glawischnig-Piesczek - a member of the 'Nationalrat' (House of Representatives of the Parliament, Austria), chair of the parliamentary party 'die Grünen' (The Greens) and federal spokesperson for that party - and Facebook Ireland, challenging a decision by the lower court, 'Oberlandesgericht Wien' (Higher Regional Court, Vienna). In that case, Glawischnig-Piesczek sued Facebook before the Austrian courts, requesting that Facebook Ireland be ordered to remove a comment deemed harmful to her reputation, published by a user on that social network, and any identical or equivalent content.

The Austrian Supreme Court asked the CJEU for clarification concerning the interpretation of Article 15(1) of the so-called e-Commerce Directive, which provides as follows: Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

In particular, the Austrian Supreme Court asked whether Article 15(1) of the e-Commerce Directive should be interpreted as precluding a court of a Member State from being able to: 1) order a hosting provider to remove or disable access to information, which it has stored and the content of which is identical to that of information which has previously been declared illegal, irrespective of who requested the storage of that information; and 2) order a hosting provider to remove or disable access to information, which it has stored and the content of which is equivalent to that of information which has previously been declared illegal; and 3) extend the effects of such an injunction worldwide.[740]

Judgment of 3 October 2019, Glawischnig-Piesczek, C-18/18

The Court started its analysis by making clear that the immunity from suit granted by Article 14 of the e-Commerce Directive is not a general immunity from every legal obligation. Specifically, the national authorities remain competent to require a host to terminate access to or remove illegal information. The Court also noted that Article 18 of the e-Commerce Directive requires Member States to have in place appropriate court actions to deal with illegal content. The Court held that no limitation on the scope of such national measures can be inferred from the text of the e-Commerce Directive.[741]

740 Court of Justice of the European Union, PRESS RELEASE No 128/19, Luxembourg, 3 October 2019.

741 *Glawischnig-Piesczek*, C-18/18, para. 30.

According to the Court, Member States enjoy broad discretion in relation to actions and procedures for taking necessary measures.[742] Such a margin of discretion is due to, among others, the rapidity and geographical extent of the damage arising in connection with information society services. Both of these factors were also clearly at play in the present case.[743]

The Court decided to distinguish between injunctions concerning information whose content is identical to the one which was previously deemed illegal and injunctions concerning information with equivalent content - whose message remains essentially unchanged and therefore diverges very little from the content which gave rise to the finding of illegality.[744] When it comes to information with equivalent content the Court sought a balanced solution. It considered that injunctions should generally be able to extend to information, the content of which, whilst essentially conveying the same message, is worded slightly differently, because of the words used or their combination, compared with the information whose content was declared to be illegal.[745]

CJEU highlighted the fact that while Article 15 of the e-Commerce Directive prohibited general monitoring as recital 47 in the preamble of the Directive makes clear, monitoring 'in a specific case' does not fall within that prohibition. It then held that such a specific case may, in particular, be found, as in the main proceedings, in a particular piece of information stored by the hosting provider concerned at the request of a certain user of its social network.[746]

The Court determined an equivalent meaning to be about the message the information posted conveys and which was essentially unchanged. Given the focus on meaning not form, the Court held that an injunction could extend to non-identical posts as otherwise the effects of an injunction could easily be circumvented. The Court then considered the balance between the competing interests and commented that the equivalent information identified by court order should contain specific elements to identify the offending content and in particular must not require the host to carry out its own independent assessment. In terms of assessing the burden on the host, the court noted that the host would have recourse to automated search tools and technologies.[747]

As regards territorial scope, the Court once again confirmed the broad reading of Article 18(1), e-Commerce Directive, which did not make provision for any limitation, including a territorial limitation, on the scope of the measures which Member States are entitled to adopt.[748] The Court also noted that Article 18 of

742 *Glawischnig-Piesczek*, C-18/18, para. 29.
743 *Glawischnig-Piesczek*, C-18/18, para. 36.
744 *Glawischnig-Piesczek*, C-18/18, para. 39.
745 *Glawischnig-Piesczek*, C-18/18, para. 41.
746 *Glawischnig-Piesczek*, C-18/18, para. 35.
747 *Glawischnig-Piesczek*, C-18/18, para. 46.
748 *Glawischnig-Piesczek*, C-18/18, para. 49.

the e-Commerce Directive makes no provision for territorial limitations on what measures Member States may make available. In principle, world-wide effects would be permissible[749], but this is subject to the proviso that EU rules must be consistent with the international law framework - Member State courts may order platforms to take down illegal content and ensure that identical and equivalent content is also taken down. The effect of such orders may extend globally, subject to compliance with relevant international law, which is for the Member State courts to assess.

Comparing Case C-507/17 with Case C-18/18

Both Google v. CNIL and the Facebook Ireland cases tackle the same legal question, namely the territorial effect of removal of information. However, the legal frameworks of these cases were presented differently.

In both cases, the CJEU begins its reasoning by reading into the e-Commerce Directive and the GDPR, respectively, the wish of the EU legislature to strike a balance between the interests at stake.[750] In the Facebook case, the interest of the person seeking to have defamatory content taken down is balanced against the difficulty of the hosting provider to comply with a measure in respect of the e-Commerce Directive. In the Google case, the interest of the person seeking to take down content infringing his data protection rights is balanced against the right to freedom of information which evidently is adversely affected by a de-referencing order in respect of the GDPR.

In the Google case the CJEU reasons that while EU legislature has struck a balance between the right to privacy and the right to freedom of information[751] as regards the application of the right to be forgotten within the EU, it has not struck such a balance as regards application outside the EU territory.[752] This is because the rights arise from the EU Charter of Fundamental Rights.

The CJEU holds that nowhere does the GDPR indicates that any of its provision should apply outside of the territory of the EU, therefore, it is only required to be given effect to within the territory of the EU.[753] However, the CJEU argues that neither does the GDPR expressly prohibit its application worldwide.[754] While the fact that EU law does not require extraterritoriality, the GDPR's silence on the point gives space to a national court to make an order with extra-territorial effect. In Google v. CNIL, while the Court recognised the possibility for national courts to make orders for de-referencing with extra-territorial effect, it expressly noted that in doing so they must weigh up the competing interests of the data subjects and the right of others to

749 *Glawischnig-Piesczek*, C-18/18, para. 50.
750 *Google v. CNIL*, C-507/17, para. 60, *Glawischnig-Piesczek*, C-18/18, para. 43.
751 See Article 17(3)(a) of the GDPR.
752 *Google v. CNIL*, C-507/17, para. 61.
753 *Google v. CNIL*, C-507/17, para. 62 and 63.
754 *Google v. CNIL*, C-507/17, para. 72.

freedom of information.[755] It is noticeable that in Glawischnig-Piesczek the balancing is different. The Court notes the interest of the subject of the information and also the need not to impose an excessive burden on the hosting provider.[756] The existence of other rights: the right of the host to carry on a business and the rights of those posting the material and those wishing to receive it – both aspects of freedom of expression - are not expressly mentioned. To some extent, the issue of rights will be covered through the national courts, which will be the bodies to carry out that balancing within their own national frameworks and within the limits of EU law. By contrast to Google v CNIL, however, there is no instruction from the Court that these are matters to be considered, nor any express recognition that the balance between the right to private life, including the protection of reputation and freedom of expression differs between territories. What might be seen as the legitimate protection of private life in one place is an infringement of speech in another.

In the Facebook case the CJEU simply states the balance of the individual's and the host provider's interests must mean that the hosting provider cannot be burdened with an excessive obligation, that is, a hosting provider cannot be obliged to generally monitor for illegal activity.[757] In fact, the Member States are expressly prohibited from imposing such a general obligation by Article 15 of the E-Commerce Directive; therefore, a balance struck in this sense is purely made in terms of EU legislation and, by implication, cannot be applied to measure which have an effect worldwide.

The CJEU posits that nowhere does the e-Commerce Directive make any territorial limitation to the application of the measures permitted under Article 18, therefore, those measures may be given worldwide effect.[758] Nevertheless, in the case that a Member State applies a measure with the worldwide effect, it must do so in a manner consistent with the framework of the relevant international law.[759]

The effect of the two cases is the convergence of the territorial scope of the GDPR and the e-Commerce Directive. That is, they can apply within the EU territory but also with global effect provided that a balance must then be struck between the interests at stake, in the case of the GDPR, in terms of national standards of protection of fundamental rights, and, in the case of the e-Commerce Directive, in terms of international law.

Conclusion

Google v CNIL is a long-awaited clarification of, at the very least, the geographical boundaries of the right to be forgotten. As the Court held, there is little room for

755 *Google v. CNIL*, C-507/17, para. 72.
756 *Glawischnig-Piesczek*, C-18/18, para. 45 and 46.
757 *Glawischnig-Piesczek*, C-18/18, para. 43.
758 *Glawischnig-Piesczek*, C-18/18, para. 49 and 50.
759 *Glawischnig-Piesczek*, C-18/18, para. 51.

interpretation under the current legal framework of data protection to establish a global application of such a right. It highlighted the difficulties of global de-referencing noting that public interest in access to information substantially vary among third States, therefore, the balancing of fundamental rights would also differ. The Court went on to say that the EU framework does not provide for cooperation instruments and measures outside its territory and chose the EU-wide approach. The decision is critical because, at first glance, it appears to have closed the door for EU residents to demand a worldwide removal of their information, in certain circumstances, from search engine results under the GDPR. The Court explicitly set limits on the territorial scope of an individual's right to de-reference. In simple terms, this means that Google is only required to remove links to personal data from internet searches conducted within the EU.

On the other hand, just because the law stands as it currently does, it does not mean that it is adequate. By explicitly limiting the territorial scope of the right to be forgotten, the Court may seem to have inadvertently limited the impact and protective effect of this right. Given the importance of a global application of the right, allowing internet users conducting searches outside the EU to still be able to access the links de-referenced in the EU after this judgment will potentially undermine the right to be forgotten and weaken the protection sought to be achieved by the right or, at the minimum, the Union's objective of guaranteeing a high level of protection of personal data cannot be fully met. The CJEU's decision provided clarity on the scope of the right under EU law, it also left areas of uncertainty. For example, since the Court left the option open for DPAs to determine the conditions which will justify a delisting on all versions of a search engine based on national standards of the protection of fundamental rights, it is expected that the CJEU will continue to see more questions about the global reach of the EU's data protection.

In light of all of this, it is a missed chance to develop individual rights in the digital age further, promoting human dignity in the digital age. I believe that the Court has failed to recognize its own mission and mandate.

There are also some other immediate issues to mention. In both cases, the Court emphasises the need to act "within the framework of the relevant international law". The problem is the lack of consistent and sufficient international law in these matters. In general, the CJEU's approach is very much aligned with the US, Supreme Court of the United States in particular, judicial approach in similar extraterritoriality issues, such as sanctions law or export controls.[760] However, as prof. Svatesson points

760 Van Calster G., Steady now. Eva Glawischnig-Piesczek v Facebook. The CJEU on jurisdiction and removal of hate speech, Conflict of Laws /Private international law, EU law - General, October 10, 2019, https://gavclaw.com/tag/c-13617/.

out,[761] the Austrian court may now force Facebook to prevent future publications, that may originate in the US and be lawful there, with worldwide effect. Now re-read that sentence replacing „Austrian" with „Chinese", and „US" with „EU". I can only imagine that the Court's ruling is likely to infuriate US lawyers worried about its impact on freedom of speech.

The court recognizes the concern about general monitoring but says that is addressed if there is sufficient clarity as to what kinds of equivalent content would qualify. According to the court, if there is sufficient clarity, then companies like Facebook would be freed from having to make the kind of independent assessment that would raise concern. They could simply carry out the takedown requirements with automated search tools and technologies. However, it's not entirely clear how companies are supposed to determine what is identical unless the criteria for this is limited to shares of the precise post with the precise picture and precise words.[762] The court is presuming a level of technological sophistication and degree of specificity that simply do not, and likely never will exist. Even applying this to identical posts is challenging.

The judgment of the Court in the Facebook case has some implications. It strengthens the protection of parties affected by illegal content but seeks to achieve this without undermining the validity of e-Commerce Directive Article 15. As such, it does not provide a straightforward solution to each and every future case and sets quite demanding requirements for both national courts and host providers. The judgment is clearly relevant beyond the social media context but can also be applied to other platforms like online marketplaces. Operators of such platforms could be required to take steps to monitor their content e.g. as regards the recurring presence of misleading information.

Of course, one cannot help noticing the similarity between the question of territorial scope addressed Google and Facebook cases.

In Glawischnig-Piesczek, the Court did not provide for an equally balanced framework but limited itself to stating that injunctions with worldwide effects are not precluded by e-Commerce Directive. This remains in line with the opinion of Advocate General Szpunar[763] - the same AG whose advice was followed in the Google case. Both findings are, not necessarily inconsistent. In fact, the opinion in Glawischnig-Piesczek explicitly refers to the Google case. According to the AG, like

761 Svatesson D., Bad news for the Internet as Europe's top court opens the door for global content blocking orders, October 3, 2019, https://www.linkedin.com/pulse/bad-news-internet-europes-top-court-opens-door-global-svantesson/

762 Daskal J., A European Court Decision May Usher In Global Censorship, 3 October, 2019, https://slate.com/technology/2019/10/european-court-justice-glawischnig-piesczek-facebook-censorship.html

763 OPINION OF ADVOCATE GENERAL SZPUNAR delivered on 4 June 2019, *Glawischnig-Piesczek*, C-18/18, EU:C:2019:458.

with the right to be forgotten, „the legitimate public interest in having access to information will necessarily vary, depending on its geographic location, from one-third State to another".[764] Consequently, the limitation of extraterritorial effects of injunctions concerning harm to private life and personality rights, for example by way of geo-blocking, may remain „in the interest of international comity".[765]

It is important for the CJEU to provide clarity on the territorial extent of removal requests and to ensure the effective protection of personal data at the same time. It would not be preferable for the Court to create a general rule because such a rule does not fit in the system of the balancing test. A general rule to remove information on a worldwide level would, in some cases, disproportionally harm the freedom of access to information of people outside the EU. On the other hand, a general rule that information only has to be removed within the EU, hence geographical restricted, will not protect the privacy of data subjects in certain cases. I believe that a national judge should have the freedom to decide on a case level whether specific information can be removed globally or locally.

To partially answer my initial question about the general differences in the two Court's judgment I would like to say that, yes to a certain point the characteristics of both companies, Facebook and Google, matter. And therefore the Court used different balancing. The question is, can national courts use both balancing test in one case in the future? One thing I find quite certain. In both cases, the Court rules that EU law - privacy law in the case of Google v. CNIL, platform liability law in the case of Glawischnig-Piesczek - does not prevent national courts in EU member states from ordering the de-listing or the takedown of content globally. However, while the Google case left open the legal basis for such rulings, inviting further litigation on that matter under national law, the Facebook case is quite clear about deferring.

5.1.5. Germany's Federal Cartel Office vs Facebook

Germany's Federal Cartel Office ordered a crackdown on Facebook's data collection practices after ruling the world's largest social network abused its market dominance to gather information about users without their knowledge or consent.

The aim is to to not allow Facebook in the future to force its users to agree to the practically unrestricted collection and assigning of non-Facebook data to their Facebook accounts. The cartel office objected in particular to how Facebook acquires data on people from third-party apps - including its own WhatsApp and Instagram services - and its online tracking of people who aren't even members. That includes tracking visitors to websites with an embedded Facebook 'like' or share button - and pages where it observes people even though there is no obvious sign the social network is present.

764 OPINION OF ADVOCATE GENERAL SZPUNAR, para. 99.
765 OPINION OF ADVOCATE GENERAL SZPUNAR, para. 100.

The ruling does not yet have legal force and Facebook has a month to appeal, which the social network said it would do. At this point Cartel Office requires that collecting data from third-party websites and assigning them to Facebook would only be allowed if users give their voluntary consent. If consent is withheld, Facebook would have to substantially restrict its collection and combining of data, and should develop proposals for solutions to do this within 12 months.[766]

5.1.6. Schengen routing system

Among other solutions, Germany and France are considering a so-called Schengen routing system in which as much online data would be kept in Europe as possible. But there is a question if it would really limit surveillance or just be profitable for EU companies.[767]

Schengen Routing refers to the practice of routing Internet traffic between hosts located in the Schengen Area, not leaving the borders of countries part of the Schengen Treaty. Such Internet traffic not leaving the Schengen Area is more difficult to be wiretapped by non-Schengen intelligence agencies, since the Internet traffic remains still unencrypted. However, this traffic remains still vulnerable to wiretapping activities that may occur within Schengen.[768]

Deutsche Telekom, one of Europe's largest telecommunications companies, raised the idea of creating a European data network. It might function roughly in accord with the Schengen Agreement, which allow for the free movement of people and goods across participating EU members states. However, the Schengen zone does not include all EU countries. If a Schengen routing system were developed, it would offer an elegant way to bypass Great Britain, which is not part of the Schengen area and whose signals intelligence service, known as GCHQ, has also been revealed to be mining data from the EU.[769]

Can national borders even be combined with the idea of the internet as a worldwide network? There are some doubts[770] that is possible – after all, the internet was not built up by states but has had a global structure right from the start. The Internet companies' massive servers are generally located abroad, and the Internet

766 Busvine D., Facebook's data gathering hit by German anti-trust clampdown, February 2019, https://www.reuters.com/article/us-google-lawsuit-illinois/u-s-judge-dismisses-suit-versus-google-over-facial-recognition-software-idUSKCN1OT001

767 Seiffert J., Weighing a Schengen zone for Europe's Internet data, February 2014, https://www.dw.com/en/weighing-a-schengen-zone-for-europes-internet-data/a-17443482

768 Pohlmann N., Sparenberg M., Siromaschenko I., Kilden K., Secure Communications and Digital Sovereignty in Europe, ISSE 2014 Securing Electronic Business Processes, Brussels, Belgium, 2014, p. 155–169

769 Schaefer L., Deutsche Telekom: 'Internet data made in Germany should stay in Germany', September 2013, https://www.dw.com/en/deutsche-telekom-internet-data-made-in-germany-should-stay-in-germany/a-17165891

770 https://www.internet-sicherheit.de/?L=2

service providers send data packets across various countries. While it is possible for data traffic within Europe to be also be restricted solely to European channels, such traffic makes up just a small part of what Europeans do online. For example, while surfing on Facebook, shopping on Amazon or using other big portals, the data is leaving the German and European zone anyway.

Jan Philipp Albrecht, a German member of the European Parliament for the Green party, agreed, that a Schengen-style system should not be the focus. - instead, it is needed to have a legal framework which secures fundamental rights in the European market, explaining this would provide leverage in dealing with online companies located outside of the EU.

Europe's Internet traffic is still far from being encrypted in a standardized way. Most people who want to send their e-mail securely have to take matters into their own hands and use a software package to assist with encryption and decryption to read the messages when they arrive.[771]

Problem is that according to some research[772] Schengen Routing compliance is not achieved in any of the Schengen countries, contradicting the claim that Schengen routing already was a factual reality today, as it has been stated by the Association of the German Internet Industry. Therefore, intelligence agencies still can perform potential wiretapping activities outside the Schengen jurisdiction on traffic originating within and destined to the Schengen Area.

5.2. US vs Dominant ICT Companies

The social networking service Facebook has agreed to settle Federal Trade Commission charges that it deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public.[773] Facebook was obligated to keep the promises about privacy that it makes to its hundreds of millions of users. FTC claimed that Facebook's innovation does not have to come at the expense of consumer privacy. However, in 2011 FTC released a list with a number of instances in which Facebook allegedly made promises that it did not keep:[774]

771 Seiffert J., Weighing a Schengen zone for Europe's Internet data, February 2014, https://www.dw.com/en/weighing-a-schengen-zone-for-europes-internet-data/a-17443482

772 Donni D., Machado G., Tsiaras Ch., Stiller B., Schengen Routing: A Compliance Analysis, https://files.ifi.uzh.ch/CSG/staff/doenni/extern/publications/Schengen_Routing_A_Compliance_Analysis_AIMS_2015.pdf

773 UNITED STATES OF AMERICA FEDERAL TRADE COMMISSION, FILE NO 092 3184, https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf

774 UNITED STATES OF AMERICA FEDERAL TRADE COMMISSION, DOCKET NO. C-0923184, https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf

- In December 2009, Facebook changed its website so certain information that users may have designated as private – such as their Friends List – was made public. They didn't warn users that this change was coming, or get their approval in advance.
- Facebook represented that third-party apps that users' installed would have access only to user information that they needed to operate. In fact, the apps could access nearly all of users' personal data – data the apps didn't need.
- Facebook told users they could restrict sharing of data to limited audiences – for example with "Friends Only." In fact, selecting "Friends Only" did not prevent their information from being shared with third-party applications their friends used.
- Facebook had a "Verified Apps" program & claimed it certified the security of participating apps. It didn't.
- Facebook promised users that it would not share their personal information with advertisers. It did.
- Facebook claimed that when users deactivated or deleted their accounts, their photos and videos would be inaccessible. But Facebook allowed access to the content, even after users had deactivated or deleted their accounts.
- Facebook claimed that it complied with the U.S.- EU Safe Harbor Framework that governs data transfer between the U.S. and the European Union. It didn't.

The proposed settlement bars Facebook from making any further deceptive privacy claims, requires that the company get consumers' approval before it changes the way it shares their data, and requires that it obtain periodic assessments of its privacy practices by independent, third-party auditors for the next 20 years.

The proposed settlement bars Facebook from making any further deceptive privacy claims, requires that the company get consumers' approval before it changes the way it shares their data, and requires that it obtain periodic assessments of its privacy practices by independent, third-party auditors for the next 20 years. Specifically, under the proposed settlement, Facebook is:

- barred from making misrepresentations about the privacy or security of consumers' personal information;
- required to obtain consumers' affirmative express consent before enacting changes that override their privacy preferences;
- required to prevent anyone from accessing a user's material more than 30 days after the user has deleted his or her account;
- required to establish and maintain a comprehensive privacy program designed to address privacy risks associated with the development and management of new and existing products and services, and to protect the privacy and confidentiality of consumers' information; and
- required, within 180 days, and every two years after that for the next 20 years, to obtain independent, third-party audits certifying that it has a privacy

program in place that meets or exceeds the requirements of the FTC order, and to ensure that the privacy of consumers' information is protected.[775]

If the FTC finds that Facebook failed to comply with the consent decree it agreed to in 2011, it could be liable for trillions of dollars in fines. Violations of the agreement could carry a financial penalty of $40,000 per violation, meaning that if the social network mishandled 50 million Americans' data, it could face fines up to $2 trillion. It's not clear though that the FTC would necessarily seek the maximum penalty.[776]

The FTC has strongly advocated for commercial practices that facilitate individual control of personal information. In 2010, the FTC released a preliminary report on privacy that proposed a policy framework relying heavily on improved transparency, consumer education, and simplified settings and choices for data sharing. These principles were also at the heart of the agency's enforcement actions against Google and Facebook. The final version of this report, released in late 2012,[777] adopted a modified approach that placed greater emphasis on the context of the data transaction, implementing privacy by design and the need for further enforcement and accountability for commercial practices.

Another effort straight from the US is Freedom from Facebook.[778] The organization's demand is that the Federal Trade Commission (FTC) should break up Facebook, splitting off subsidiaries such as Instagram, WhatsApp and Messenger in order to boost competition in the social networking sector. The organization also want stronger privacy protections and the "freedom to communicate across networks."

FACEBOOK 5 billion fine

Facebook Inc. has been paying hundreds of outside contractors to transcribe clips of audio from users of its services. The Irish Data Protection Commission, which takes the lead in overseeing Facebook in Europe, said it was examining the activity for possible violations of the EU's strict privacy rules.[779]

---

775 Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises, November 2011, https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep

776 Matsakis L., THE FTC IS OFFICIALLY INVESTIGATING FACEBOOK'S DATA PRACTICES, March 2018, https://www.wired.com/story/ftc-facebook-data-privacy-investigation/

777 Federal Trade Commission. "Protecting Consumers in an Era of Rapid Change." March 2012. www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumerprivacy-era-rapid-change-recommendations/120326privacyreport.pdf

778 https://freedomfromfb.com/

779 Bodoni S., Facebook Quizzed by Watchdog for Listening to Users' Chats, https://www.bloomberg.com/news/articles/2019-08-14/facebook-quizzed-by-privacy-watchdog-for-listening-to-user-audio, August 14, 2019

Amazon.com Inc., Google, Apple and now Facebook have come under fire for collecting audio snippets from consumer computing devices and subjecting those clips to human review, a practice that critics say invades privacy. It is not just the Irish regulator, where Google, Apple and Facebook have their main EU base, which has started digging deeper into possible privacy violations. Officials in the U.S. and elsewhere in Europe are also probing processing by human reviewers employed to listen to voice commands recorded by digital assistants.

Facebook confirmed that it had been transcribing users' audio and said it will no longer do so, following scrutiny into other companies. Much like Apple and Google, they paused the human review of audio. Big tech companies including Amazon.com Inc. and Apple Inc. have come under fire for collecting audio snippets from consumer computing devices and subjecting those clips to human review, a practice that critics say invades privacy. It first reported in April 2019that Amazon had a team of thousands of workers around the world listening to Alexa audio requests with the goal of improving the software, and that similar human review was used for Apple's Siri and Alphabet Inc.'s Google Assistant. Apple and Google have since said they no longer engage in the practice and Amazon said it will let users opt-out of human review.

The $5 billion penalty against Facebook is the largest ever imposed on any company for violating consumers' privacy and almost 20 times greater than the largest privacy or data security penalty ever imposed worldwide. It is one of the largest penalties ever assessed by the U.S. government for any violation.[780]

Facebook has long denied that it collects audio from users to inform ads or help determine what people see in their news feeds. CEO Mark Zuckerberg denied the idea directly in Congressional testimony. The Facebook data-use policy, revised in 2018 to make it more understandable for the public, includes no mention of audio. It does, however, say Facebook will collect "content, communications and other information you provide" when users "message or communicate with others." Facebook says its "systems automatically process content and communications you and others provide to analyze context and what's in them." It includes no mention of other human beings screening the content. In a list of "types of third parties, we share information with," Facebook doesn't mention a transcription team, but vaguely refers to "vendors and service providers who support our business" by "analyzing how our products are used."[781]

780 Nuñez M., FTC Slaps Facebook With $5 Billion Fine, Forces New Privacy Controls, Jul 24, 2019, https://www.forbes.com/sites/mnunez/2019/07/24/ftcs-unprecedented-slap-fines-facebook-5-billion-forces-new-privacy-controls/#3e7bb16a5668

781 Frier S., Facebook Paid Contractors to Transcribe Users' Audio Chats, https://www.bloomberg.com/news/articles/2019-08-13/facebook-paid-hundreds-of-contractors-to-transcribe-users-audio, August 13, 2019

Additionally, FTC has added new restrictions to the way the tech giant handles user data in hopes it will change Facebook's entire privacy culture. The 20-year agreement orders Facebook to restructure the way it handles user privacy—including changes at the board level and in the way the company will handle relationships with third-party developers. The settlement also establishes new guidelines for how the company will be held accountable for future privacy violations. The settlement includes several provisions that limit the power of Mark Zuckerberg's decision-making. It mandates Facebook create an independent privacy committee on its board of directors whose members can only be fired by two-thirds voting shares—effectively preventing Zuckerberg from controlling the vote. Facebook will also be required to submit reports to the FTC on a quarterly and annual basis, certifying that the company is complying with the agreement. [782]

Around the same time, Securities and Exchange Commission announced[783] fining Facebook for $100 million as part of a settlement tied to a probe into the social network's handling of users' data. The investor protection agency alleged that Facebook's public disclosures didn't offer sufficient warning that developers and other third parties may, in obtaining user data, have violated the social network's policies or failed to gain user permission.[784]

5.3. Other efforts

Protection of personal information will likely only be possible through the application of a variety of techniques. Consumer groups, privacy advocates and data protection commissioners can provide information on how organizations should collect, use and disclose personal information in accordance with fair information practices. We can also educate the public on the existence of different privacy-enhancing technologies, as well as monitoring their development.[785]

Online companies typically make money by utilizing data gleaned from their users to sell targeted ads. If the flow of user data slows down, so does the money. A study commissioned by the Interactive Advertising Bureau with researchers from Harvard Business School underscores the point: at least half of the Internet's economic

782 Case No. 19-cv-2184, United States of America v. FACEBOOK, Inc., https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf

783 Securities and Exchange Commission , Press Release - Facebook to Pay $100 Million for Misleading Investors About the Risks It Faced From Misuse of User Data, Jul 24, 2019, https://www.sec.gov/news/press-release/2019-140

784 Sherr I., 2019, Facebook lost control of our data. Now it's paying a record $5 billion fine, Jul 24, https://www.cnet.com/news/facebook-lost-control-of-our-data-now-its-paying-a-record-5-bill

785 Cavoukian A., Privacy as a Fundamental Human Right vs. an Economic Right: An Attempt at Conciliation, September 1999, http://www.ontla.on.ca/library/repository/mon/10000/211714.pdf, p. 29.

value is based on the collection of individual user data, and nearly all commercial content on the Internet relies on advertising to some extent. Digital advertising grew to almost $200 billion in 2019, a sum that already exceeds spending on broadcast television advertising. Essentially, the collection of user data makes possible the free access to maps, email, games, music, social networks and other services. It's the way we pay for supposedly free access.[786]

Digital privacy advocates, understandably, view the online ecosystem differently. They are alarmed by the growth of the surveillance economy, in which companies compile and store information about what a user reads, looks for, clicks on or buys. In this world, the disclosure is meaningless, because almost no one reads the terms of service that define the relationship between the customer and the company.

The industry recommendation is expected to distinguish between companies that have a "first party" relationship with users — consumer-facing Internet content providers and Internet service providers — and "third party" companies, which include most small advertising-technology companies. First-party relationships would be created if the user "intends to interact" with the web company (or a service provider acting on behalf of that company). For example, logging into Facebook would count as a "user action" that would allow Facebook to track your activity "across multiple distinct contexts," including other websites. Third-party relationships would have far more limited tracking abilities. For example, if a user visits a site that integrates an advertisement with content from other sources, the ad server would not be able to place a tracking "cookie" for marketing purposes on your device without your consent. This dubious distinction would harm competition in the online ad market by turning "Do Not Track" into "Do Not Track for small ad companies only." If the industry group recommends a lopsided version of "Do Not Track," as expected, the commission should not go along with it. The correct balance between privacy and competition is a decision better left to Congress than to a feckless regulator.[787]

Instead of following the approach that led to the end of unwanted telemarketing, the commission adopted a strategy that favours big companies and Washington lobbyists over Internet users and online privacy: vague goals, endless meetings, more warnings for users and no real impact on business practices. The outcome, as Mr. Campbell puts it, "could be worse than doing nothing at all."

This is not simply historical commentary. The United States today faces the highest levels of identity theft and data breaches in the world. Most user passwords

786 Enberg J., Global Digital Ad Spending 2019. Digital Accounts for Half of Total Media Ad Spending Worldwide. March 28, 2019, https://www.emarketer.com/content/global-digital-ad-spending-2019

787 The Slow Death of 'Do Not Track', http://www.nytimes.com/2014/12/27/opinion/the-slow-death-of-do-not-track.html?module=Search&mabReward=relbias&

have been compromised. And the risks to "digital natives" will only increase as more data that cannot be protected is gathered.[788]

The controversy centres around a cookie - a simple text file which can track a number of user activities - which Facebook has used for the last five years. Even non-members who visited any net page that fell under the facebook.com domain would have what Facebook calls its datr cookie - which has a two-year lifespan - installed on their browser.

Facebook head of security Alex Stamos said[789] the cookie can help in a number of ways such as:

- preventing the creation of fake accounts
- reducing the risk of users' accounts being taken over by other people
- protecting users' content against theft
- preventing distributed denial of service attacks

It also pointed out that the cookie was associated only with browsers, not individual people, and does not contain any information that is tied to a particular person. – so no Personal Data gathering, unlike court decided and commissioner decided.

One of the report authors, Brendan Van Alsenoy said his team of researchers did not "buy the security argument". "We don't find it persuasive. We think it is excessive. There are less intrusive ways to do this,"

Facebook, it pointed out that the firm already faced many instances when it could not track users - such as the 198 million net users who use adblockers. "To the best of our knowledge ad-blocking users do not pose a critical threat to Facebook nor do users who install them need to go through burdensome security checks when they log in to Facebook."[790]

The judge ruled that this is personal data, which Facebook can only use if the internet user expressly gives their consent, as Belgian privacy law dictates.[791]

Data Anonymity

The possibility of correctly identifying people and attributes from anonymized data started one of the most important debates in privacy law. The credibility of anonymization, which anchors much of privacy law, is now open to attack. Critics of anonymization argue that almost any data set is vulnerable to a reidentification

788 Online Privacy: Who Writes the Rules?, http://www.nytimes.com/2015/01/01/opinion/online-privacy-who-writes-the-rules.html?_r=0

789 https://www.facebook.com/notes/alex-stamos/preserving-security-in-belgium/10153678944202929

790 http://cosic-be.blogspot.be/2015/10/preserving-privacy-in-belgium.html and What is Facebook doing with my data?, http://www.bbc.com/news/magazine-34776191

791 Belgian court orders Facebook to stop tracking non-members, http://www.theguardian.com/technology/2015/nov/10/belgian-court-orders-facebook-to-stop-tracking-non-members

attack given the inevitability of related data becoming publicly available over time, thereby setting the stage for a linkage attack. Defenders of anonymization counter that despite the theoretical and demonstrated ability to mount such attacks, the likelihood of reidentification for most data sets remains minimal. These divergent views might lead us to different regulatory approaches. Those that focus on the remote possibility of reidentification might prefer an approach that reserves punishment only in the rare instance of harm, such as a negligence or strict liability regime revolving around harm triggers. Critics of anonymization might suggest we abandon deidentification-based approaches altogether, in favor of different privacy protections focused on collection, use, and disclosure that draw from the Fair Information Practice Principles (FIPPs[792]).[793]

According to Rubinstein and Hartzog, neither technologists nor policymakers alone can protect us. We should think of reidentification as a data release problem. Sound data release policy requires a careful equilibrium on multiple fronts: law and technology, data treatment and data controls, privacy and utility. In their opinion, no matter how much we discuss about anonymization, the conclusion is that anonymization is dead and therefore we should focus on safe release of data.[794] I agree with this opinion. It is talked so much about storing and analysing, yet not too often, we remember about the origin of the data and how recklessly we release it, and we share it.

On the other hand I am not willing to dismiss the anonymization in general, even though anonymising data is a very difficult. When it comes to anonymising, three high-profile failures are widely cited:

1. AOL's 2006 release of anonymous search data;[795]
2. The State of Massachusetts's Group Insurance Commission release of anonymised health records;[796]
3. Netflix's 2006 release of 100m video-rental records.[797]

Researchers showed how relatively simple techniques could be used to re-identify the data, usually picking out the elements of each record that made them unique. According to wide research it is actually pretty simple to merge the "anonymous"

792 NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE, Appendix A – Fair Information Practice Principles (FIPPs), http://www.nist.gov/nstic/NSTIC-FIPPs.pdf

793 Rubinstein, Ira and Hartzog, Woodrow, Anonymization and Risk (August 17, 2015). Washington Law Review, Vol. 91, No. 2, 2016; NYU School of Law, Public Law Research Paper No. 15-36. Available at SSRN: http://ssrn.com/abstract=2646185, p. 2, 3.

794 Ibid., p. 54.

795 AOL releases search data on 500,000 users, http://arstechnica.com/uncategorized/2006/08/7433/

796 "Anonymized" data really isn't—and here's why not, http://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/

797 Netflix Spilled Your Brokeback Mountain Secret, Lawsuit Claims, http://www.wired.com/2009/12/netflix-privacy-lawsuit/

record with a different "anonymised" database and out pops the near-certain identity of the person. In the past, it was used mostly for identifying medical patients; today it can be used for any other purpose. In fact, de-anonymising has become a kind of full-contact sport for computer scientists, who proved that anonymisation schemes easy to defeat with clever re-identifying tricks. One example is how the "anonymised" data from a European phone company could be re-identified with 95% accuracy, given only four points of data about each person, with only two data-points, more than half the users in the set could be re-identified.[798] The study was conducted during fifteen months. It was the study of human mobility data for one and a half million individuals to find that human mobility traces are highly unique. In fact, in a dataset where the location of an individual is specified hourly, and with a spatial resolution equal to that given by the carrier's antennas, four spatio-temporal points are enough to uniquely identify 95% of the individuals.

The problem is that too often we hear that privacy is dead, irrelevant, or unimportant. However, it is important to remember the reason anonymization and pseudonymization are being contemplated in the General Data Protection Regulation is because its authors say that privacy is important, and worth preserving. They are talking about anonymising data sets because they believe that anonymization will protect privacy, and that means that they are saying, implicitly, privacy is worth preserving. The General Data Protection Regulation contains the definitions used in the document, that establishes the idea that there is such a thing as "anonymous" data and exempts it from regulation, and creates a second category of "pseudonymous" information that can be handled with fewer restrictions than are placed on personally identifying information.

According to Seth David Schoen[799], anonymization extremely difficult in our times. Just because something seems anonymous, does not mean it really is, both because of the mathematics of individual distinctiveness and because of the huge number of databases that are becoming available. That means we have to be extremely careful about whether things are truly anonymous, and not rely on our intuition alone. It is hard not to agree with this opinion, especially considering huge number of easy accessible databases.

It seems that, let me call it de-identification, is very difficult, but not impossible. According to Ed Felten[800], there is an emerging science of privacy-preserving data analysis that can be applied in some settings. Generally, data derived from the characteristics of individuals, including behavioural data, will likely convey

798 Y. de Montjoye, C. A. Hidalgo, M. Verleysen & V. D. Blondel, Unique in the Crowd: The privacy bounds of human mobility, Scientific Reports 3, Article number: 1376 (2013), http://www.nature.com/articles/srep01376

799 Staff technologist at the Electronic Frontier Foundation, https://www.eff.org/

800 Former member of the US Federal Trade Commission

information about individuals, absent some rigorous technical basis for believing otherwise.

Going further, Microsoft has pushed for an approach they call differential privacy[801]. In very short, it can be described with an example where researchers pose research questions to the original data controller, which returns intentionally corrupted answers, and it is possible allegedly mathematically quantify how much privacy harm was done in the process and then debate whether it was worthwhile in light of the benefits of the research.[802]

No matter how it is analysed now, the issue of anonymising data has two layers. The legal and practical. I find it very promising that it is included in the discussion connected to the coming regulation, but at the same time, all the concerns emphasised by experts show that this matter has to be takin seriously and with lots of precautions. It would be very unfortunate if we end up without proper regulations, because practical or technical consequences were oversight.

Both the European Commission and various E.U. Member States are also implementing regulations compelling private telecommunication companies to collect and store information potentially needed by security agencies in the context of future criminal acts,[803] a striking change of data processing methods indeed. The government no longer sticks to the traditional direct collection of data. It turns instead to private entities. In doing so, the state not only acknowledges that the majority of data is stored in the private sector, but also establishes a processing model systematically combining information gathered in both public and private sectors. As a result, the government can limit its own gathering activities and opt for compelling services by businesses using data that might be of interest to public agencies.[804]

5.3.1. NOYB – European Center for Digital Rights

European Center for Digital Rights - NOYB ("none of your business") is a non-profit organization based in Vienna, Austria established in 2017.[805] One of the co-foundeders is Austrian lawyer and privacy activist Max Schrems. NOYB aims to launch strategic court cases and media initiatives in support of the General Data

801 C. Dwork, Differential Privacy, Microsoft Research, http://research.microsoft.com/pubs/64346/dwork.pdf

802 Data protection in the EU: the certainty of uncertainty, http://www.theguardian.com/technology/blog/2013/jun/05/data-protection-eu-anonymous

803 Simitis S., Datenschutz - Rfickschritt oder Neubeginn?, 51 NJW 2473, 2477 (1998).

804 Simitis S., Privacy - An Endless Debate, California Law Review, Vol. 98, Issue 6, December 2010, p. 2002-2003

805 Scally, D.,Time to tell tech firms that private data is 'none of your business' – Max Schrems. Privacy activist is creating a non-profit organisation to fight for data protection, November 30, 2017, https://www.irishtimes.com/business/technology/time-to-tell-tech-firms-that-private-data-is-none-of-your-business-max-schrems-1.3309734

Protection Regulation, the proposed ePrivacy Regulation, and information privacy in general.[806]

NOYB started with filling complaints against Facebook and subsidiaries WhatsApp and Instagram, as well as Google LLC (targeting Android), for allegedly violating Article 7(4) by attempting to completely block use of their services if users decline to accept all data processing consents, in a bundled grant which also includes consents deemed unnecessary to use the service.[807]

Following the NOYB complaint, the French data protection authority (CNIL) announced that it has imposed a record fine of € 50 million on Google for violating the GDPR on 21 January 2019.[808] The penalty is based on two complaints by noyb.eu and the French NGO 'La Quadrature du Net' based on 'forced consent' on May 25, 2018. The GDPR prohibits such forced consent and any form of bundling a service with the requirement to consent (see Article 7(4) GDPR). Consequently access to services can no longer depend on whether a user gives consent to the use of data. On this issue a very clear guideline of the European data protection authorities has already been published in November 2017.[809]

5.3.2. Regulating Privacy

There is a proposition for three concepts of privacy regulation with consideration how they might address the challenges of privacy self-management in the big-data ecosystem:[810]

1) Individual empowerment through education and data portability;

Problems with individual control in the context of big data are numerous, and many stem from a fundamental disconnect between the information accessible to individuals regarding the likely uses of their personal information and the actions they can take to protect such information. Concepts of data sovereignty[811] and

806 Austrian activist launches consumers' digital rights group, November 28, 2017, https://www.apnews.com/18a537b8b234445fa4eab2633a4a516d

807 GDPR: noyb.eu filed four complaints over "forced consent" against Google, Instagram, WhatsApp and Facebook, Vienna 2018, https://noyb.eu/wp-content/uploads/2018/05/pa_forcedconsent_en.pdf

808 The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, January 2019, https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

809 Guidelines on Consent under Regulation 2016/679 (wp259rev.01), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

810 De Mooy M., Rethinking Privacy Self-Management and Data Sovereignty in the Age of Big Data. Considerations for Future Policy Regimes in the United States and the European Union, 2017, https://cdt.org/files/2017/04/Rethinking-Privacy_2017_final.pdf, p. 24.

811 A fundamental right and an individual's ability to maintain transparency and control over the possession, use, or deletion of one's personal data, subject to the laws of the jurisdiction in which the individual resides. The legal right of an individual to maintain control over the possession, use and deletion of their personal information, subject to the laws of the jurisdiction in which the individual resides.

data portability[812] offer levels of individual empowerment that could close this disconnect.

Data sovereignty and data portability would ideally facilitate increased engagement with data-management tasks, allowing people to determine how, when and for what purposes their data are used. It would give individuals authoritative legal rights over the data, with these rights traveling as the information moved. Data sovereignty also refers to the ownership of and responsibility for information. Proponents of this concept believe it offers a way to give people a power of self-determination regarding their information in big-data systems, leveling the playing field between individuals and the commercial and noncommercial entities that capture and share their information. In this way, data sovereignty mirrors some of the concepts in individual control, because it implies the ability to "access, create, modify, package, derive benefit from, sell or remove data, but also the right to assign these access privileges to others."[813] Overall, the ideas of data authority and portability are appealing to many people who envision a system in which they have complete control over the use or removal of their personal information.

Data sovereignty does appear to address the concerns of the individuals who consistently state in public-opinion polls that they feel powerless and resigned to the ubiquitous collection and use of their data. Ownership is a formidable way to empower individuals.

Data portability would allow individuals to move their personal information at will, and thus is complimentary to ownership regimes as a method of creating a more level playing field between individuals and businesses in a big data world.

The viability of the data-sovereignty and data-portability concepts depends on whether concerns regarding the ability of an individual to engage rationally. Any framework that emphasizes these two concepts must build or require the creation of technical tools for data management, implement consistent education and outreach programs aimed at improving individuals' capacities to navigate data choices, and finally create policy levers that allow individuals to negotiate fair terms for the use of their data.

It is likely that most people would be reluctant to devote themselves to taking the time and learning the skills required to manage data effectively. What people desire is the freedom to pursue the ends of digital production, without being inhibited by the means.[814]

---

812 Data portability is the right of an individual to move his or her personal information between online locations without loss or distortion.

813 Loshin, D. "Knowledge Integrity: Data Ownership." 2002. http://ori.dhhs.gov/education/products/n_illinois_u/datamanagement/dotopic.html

814 Obar, Jonathan A., Big Data and The Phantom Public: Walter Lippmann and the Fallacy of Data Privacy Self-Management (August 20, 2015). https://ssrn.com/abstract=2239188

Additionally, it is difficult to imagine how data-portability and data-sovereignty laws would function in all of today's current legal settings; for example, how would portability square with antitrust law in the United States? Large internet companies like Facebook, which have already established a brand and hold data relating to as many as a billion people worldwide, would be less affected by users' ability to move their information from place to place than would small business operators. This in turn could result in less competition and diminished choice for individuals. Another consideration is that giving individuals more control over their personal information could indirectly impact the fairness of data analytics, resulting in "cumulative disadvantage" due to the narrowing of possible categories or results.[815]

In a policy framework centered on data ownership and portability, the government would need to implement education programs providing individuals and businesses with the appropriate tools to maneuver in the new data landscape. Helping the public understand data-processing practices and data-ownership rights, as well as their implications, should be in part the responsibility of the government, perhaps in partnership with commercial or nonprofit entities with communications expertise.

2) Corporate accountability through industry self-regulation;

It is incredibly difficult for the average person to understand how data is collected, shared and used in the vast online ecosystem, and many regulatory systems ask individuals to make decisions despite this void of understanding. The role of the user's self-determination in situations in which consumers are not able to understand deeply data processing and its purposes,[816] or are not in the position to decide[817] render individual control useless[818] and create resentment against the forces that produce this helplessness. Companies, fearing liability yet subject to enormous pressures to get their products to market quickly, often end up offering their customers minimal choice and more notice, rather than spending the time to implement thoughtful data practices and policies.

The use of impact assessments in a self-regulatory scheme is one approach that could potentially provide more clarity and actionable information for individuals, while balancing companies' legitimate business interests. Under this model,

---

815 Oscar H. Gandy Jr., Engaging Rational Discrimination: Exploring Reasons for Placing Regulatory Constraints on Decision Support Systems, 12 Ethics & Info. Tech. 29, 37-39 (2010).

816 The Boston Consulting Group. "The Value of Our Digital Identity." 2012: 4. www.libertyglobal.com/PDF/public-policy/The-Value-ofOur-Digital-Identity.pdf

817 Art. 7 (4), PGDPR ("Consent shall not provide a legal basis for processing, where there is a significant imbalance between the position of the data subject and the controller"). In 2013, the Committee on Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament dropped Art. 7 (4), see Art 7 PGDPR-LIBE.

818 Mantelero, A., "The Future of Consumer Data Protection in the E.U.: Rethinking the 'Notice and Consent' Paradigm in the New Era of Predictive Analytics." Computer Law & Security Report 30, Nov. 2014: 643, 655.

companies themselves would produce assessments giving individuals a better understanding of how or when their personal information might be used in ways that are potentially beneficial or detrimental to them. A self-regulatory assessment system could also prompt companies to review their own data practices more rigorously, increasing transparency without increasing their liability. To be effective, voluntary risk assessments would have to address data processing and its subsequent uses, including variables such as the relationship between the purposes, the context of collection, the reasonable expectations of the data subjects, the nature of the personal information and the impact of its collection and use on the data subjects.[819]

One of the most important considerations in performing self-regulatory assessments would be determining when they should take place - that is, either before or after data is collected. Pre-collection assessment probably provides the most protection for consumers, as any such procedure would likely limit the scope and amount of data obtained. Post-collection assessments are also potentially useful as a way to explain the details of data processing and use to consumers, as well as serving as a form of accountability regarding actual practices but could also end up functioning as simply as another box to check as companies rush to launch a product.

Self-regulatory schemes are typically greatly limited by a lack of transparency and enforcement. Indeed, it was in part due to the failure of self-regulation in the first place that data-protection regulations were created in Europe (though the primary goal of the DPD was harmonization of standards across the European Union). The same is true in the United States, albeit to a lesser extent. It is possible that a legally mandated requirement to conduct impact assessments at the company level could obviate this.

A 2015 report from the OECD states that the success of industry self-regulation depends on a number of factors, including:

- the strength of the commitments made by participants;
- the industry coverage of the self-regulation;
- the extent to which participants adhere to the commitments;
- the consequences of not adhering to the commitments.[820]

Self-regulation commitments could create market barriers for existing small businesses that could not afford to implement the requirements; these costs could end up being passed along to consumers. The power of big business interests might also mean that the scheme could wind up being less favorable to smaller business needs. One step toward the achievement of balance in a self-regulatory framework

819 Article 29 Working Party, Opinion 03/2013 on purpose limitation. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

820 OECD. Industry Self-Regulation: Role and Use in Supporting Consumer Interests. Organization for Economic Cooperation and Development, March 2015.

might be increasing the participation of stakeholders such as governments and civil-society or consumer organizations.

3) Collective accountability using legally mandated impact assessments.

In the automobile, pharmaceutical and environmental sectors, as examples, the public is not expected to understand the details of how regulated products work or what side effects they may produce. We do not expect individuals to perform their own assessments of risk in these areas; instead, we rely on entities, created by government mandate, that have the expertise to evaluate the efficacy and safety of products or industrial practices. In the same way, data -usage regimes could require a rigorous assessment of the impact of any big-data processing, performed before such processing takes place, which would consider the impact and ethical considerations of the data use for individuals as well as for society.[821]

Education is a crucial component to this approach as well, even though legally mandated collective risk assessments would decrease the data-management burden on the individual in the short run. To avoid overly paternalistic regulation and a continued disempowerment of the public, policymakers would need to increase transparency and accountability by publishing assessments along with contextual information describing how the public interest might be adversely or positively affected as a result of the data processing or use.

A number of logistical questions would have to be answered regarding these assessments. For example, what method would be used to perform the assessments? How would they be altered or standardized across sectors and countries? What parties would be responsible for performing the assessments, and how frequently would they be required?

This collective approach to the use of assessments beyond a self-regulatory scheme would necessitate the creation of legal mandates for data controllers - that is, the entities deciding on the objectives and methods of the processing of personal data. It would restrict the role played by individual control in order to increase the influence of independent authorities acting on behalf of the common good.[822]

In this scenario, data-protection authorities rather than individuals would be viewed as holding the technological knowledge necessary to evaluate collective risks associated with data processing and would adopt the appropriate legal remedies and oversight mechanisms to address them.

821 Mantelero, A., "Data protection in a big data society: Ideas for a future regulation." Digital Investigation, November 2015.

822 Bygrave L., Data Protection Law. Approaching its Rationale, Logic and Limits (n 32) 86 ("the monitoring and enforcement regimes set up by data protection laws are also a mixture of paternalistic and participatory control forms").

Rather than entirely reshaping traditional models of data protection in the United States and the European Union, this option would be responsive to the power asymmetry between data subjects and controllers created by the big data environment.

An ideal policy solution would combine the strengths of each framework discussed here. Empowerment, ownership, portability, corporate accountability and collective assessment work well in conjunction with one another and would benefit from the inclusion of key FIP (Fair Information Practices) principles such as access, transparency, purpose and use limitations, data minimization, and data retention.

5.3.3. Self-Regulation and Social Engagement

There are ideas about Privacy being more than just a Fundamental Human Right, but also right having an economic, marketable value at least since 1990s'. Ann Cavoukian asks:

"*Can privacy issues be resolved by relying on the economic self-interest of individuals to make the appropriate decisions as to the degree of privacy that should be provided?*"[823]

She proposed market approach to privacy.[824] Especially if individual control and personal choice if a market framework for protecting privacy was to be adopted.

Considerable debate has developed over the merits of legislation vs. self-regulation as the mechanism of choice for protecting informational privacy in the private sector.[825]

Self-regulation rather than legislation is seen as the most appropriate mechanism to protect privacy on the grounds that legislation is too inflexible and time-dependent to be responsive to the fast-moving world of information technology.

Government legislation will likely lead to an overly bureaucratic and cumbersome regulatory process that will only result in raising the operating costs of the businesses involved. While undoubtedly there is some merit in this claim, it cannot be denied that business has been very slow to adopt self-regulation, even though it is said to be its preferred course of action. Policymakers should recognize progress in self-regulation and not rush to regulate the Net in ways that could undermine electronic commerce.

---

823 Cavoukian A., Privacy as a Fundamental Human Right vs. an Economic Right: An Attempt at Conciliation, 1999, http://www.ontla.on.ca/library/repository/mon/10000/211714.pdf, p. 1

824 Some of the scholars associated with the market approach include: Eli Noam, Kenneth C. Laudon, Hal Varian, Peter Swire, among others. Their views are collected in a paper issued by the U.S. Department of Commerce, Privacy and Self-Regulation in the Information Age, National Telecommunications and Information Administration, Washington, D.C., 1997.

825 Privacy and Self-Regulation in the Information Age, issued by the National Telecommunications and Information Administration, U.S. Department of Commerce, 1997

Self-regulation cannot be comparable to an organization adopting a code of conduct with respect to how it will deal with personal information. While such codes are commendable and to be encouraged as a way to create a corporate culture respectful of privacy, codes alone cannot be fully relied on. If they are voluntary, thus not universally adopted, individuals are compelled to expend considerable time and energy researching which firms have codes and how effectively they are enforced. Therefore, irrespective of how individuals negotiate their privacy, the possibility remains that they may not be able to hold the firm to respect their choices.[826]

Providers have realized the pressing need for clear rules, but their primary choice is self-regulation,[827] as the case of Facebook reveals, despite its founder's assertion that social concerns about privacy are diminishing. Hence, providers maintain a policy that permits them to safeguard their autonomy and avoid legislative scrutiny. Nonetheless, self-regulation does not suffice, as with automated data retrieval.[828]

While data protection laws create a formal administrative framework for the protection of personal information, they do not encourage individuals to take an active role in the protection of their own personal information.[829] Individuals have asymmetrical information and bargaining power relative to various organizations. Under these conditions, individuals are not in an ideal position to exercise control or make informed choices with respect to the uses of their personal information.[830]

Whatever value privacy may have for individuals, this will be determined by everyone's utility preferences. Individuals would set the price of their personal information in competitive markets that, in theory, should permit individuals to obtain the level of informational privacy most desirable to them, and permit businesses to obtain the optimal volume of personal information in order to carry on commercial transactions. This is with the assumption that companies have a legitimate interest in acquiring personal information for business purposes, and this should not be arbitrarily restricted.[831]

---

826 Implementing Privacy Codes of Practices, Colin Bennett chapter 2

827 Facebook Changes Privacy Policy, BBC, Aug. 27, 2009, http://news.bbc.co.uk/2/hi/8225338.stm; Facebook Gives Users More Control of Privacy, BBC, Dec. 9, 2009, http://news.bbc.co.uk/2/hi/technology/8404284.stm; Facebook Faces Criticism on Privacy Change, BBC, Dec. 10, 2009, http://news.bbc.co.uk/2/hi/8405334.stm; Haupt F., Sag mir, wo du stehst und wohin du gehst, FRANKFURTER ALLGEMEINE ZEITUNG, Mar. 20, 2010, at 42; Wieduwilt H., Gesucht: Mdnnlich, liiert, heterosexuell, aus Berlin, FRANKFURTER ALLGEMEINE ZEITUNG, Dec. 22, 2009, p. 19.

828 Simitis S., Privacy - An Endless Debate, California Law Review, Vol. 98, Issue 6, December 2010, p. 2004

829 Cavoukian A., Privacy as a Fundamental Human Right vs. an Economic Right: An Attempt at Conciliation, September 1999, http://www.ontla.on.ca/library/repository/mon/10000/211714.pdf, p. 12.

830 Ibidem, p. 26.

831 Priest W. C., The Character of Information: Characteristics and Properties of Information Related to Issues Concerning Intellectual Property, Office of Technology Assessment, 1994.

Another idea is promoted in the paper "Online Privacy: Towards Informational Self-Determination on the Internet".[832] The authors want to raise awareness for the actual state of the art of online privacy, especially in the international research community and in ongoing efforts to improve the respective legal frameworks, and to provide concrete recommendations to industry, regulators, and research agencies for improving online privacy. They examine how the basic principle of informational self-determination, as promoted by European legal doctrines, could be applied to infrastructures like the internet, Web 2.0 and mobile telecommunication networks. The idea comes from the fact that collection and monetization of user data has become a main source for funding "free" services like search engines, online social networks, news sites and blogs, neither privacy-enhancing technologies nor its regulations have kept up with user needs and privacy preferences.

Michelle De Mooy in her paper about rethinking privacy[833] starts with the idea that the rise of large data collection and processing, also known as big data, has challenged the validity of data-protection regimes founded on ideals of individual control. She examines possible new ways to achieve individual control in big-data world. Three complementary notions of privacy self-management that may offer a way forward in constructing modern privacy regulations, with data sovereignty playing the central role were investigated.

The first concept, dealing with education and data portability, would give more responsibility to individuals, empowering as well as burdening them. However, since the empowerment of individuals alone cannot address all the challenges presented by big data, a second approach would make companies responsible for data protection in the form of voluntary industry self-regulation. This would relieve individuals of a portion of the data-management burden; however, self-regulation often fails to meet the standards of accountability and transparency fully.

To account for this potential shortfall, a third concept is introduced, in which third parties would perform state-mandated impact assessments of data-management practices, advocating for users' interests and creating greater transparency. However, while these third-party assessments could help users, there is a risk of treating users in a patronizing manner. To prevent this, users would need to engage in the education addressed in the first concept, thus enabling them to use the assessments in a self-determined manner. These collective approaches can address the challenges posed by big data. The basis for their implementation remains governmental regulation, which assigns rights to individuals, creates a dependable framework and balances

832 Fischer-Hübner S., Hoofnagle C., Krontiris I., Rannenberg K., Waidner M., Online Privacy: Towards Informational Self-Determination on the Internet (August 29, 2011). Dagstuhl Manifestos, Vol. 1, Issue 1, 2011, https://ssrn.com/abstract=2468200

833 De Mooy M., Center for Democracy and Technology, Rethinking Privacy Self-Management and Data Sovereignty in the Age of Big Data. Considerations for Future Policy Regimes in the United States and the European Union, 2017, https://cdt.org/files/2017/04/Rethinking-Privacy_2017_final.pdf

power asymmetries. As regulatory systems have been stretched to their limits by the challenges of digitization, a multipronged approach of the kind advocated by this report is necessary to overcome the weaknesses inevitable in any single concept.

Finally, Taj-Johnston Montesano[834] proposed a solution he called Project R.O.S.E. (Return On Social Engagement) - Digital Privacy Assets and the right to economic self-determination. It is a new vision of human empowerment and inclusion that seeks to provide a market-based solution to reduce the widening gulf in the digital economy between the elite beneficiaries of data collection/mining and the disenfranchised masses who generate the data in their daily communications and transactions but are excluded from participating in their exploitation.

The creation of a data marketplace in which individuals have a relationship of sovereignty to their personal data, with the ability to move data at will, is one way these concepts might work in practice. The data-marketplace idea has been proposed numerous times over the years. One scholar has dubbed this a "National Information Market" (NIM)[835]; it follows an economic model under which individuals would sell personal information only if they were offered an acceptable price (one equal or greater than the value of not releasing the information). Under the NIM scenario, individual considerations and valuations of personal privacy would function as a limiting factor on the market, as buyers would also be determining whether the social value of the access to the information, they hope to purchase was worthwhile.[836]

The aim of the project was to provide a more sustainable model of the data economy by gathering members into a collective organization with a transparent charter and structure to enable and promote individual inclusion, protection, and participation in the new economy; thereby providing more equitable distribution of assets, more opportunities for entrepreneurial growth and a sustainable vehicle for social enterprise.[837]

In the discussion about discussion one more thing needs to be considered. The same people who otherwise insist on the inaccessibility of their private sphere have evidently not the slightest hesitation to publicly revealing all its details. It is no wonder that social networking information, provided, for instance, by widespread flirting on Facebook, is now used in the United Kingdom as a divorce reason in every fifth divorce or separation case. An evaluation of chatting on the Internet has shown that it manifestly contributed to the proliferation of divorces in the last two years.[838] But the more the Internet is used to circulate and access strictly personal

834 http://mcpinvest.at/founders/

835 Laudon, K. C. "Markets and Privacy." Communications of the ACM 39 (9), 1996: 92-104.

836 Mungan, M., "Conditional Privacy Rights." April 16, 2016.

837 Project R.O.S.E., http://mcpinvest.at/projects1/

838 Facebook liefert immer ofter Scheidungsgrund, FRANKFURTER ALLGEMEINE ZEITUNG, Dec. 24, 2009, p. 8.

information, the clearer the question arises: Can a legally guaranteed respect for privacy be upheld in a society in which technology incites and sustains a constant disclosure of highly private data?[839]

5.3.4. Privacy Enchancing Technologies (PETs)

Privacy-enhancing technologies or PETs are another element in this privacy architecture, offering potential privacy solutions in the context of electronic communications that identify individuals during interactive sessions. PETs could restrict the gathering of personally identifying information through a variety of means building on encryption, during the course of such sessions. These technologies offer another way for individuals to exercise freedom of choice, by permitting them to engage in transactions without revealing personal information unnecessarily, or without revealing any identifying information at all. Emerging technologies, especially those focussing on anonymous and pseudonymous identifiers, may well advance as the primary means of protecting online privacy.

A technological solution to privacy seems a fitting approach in an age of information technology. This solution may, therefore, be viewed as just another type of market solution. If hardware and software can be designed to incorporate privacy protections, and such technologies are readily accessible to the general public, PETs can become a core feature of how to resolve privacy problems raised by technology itself.[840]

The principal privacy-enhancing technology is strong encryption, which permits individuals to keep their communications and their identities confidential. In the context of our discussion of how markets could protect privacy, PETs can be viewed as a parallel approach. By limiting access to personal information through the design of various emerging technologies, PETs will limit the creation of databases of personal information and the disclosure of that information to third parties.[841]

As the collection of personally identifiable information by online services has grown, so too has public concern about online privacy. In an effort not to alienate their online customers, companies are beginning to become mindful of consumer privacy. And yet, the cost of "permission marketing," which requires customer consent prior to initiating marketing efforts, can be significant.

---

839 Simitis S., Privacy - An Endless Debate, California Law Review, Vol. 98, Issue 6, December 2010, p. 2004-2005

840 Information and Privacy Commissioner/Ontario and Registratiekamer (Netherlands)Privacy-Enhancing Technologies: the path to anonymity, 2 vols., 1995

841 Cavoukian A., Privacy as a Fundamental Human Right vs. an Economic Right: An Attempt at Conciliation, September 1999, http://www.ontla.on.ca/library/repository/mon/10000/211714.pdf, p. 22.

After more than 20 years of research in the area of privacy and PETs, there exists a wide variety of mechanisms.[842] Broadly speaking, we could distinguish between opacity tools and tools that enforce other legal privacy principles, such as transparency, security or purpose binding.

Opacity tools can be seen as the "classical" PETs, which "hide information", i.e. striving for data minimization and unlinkability. They cover a wide variety of technologies, ranging from cryptographic algorithms and protocols (e.g., [homomorphic] encryption, blind and group signatures, anonymous credentials, oblivious transfer, zero-knowledge proofs etc.) to complex systems like user-centric identity management. Opacity tools can be further characterized depending on whether they focus on data minimization at the network layer or at the application layer.

Transparency-enhancing tools (TETs) belong in the second category of PETs and focus on enforcing transparency, in cases where personal data need to be processed. Transparency understood us the informative representation to the user of the legal and technical aspects of the purpose of data collection, how the personal data flows, where and how long it is stored, what type of controls the user will have after submitting the personal data, who will be able to access the information, etc.[843]

TETs frequently consist of end-user transparency tools and services-side components enabling transparency. The end-user tools include, among other techniques:

(1) tools that provide information about the intended collection, storage and/or data processing to the users when personal data are requested from their system (via personalized apps or cookies)

(2) technologies that grant end-users online access to their personal data and/or to information on how their data have been processed and whether this was in line with privacy laws and/or negotiated policies.

Examples are the Google Dashboard or the Amazon's Recommendation Service, which grant users online access to their data and allow them to rectify and/or delete their data. However, these are server-side functions and not user-side tools and they usually grant users access only to parts of their data and not to all the data that the respective service processes. An example of user-side transparency enhancing tool is the Data Track developed in the EU project PrimeLife, which gives the user an

842 Fischer-Hübner S., Hoofnagle Chris J., Krontiris I., Rannenberg K., Waidner M.,Online Privacy: Towards Informational Self-Determination on the Internet (August 29, 2011). Dagstuhl Manifestos, Vol. 1, Issue 1, 2011, http://drops.dagstuhl.de/opus/volltexte/2011/3205/pdf/dagman_v001_i001_p001_11061.pdf, p. 8.

843 Fischer-Hübner S., Hoofnagle Chris J., Krontiris I., Rannenberg K., Waidner M., Online Privacy: Towards Informational Self-Determination on the Internet (August 29, 2011). Dagstuhl Manifestos, Vol. 1, Issue 1, 2011, http://drops.dagstuhl.de/opus/volltexte/2011/3205/pdf/dagman_v001_i001_p001_11061.pdf, p. 7.

overview of what data have been sent to different data controllers and also makes it possible for a data subject to access her personal data and see information on how her data have been processed and whether this was in line with privacy laws and/or negotiated policies.

In the current state, once the data has been submitted to an online information system, individuals get no knowledge about any further processing. But, even if we assume that the data processing of such complex systems like Facebook, Apple iTunes or Google Search could be transparent to the public, it would be hard or impossible for ordinary individuals to understand what happens with their data. Full transparency of data movements also increases security problems in such environments, if misused with malicious intent. Consequently, this limitation leads to the observation that it is more important for individuals to understand the outcome and implications of data flows in complex online information systems than understanding the full data movements. One technique, among others, that can achieve this kind of transparent outcome-based approach is the creation of ad-preferences by some third-party advertisers, where users are allowed to see the set of outcomes, based on which the data has been forwarded to the third-party (examples here would include Google Ad Categories or the Deutsche Telekom Privacy Gateway for location-based services).

Infrastructures have not been designed with privacy in mind, and they evolve continuously and rapidly integrating new data collection practices and flows. Current privacy mechanisms not only have difficulties in catching up with these developments, but they also collide with some security and business requirements. A redesign of the system in question can often resolve the collision of interests, but this sometimes requires costly investments.[844]

The demand of users for PETs is rather low today. One reason for this is the lack of user awareness with respect to privacy problems, which can be partly attributed to missing transparency of data acquisition and the related information processing, as emphasized above. A second reason lies in the complicated and laborious nature of control imposed on persons, as no legal standards or general consumer protection rules exists. Finally, PETs do not always take into consideration the evolution of privacy models caused by the rapid creation of new technologies and communication models.[845]

---

844 Fischer-Hübner S., Hoofnagle Chris J., Krontiris I., Rannenberg K., Waidner M., Online Privacy: Towards Informational Self-Determination on the Internet (August 29, 2011). Dagstuhl Manifestos, Vol. 1, Issue 1, 2011, http://drops.dagstuhl.de/opus/volltexte/2011/3205/pdf/dagman_v001_i001_p001_11061.pdf, p. 8.

845 Fischer-Hübner S., Hoofnagle Chris J., Krontiris I., Rannenberg K., Waidner M., Online Privacy: Towards Informational Self-Determination on the Internet (August 29, 2011). Dagstuhl Manifestos, Vol. 1, Issue 1, 2011, http://drops.dagstuhl.de/opus/volltexte/2011/3205/pdf/dagman_v001_i001_p001_11061.pdf, p. 8.

The lack of adoption of existing PETs lies in some models in data commerce that are based on access to personal data. In the current eco-system, doing nothing about privacy or even aggressively collecting data sometimes pays off, as some companies seem to acquire new clients with new features based on creative data use and serendipity. Furthermore, for some players, implementing complex data minimization schemes is costly and time consuming and makes information filtering catered to the end-user much harder, if not impossible.[846]

There is a lack of clear incentives for enterprises to manage personal data in a privacy-respecting manner, to design privacy-preserving products, or to make the use of personal data transparent to the data subject for following reasons:

1. Lack of customer (individuals, business partners) and market demand for privacy respecting ICTs, systems, services and controls (beyond punishments for breaches and other excesses). Usage models for privacy-enhancing technologies cannot currently be targeted to customer demand;
2. Some industry segments' norms, practices and other competitive pressures that favour exploiting personal data in ways contrary to privacy and the spirit of informational self-determination (resulting in diffusion of transparency and accountability);
3. Poor awareness, desire, or authority within some industry segments on the operationalization of privacy (e.g., to integrate existing PETs, to design privacy-respecting technologies and systems, and to establish, measure and evaluate privacy requirements);
4. Lack of clarity, consistency, and international harmonization in legal requirements governing data privacy within and across jurisdictions (avoided, for example, by migrating data somewhere up in the cloud).

Some answers and solutions:

1. the protection of privacy of users across different media,
2. the transparency for processing of personal data,
3. the acceptance and incorporation of improved privacy-enhancing technologies by technologists outside of the "privacy community".[847]

846 Fischer-Hübner S., Hoofnagle Chris J., Krontiris I., Rannenberg K., Waidner M., Online Privacy: Towards Informational Self-Determination on the Internet (August 29, 2011). Dagstuhl Manifestos, Vol. 1, Issue 1, 2011, http://drops.dagstuhl.de/opus/volltexte/2011/3205/pdf/dagman_v001_i001_p001_11061.pdf, p. 9.

847 Fischer-Hübner S., Hoofnagle Chris J., Krontiris I., Rannenberg K., Waidner M., Online Privacy: Towards Informational Self-Determination on the Internet (August 29, 2011). Dagstuhl Manifestos, Vol. 1, Issue 1, 2011, http://drops.dagstuhl.de/opus/volltexte/2011/3205/pdf/dagman_v001_i001_p001_11061.pdf, p. 9.

Challenges to the PETs:[848]

1. Promoting Transparency - Transparency enhancing technologies - (TETs), which have been developed in the recent years within research projects and by the industry, can help end-users to better understand privacy implications and thus help to increase the user awareness, as we demanded. On the other hand, allowing users to control and correct their data processed at services sides will also lead to better data quality for the respective industries. Industry needs to foster in-house transparency and awareness for the risks of system-imminent privacy issues in order to effectively enhance privacy in the developed products and services. Principles, such as data minimization and purpose-binding, have to become design principles for processes, IT, service and product design. Industry needs to consistently consider privacy issues, risks, and privacy principles in internal guidelines. These guidelines need to be communicated to engineers, developers, etc. to create a "culture of privacy".
2. Designing and Delivering Privacy Respecting Products to End-users -
3. When building applications, engineers often lack practical knowledge on incorporating PETs to achieve security and privacy protection. To support engineers in employing privacy-enhancing technologies, we propose to build blueprints and sample prototypes for key scenarios and for different industries. Examples for such prototypes include the following:
   I. A service that can be delivered to a user on a mobile device, such that the parties involved are able to deliver their parts and are paid for their service, while the user is ensured that every such party receives and stores only minimal data. The user is provided with transparency and control of his own data flows, while data dispersion is minimized, e.g. by attribute-based access-control.
   II. A communication platform that offers its users a convenient communication and collaboration environment with simple and secure user privacy controls to set the audience for certain private data dependent on different social roles and the support of user pseudonyms. The prototype must further demonstrate its economic viability by proper business models that do not conflict privacy requirements.
4. Identity Management as a Key Technique - Identity management is instrumental to the implementation of online privacy management.[849] Identity management can be used to manage handling of data relevant to

848 Fischer-Hübner S., Hoofnagle Chris J., Krontiris I., Rannenberg K., Waidner M., Online Privacy: Towards Informational Self-Determination on the Internet (August 29, 2011). Dagstuhl Manifestos, Vol. 1, Issue 1, 2011, http://drops.dagstuhl.de/opus/volltexte/2011/3205/pdf/dagman_v001_i001_p001_11061.pdf, p. 9-11.

849 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_en.pdf

satisfy privacy requirements, such as data minimization and transparency. The scope of identity management is quite broad, comprising authoritative information about legal persons, customer or user relationships, self-issued claims, pseudonyms and anonymous credentials. A minimum of personal data must be conveyed to the service in order to authenticate and authorize the accessing subject. For this the user-centric identity management could be useful. In this context implies that personal data – even in cases that is created by a service – is always handed back to the user upon completion of the service. If the user desires consistency across service invocation, it is her decision to hand over the data again to the same or another service. This way, individuals can supervise and limit personal data disclosure and exercise rights of access to their data held by third parties. User-centric identity management allows users to detect any linkages to third parties created from the primary relationship. Enterprise policies and procedures should support user-centric identity management as well, to prevent unwanted linkages and inadvertent disclosures of personal data.

Neither the current European legal framework, nor the US approach toward private sector self-regulation, has been effective for the protection of privacy online, particularly with regard to new business models, such as behavioural targeting, user profiling, social networking and location-based services. Key weaknesses in the EU framework include that:

1) services based predominantly in the US are effectively outside European jurisdiction
2) European users have little choice but to "consent" to companies' terms of use and privacy policies in the absence of alternatives of comparable functionality,
3) the concept of "personal data" is currently the necessary trigger for the applicability of the GDPR
4) seems to be too much reliance on ex post securing of data rather than on ex ante elimination of privacy risks through data minimization (for example Art.29 WP Opinion on smart metering10 omitted entirely any consideration of radical data minimization through cryptographic methods).[850]

5.3.4. Technological solution (the Blockhain technology)

Conflict between law and technology isn't new. Even the best law could become helpless ore even useless in the confrontation with the new technology. However, it is important to point that if there is no legal regulation on new technological

850 http://research.microsoft.com/en-us/projects/privacy_in_metering/3. Brandimarte L., Acquisti A., Loewenstein G. Privacy concerns and information disclosure: An illusion of control hypothesis. In Proceeding of the 9th Workshop on the Economics of Information Security (WEIS 2010), June 2010.

phenomenon then "society has been caught napping"[851]. Right to be forgotten, an old concept, but new addition to the law, has already met with some criticism, but now it may face another issue - blockchain technology. In some cases, as it is designed, blockchain prevents data from being erased. That includes personal data.

For the first time blockchain - a cryptographically secured chain of blocks was described in 1991 by Stuart Haber and W. Scott Stornetta.[852] Today blockchain technology is widely recognized as a support for the Bitcoin cryptocurrency.[853] Blockchain is like a large ledger. Within it, every data of every single entry is saved. When new data is added to a blockchain, peers in the network check the data to ensure that it is valid to add it, to avoid fraud by rogue nodes. The data that the peers need to check needs to be stored transparently in the blockchain.

It is very important to underline that blockchain can be used for various purposed. For handling money, it is a highly anonymous public blockchain. In case of storing user data, it can be a true distributed database that do allow for editing and deleting records. At least in some cases, but there are already some examples. Blockchain is not always anonymous, bitcoin is, blockchain not always. It very much depends on what is put there.[854] If specific blockchain can be anonymous, then theoretically it is excluded from the cover of General Data Protection Regulation.[855] All that being said, I must mention already at this point, that blockchains are not necessarily bad for privacy.

The GDPR gives individuals substantial control over their data by providing them with more information as to how their data is processed, which must be presented in a clear and understandable way. It gives the right to know when their data has been hacked, adds data protection safeguards and privacy-friendly default settings and strong enforcement of GDPR violations. Additionally, the GDPR contains a clear right to be forgotten provision in Article 17. This is designed to help people better manage data protection risks online and allow individuals to delete their data if there are no legitimate grounds for the information to remain public.

---

851 Saarenpää A., Legal Informatics: a Modern Social Science and a Crucial One [in:] Wahlgren P. (ed.), Scandinavian Studies in Law Volume 65. 50 Years of Law and IT. The Swedish Law and Informatics Research Insitute 1968-2018, Stockholm 2018, p. 18

852 Haber S., Stornetta S., (January 1991), "How to time-stamp a digital document", Journal of Cryptology. 3 (2), p. 99–111.

853 Pignal, Blockchain, The next big thing – Or is it?, The Economist Online, http://www.economist.com/news/special-report/21650295-or-it-next-big-thing; Pilkington, Blockchain Technology – Principles and Applications, p. 225, [in:] Olleros, Zhegu, Research Handbook on Digital Transformations, Cheltenman 2016

854 Lucas M., The difference between Bitcoin and blockchain for business, https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-bitcoin-and-blockchain-for-business/

855 Anonymous data that definitely not allow to identify the data subjects are excluded from the scope of the GDPR

However, the technology, as usual complicates the situation. The new personal data definition includes online identifiers as potential revealing factor. It is difficult to say, at this point, which of such online identifiers can be found in relation to blockchain technology. To make it clearer I will give an example. This is an example of TOR Project Internet Browser. This browser prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites which are blocked.[856] To be able to use the full functionality of it there are certain, strict rules. Some of them are extremely unusual, but give the idea of what can be an online identifier. From TOR browser guide, we learn:[857]

We should not resize browser window - if we do, our browser instance has a potential to have a unique viewport size and hence, there is a probability we can be tracked. Whatever size window TOR Browser opens, do not re-size it. Removing a menu bar or using full screen in TOR Browser is recommended against. The latter is known to modify the screen size, which is bad for the web fingerprint. The point of this advice is that if your browser is full screen, it will be the same size always and therefore it is potentially trackable between sessions. If a custom browser size is associated with a one-time-use anonymous session then it should not be a problem except that it leaks information about what window sizes are possible on our system, and our custom resize is very unlikely to be random. Rather probably predictably proportional to our actual screen size.[858]

Knowing something as small and as simple as a window size, let's look at blockchains. Blockchains can hold vast amounts of data and depending on the application of the blockchain some of this data may be classed as personal data under General Data Protection Regulation. Depending on how the blockchain operates, the pseudonymized public addresses which are recorded in every transaction and hashed onto the chain may also constitute personal data. If personal data is being recorded onto the chain, then every node on the network will be a data processor as soon as it receives a new block of data for updating its own copy of the ledger. This poses difficulties with ensuring compliance with the GDPR.

Additionally, every blockchain contains transaction data. That data needs to be designed so that it is not disclosive in and of itself, which may be a tricky balance as that data might also be necessary to assess whether the transaction is valid and therefore prevent fraud or errors. Transactions should also be designed so that they cannot be used to add comments that might include personal data.

856 https://www.torproject.org/projects/torbrowser.html.en

857 https://www.torproject.org/docs/faq.html.en

858 Tor Anonymity: Things Not to Do, January 4, 2016, https://news.ycombinator.com/item?id=10833629

In some cases, personal data is required to verify validity of a transaction in the blockchain. For a node to check a bitcoin transaction, it must have access to all previous transactions and can check that the person giving the bitcoins has them to give. It must be possible to reconstruct the full financial history of every person exchanging bitcoins: how many bitcoins they have, where they got those bitcoins from, whom they spend their bitcoins with - this is personal data. Pseudoanonymity[859] of the bitcoin address can help, but it can be easily breached if the address is associated with a donate button. Therefore, it is advised to hold several bitcoin addresses and not to transfer bitcoins between those accounts to avoid others linking them together.[860]

It is important to remember that blockchains do not have to expose personal data directly to reveal private information about people. A blockchain recording is used by health practitioners does not need to include the entirety of someone's health records to reveal information about them. Metadata may be sufficient to reveal personal details. It brings a question. Considering the main characteristic of the blockchain technology, that is immutability, how can we apply the right to be forgotten?

Right to be forgotten can be described as the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purpose.[861] It has clear limits and rules given in art. 17 from General Data Protection Regulation, right to erasure ('right to be forgotten'). Unlike the popular believe, it is not absolute, because of clear legal limitations. There are some possible limitations from new technologies (i.e., Blockchain)

The key benefit of blockchains is the immutability[862] of the data – all data being recorded and maintained in the chain from the start of the blockchain are an undisputable record for verification purposes. Once data has been written to a blockchain no one, not even a system administrator, can change it. If this data is made up of personal data, then erasure or rectification of the personal data would be theoretically impossible. This is likely to pose a greater issue as data subjects have a right to require data controllers to rectify and erase their data.[863]

---

859 Bitcoin is pseudonymous. Sending and receiving bitcoins is like writing under a pseudonym. If an author's pseudonym is ever linked to their identity, everything they ever wrote under that pseudonym will now be linked to them. - Bitcoin Anonymity - Is Bitcoin Anonymous?, https://www.buybitcoinworldwide.com/anonymity/

860 Tennison J., What is the impact of blockchains on privacy?, https://theodi.org/blog/impact-of-blockchains-on-privacy

861 COMMUNICATION FROM THE COMMISSION 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, p. 8

862 Immutability is relative, and relates to how hard something is to change.

863 Russel L., Blockchains: The legal landscape, https://www.blakemorgan.co.uk/training-knowledge/features-and-articles/blockchains-legal-landscape/

The unalterable character of the blockchain, it is impossible to erase data once it has been added. It seems that blockchain and right to be forgotten are not compatible. Inalterability and decentralization mean that the register is made of indelible data and that this register is shared with all user in the network. Applying the right to be forgotten is against the very principle of inalterability, which lies at the core of the blockchain technology.[864]

On the other hand, blockchain technology could also be beneficial for the protection of personal data by encoding permissions, conditions, and restrictions for its use. It could enable data portability and provide an easily auditable trail with proofs of consent.[865]

A blockchain stores a series of transactions, which can be data of any sort, in blocks, which get added to a blockchain one after the other. Blockchains are what is known as an append-only data store.[866] That means you can only add data to the store, you cannot take it away. Blockchains are maintained by a peer network of nodes in which every node has a copy of the blockchain and has equal authority to add to it. Every node publishes that data for other nodes to pick up and use. One of the unique selling points of blockchains is that once data is embedded in the blockchain it cannot be altered without that change being detected and rejected by the other nodes in the network. This is useful for data that people need to trust because it provides a guarantee that the data in the blockchain has not been changed since it was put there.

Greg McMullen[867], gave rather a pessimistic image of the possibility to apply right to be forgotten within blockchain: "*Assuming personal information is encrypted before it is written to a blockchain, destroying the key renders the data unreadable. But is this enough to comply with the right to be forgotten, if the data is technically still there? Regulators should accept the destruction of a key as an erasure for the purposes of the GDPR, so long as the destruction is done in accordance with best practices and in an auditable way*."[868]

However, there are possible ways to make changes in the blockchain, which potentially gives a chance to apply the right to be forgotten.

To clear the data out, over half the nodes would have to work together to rebuild the blockchain from before that data was added. This process is like rebuilding from

---

864 When the right to be forgotten becomes possible on the Ethereum blockchain, https://www.newsbtc.com/press-releases/bcdiploma-right-to-be-forgotten-ethereum-blockchain/

865 Lumb R., Treat D., Jelf O., EDITING THE UNEDITABLE BLOCKCHAIN. Why distributed ledger technology must adapt to an imperfect world, https://www.accenture.com/t00010101T000000__w__/it-it/_acnmedia/PDF-33/Accenture-Editing-Uneditable-Blockchain.pdf, p. 6.

866 What is the impact of blockchains on privacy? https://theodi.org/blog/impact-of-blockchains-on-privacy

867 Founder and Executive Director of IPDB Foundation, https://ipdb.io/

868 McCullen G., Blockchain & Law in 2017: Finally friends or still foes?, https://medium.com/ipdb-blog/blockchain-and-law-in-2017-f535cb0e06c4

a backup: while it was being rebuilt, the blockchain would be rewound to a previous state, days or weeks or even more out of date. During this time, the data would not be up to date. This might also be a time when unwanted changes to data that was trustworthy could get in.

Second idea is that a court could try to compel the entire set of nodes to be shut down. Putting aside that nodes may reside in different legal jurisdictions, that would have huge practical implications. It would mean removing all the rest of the data held in the blockchain as well as the target of the order. Unfortunately, blockchain is usually holding many types of data and is supporting many types of applications. Because of it, there is a real risk that bad data simply must continue to exist to prevent massive disruption to the provision of good data for other applications. Therefore, even if this solution is possible, it might be too risky for the blockchain.[869]

Other solutions include controlling what becomes public within a peer-to-peer network of trusted nodes, therefore, hiding data in the blockchain that should not be shared in the first place.[870]

There is another solution. The issue of right to be forgotten is seemingly resolvable in a permissioned system which would allow the controlling party to use a blockchain editor tool, like the one Accenture[871] has recently made an application to patent.

This solution should offer new room to manoeuvre, not only in financial services but across industries. The invention modifies existing blockchain technology to allow designated authorities to edit, rewrite or remove previous blocks of information without breaking the chain. One of its main features:

- it is compatible with current blockchain designs,
- can be implemented now,
- requires only minimal changes to current application software.

The invention enables blockchain editing by using a new variation of the so-called chameleon hash function, which can recreate matching algorithms using secure private keys. After a change, has been made to a block, the original blockchain remains fully intact and there is no need to rebuild subsequent blocks. That means flawed smart contracts could be updated at the time the contract was issued and the changes would apply to subsequent smart contracts in the chain. Even where edits to one block impact subsequent blocks, the fix would be far easier than a hard fork. The editable blockchain invention provides the means to build a virtual padlock on the link connecting two blocks.

---

869 What is the impact of blockchains on privacy? https://theodi.org/blog/impact-of-blockchains-on-privacy

870 Blockchain technologies and the EU 'right to be forgotten' – an insurmountable tension?, http://www.ibtimes.co.uk/blockchain-technologies-eu-right-be-forgotten-insurmountable-tension-1580166

871 EDITING THE UNEDITABLE BLOCKCHAIN. Why distributed ledger technology must adapt to an imperfect world, https://www.accenture.com/fi-en/insight-editing-uneditable-blockchain

Redacting the blockchain is simple: the chameleon hash key is used to unlock the link between the block that must be changed and its successor. Thanks to the key, it is possible to substitute the block with a new one without breaking the hash chain. The invention is designed to preserve the virtues of immutability as well. The editable blockchain invention is designed for permissioned systems, which have a designated administrator who manages the systems and grants permission to use it.[872]

It seems that this solution allows the application of the right to be forgotten. However, it is important to remember that all immutable unpermissioned systems are very likely to not be compliant. If Accenture's invention is truly effective, it might lead to the situation where under GDPR regime it becomes a standard blockchain.

Finally, there is a blockchain that follows the GDPR, including the right to be forgotten. It is Ethereum[873] and it allows to store diplomas and personal data. To accomplish compliance with the GDPR, the data is encrypted and secured using a set of three keys:

1. Graduate Key – This is the property of the graduate and is integrated into the diploma's URL.
2. Persistent Key – It is kept by the educational establishment. When the graduate wishes to exercise his or her right to be forgotten, he only has to destroy this key.
3. School Permanent Key – This is kept by the educational establishment.

There is an algorithm allowing total security of the diploma's keys. This is not stored and can be generated only by assembling three keys through a derivation process.[874]

Already at this point, we have ready solutions. It seems that "old" blockchains may pose some problems. However, every new database build on blockchain should be designed to comply with GDPR rules. Whether it will be using given examples or there will be some other ways, is a question of the coming future.

From a data protection perspective, blockchain is particularly interesting because it allows theoretically transactions between parties without having to disclose their identity. Anonymity and pseudonymity are also addressed as data protection law instruments. If a transaction cannot be traced back to the individuals, their fundamental right to self-determination is not affected.[875]

---

872 Lumb R., Treat D., Jelf O., EDITING THE UNEDITABLE BLOCKCHAIN. Why distributed ledger technology must adapt to an imperfect world, https://www.accenture.com/t00010101T000000__w__/it-it/_acnmedia/PDF-33/Accenture-Editing-Uneditable-Blockchain.pdf, p. 7.

873 https://www.ethereum.org/

874 The Right to Be Forgotten Becomes Possible on the Blockchain, http://cryptotimes.org/blockchain/right-forgotten-becomes-possible-blockchain/

875 Wilke S., Krings D., Blockchain from a perspective of data protection law. A brief introduction to data protection ramifications, https://www2.deloitte.com/dl/en/pages/legal/articles/blockchain-datenschutzrecht.html

Can blockchain technology be an opportunity for personal data protection? To certain extend, yes. Blockchains are decentralized and distributed. Currently, various trusted third parties process personal data. These entities are centralized and, therefore, often constitute single points of failure. Leaks of unimaginable amounts of data because of cybercrime often occur in the form of an attack on a single entity, such as a hospital, email service provider, etc.[876]

Blockchains are public and transparent. We do not currently have any effective control over who processes our personal data and how. In fact, the data subject is in control of their personal data only to a restricted degree. Upon a transfer of that data, the subject loses control over how it is subsequently used.

Blockchains are very safe. Using cryptography (digital signatures, encryption, timestamping) and systemically embedded economic incentives for network maintaining entities, blockchains provide a secure way of storing and managing information, including personal data.

Where all nodes in a network need to be in sync they all need to have the same version of reality which means they all need the same data. How does this fit in with the current regulatory environment around data privacy and with the new GDPR coming in? I would argue that the GDPR and blockchain advocates point to the same thing – the need to fundamentally change the way in which personal data is managed.

Most significantly, blockchain technology may enable individual control of one's personal data. According to Martin Ruubel, president of Amsterdam-based GuardTime, people will be in control of data, will be able to share it with whoever they want to, and will be paid for it.[877] In the future, the widespread adoption of blockchain technology can remove the need for large companies to maintain data and provide individuals with complete control over their personal data.[878]

Blockchain technology can better address the privacy concerns to which the GDPR and EU regulators are responding. For example, in the paper Decentralizing Privacy: Using Blockchain to Protect Personal Data[879], the authors call into question the current centralized model of protecting personal data through trusted third parties and describe a more secure, unhackable decentralized peer-to-peer personal data management system using a blockchain. The authors' proposed system focuses

876 Czarnecki J., Blockchains and Personal Data Protection Regulations Explained, https://www.coindesk.com/blockchains-personal-data-protection-regulations-explained/

877 The Top 10 Blockchain Takeaways From Europe's Trustech Conference, https://www.forbes.com/sites/laurashin/2016/12/05/the-top-10-blockchain-takeaways-from-europes-trustech-conference/#6bb7a0e97ba6

878 Blockchains Can Assist EU Regulatory Fight for Personal Data Protection, https://www.law111.com/blockchains-can-assist-eu-regulatory-fight-for-personal-data-protection

879 Zyskind G., Nathan O., Pentland A., Decentralizing Privacy: Using Blockchain to Protect Personal Data, http://ieee-security.org/TC/SPW2015/IWPE/5.pdf

on mobile platforms and ensures that individuals own and control their personal data. Individuals decide with whom they share their personal data through delegated permissions.

Another example is Civic[880]. It is a digital platform that uses Bitcoin's public blockchain for identity management.

1. A user signs up to the Civic app, which collects various identifying information for them.
2. All of that is passed through to either a government agency or a third-party identification verification service depending on the country.
3. Once verified, Civic takes a cryptographic hash of all the information, inserts the hash into the public blockchain, and then erases the personal data from their servers.
4. Then when you want to authenticate to use another service, you share whatever information they ask of you and they can send the information through Civic's special sauce algorithm to check it against the hash on the blockchain.

Once authenticated, the service using Civic no longer needs to store your information for identification or authentication purposes.

Finally, it is possible to encrypt data stored within the blockchain. The main problem with this approach is that if the decryption key for encrypted data is ever made public, the encrypted content is readable by anyone with that key; there is no way of encrypting the data with a different key once it is embedded within the blockchain. Also, if the key is ever lost, the data cannot be read. And there is the problem of sharing the key for the data amongst all those who legitimately need to be able to read it.

It must be also mentioned that the anonymity in the blockchain is far from being perfect. It is possible to associate public keys with each other, and with external identifying information. Appropriate tools allow to observe the activity of known users in detail. Additionally, an interested party can potentially deploy marked Bitcoins and collaborate with other users to discover even more information. Large, centralized services such as the exchanges and wallet services can identify and track user activity.[881]

As said at the beginning of this paper, blockchains are not necessarily bad for privacy. It all depends on how they are designed. Anyone experimenting in the area should be thinking through the implications. How the right to be forgotten plays out in the context of blockchain does, of course, remain to be seen. For example, could it be argued that there is a legitimate reason for retaining transaction blocks and precisely how EU regulators and courts would look to police this right considering

880 https://www.civic.com/intel

881 Reid F., Harrigan M., An Analysis of Anonymity in the Bitcoin System, https://arxiv.org/abs/1107.4524, p. 26.

jurisdictional hurdles are just two key questions which spring to mind. In the future, the widespread adoption of blockchain technology can remove the need for large companies to maintain this data and provide individuals with complete control over their personal data. Moreover, laws and regulations could be programmed into the blockchain itself, so that they are enforced automatically.

There is no clear answer to the question whether blockchain technology is a threat or a solution to the data protection. However, a lot depends on the design of the blockchain. The "perfect" one may in some case be a serious threat. Immutable and the same time not perfectly anonymous. Fortunately, it is possible to have blockchain respecting data protection by design. We already have some examples, given in this paper, and I am sure that with the rapidly growing popularity of the blockchain technology new ideas will emerge.

I am also sure that as blockchain technology will become widely adapted new issues reveal itself. Mostly I am concerned about personal data and every detail within blockchain database that may lead to disclosing this personal data.

There is no doubt that blockchain technology is both a challenge for programmers and lawyers, but also a possible chance to protect privacy. Despite being the potential threat to privacy itself.

5.3.5. Potential role of EU Competition Law

Margrethe Vestager was named as competition chief in the new European Commission, retaining the role she has held for the last five years in which she has clashed repeatedly with US tech giants. She is certainly not liked in the White House.[882] U.S. President Donald Trump said: "You have a woman in Europe, I won't mention her name, she's actually considered to take Jean-Claude's place ... she hates the United States perhaps worse than any person I've ever met. What she does to our country. She's suing all our companies."[883] During her time as competition chief, the Danish politician has issued huge fines to American IT giants including Google.[884]

Data protection in its complexity must be balanced against, among other[885], competition law. There are common rules on competition[886], provided by the TFEU, banning agreements, decisions and concerted practices that distort competition[887]

882 Dallison P., Trump: 'Europe treats us worse than China', June 26, 2019, https://www.politico.eu/article/trump-europe-treats-us-worse-than-china/

883 Dallison P., New Danish PM wants Vestager to stay as commissioner, June 26, 2019, https://www.politico.eu/article/new-danish-pm-wants-vestager-to-stay-as-commissioner/

884 Denmark's Vestager reappointed EU competition commissioner, September 11, 2019, https://www.thelocal.dk/20190911/denmarks-vestager-reappointed-eu-competition-commissioner

885 Free movement and the single market, intellectual property, freedom to conduct a business, freedom of expression, right to communicate information, transparency and the freedom of information.

886 TFEU, Tittle VII, Chapter 1.

887 TFEU, Article 101.

and abuses of dominant position[888]. These rules are in danger where data processing systems are concerned, as former EU Competition Commissioner Joaquin Almunia explained:

> The challenge of enforcing EU competition law in digital markets are mostly linked to their rapid evolution and the fact that dominant companies can quickly rise to prominence and become gatekeepers for other market players. This is often the result of innovation and smart business models, which we have to support. Market dominance through internal growth, innovation and success is not a competition problem. However, the abuse of dominant position is indeed a serious competition problem.[889]

Data processors that are in a dominant position are also in a very good position to enter contracts with their customers which provide a legitimate basis for personal data processing.[890] Smaller competitors that lack such contracts may find themselves excluded from certain markets by their inability to comply with data protection law.[891]

Data protection intends to give consumers control over their personal information from a human rights perspective.[892] Intersection between competition law and data privacy has never been extensively analysed by the CJEU. The Court did touch upon this issue in the *Asnef* case.[893] This case was a preliminary ruling by the Spanish Supreme Court concerning whether a system that aimed at the exchange of information between banks, namely personal data, was restrictive of competition under article 81 EC (now 101 TFEU). Without entering into detail, the CJEU held that: "(...) any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law, they may be resolved on the basis of the relevant provisions governing data protection" (emphasis added).[894]

Advocate General Geelhoed pointed in the same direction in his Opinion: "Any problems concerning the sensitivity of personal data can be resolved by other instruments, such as data protection legislation. There must be some way of informing

888 TFEU, Article 102.

889 Joaquin Almunia, Vice President of the European Commission responsible for Competition policy, Presenting the Annual Competition Report, EU Parliament, 23 September 2014.

890 Kelleher D., Murray K., EU Data Protection Law, London 2018, p. 16.

891 Rao J. M., Reiley D. H., The Economics of Spam, Journal of Economic Perspectives, vol. 26 (3), 2012, p. 87-110.

892 Graef I, Beyond Compliance: How Privacy And Competition Can Be Mutually Reinforcing, Computers, Privacy & Data Protection Conference, https://www.youtube.com/watch?v=Af1qLye_-Ok

893 Case C-235/08 Asnef-Equifax v Asociación de Usuarios de Servicios Bancarios [2006] Court of Justice of the European Union, ECR I-11125.

894 Ibid, para. 63.

the borrowers concerned of what data are recorded and of granting them the right to check the data concerning them and to have them corrected where necessary. It appears that this point is settled, regard being had to the relevant Spanish legislation and also to clause 9 of the rules governing the register".[895]

However, this statement of the Court might not be interpreted as a complete exclusion of the privacy assessment in competition law cases, just because personal data concerns are addressed in privacy law. As mentioned by Alec J. Burnside: "(...) It is hardly a blanket assertion that privacy is irrelevant to antitrust, or that antitrust must not address facts to which privacy laws may also be relevant. Rather, it indicates that antitrust rules should be applied in pursuit of antitrust goals. That is what the Court did in the case before it: apply the antitrust rules to a set of facts to which privacy disciplines had a parallel application".[896]

The Bundeskartellamt and the Autorité de la Concurrence (the German and French competition authorities) in their joint paper, 'Competition Law and Data', also acknowledged that despite personal data concerns are covered by data protection rules that does not preclude competition law intervention. For instance, it is mentioned that: "The fact that some specific legal instruments serve to resolve sensitive issues on personal data does not entail that competition law is irrelevant to personal data".[897]

Furthermore, the incorporation of different legal instruments into competition analysis was already addressed by the CJEU's decision in Allianz Hungária. In this case, it was found that if other national law goals were being prevented, that could be considered in order to determine if there was a restriction on competition.[898] In addition, EU general objectives which are established in the TFEU have been considered by the Commission to deal with competition concerns. An illustration of that is the Universal/EMI merger case where cultural diversity concerns were addressed under the justification of article 167/4 TFEU that refers that cultural diversity should be taken into account under other Treaties' provisions. Accordingly, article 16 TFEU establishes data protection right in the provisions of general application of the TFEU: "Everyone has the right to the protection of [their] personal data".

Therefore, the argument that competition law should not look into data protection because that is not within its scope or because there are other set of rules in place, is questionable and it does not seem coherent.

Furthermore, some scholars have argued that competition law should not fulfil the function of enforcing data protection rules, since as data protection develops,

895 Ibid, para 56.

896 Burnside A., No Such Thing As A Free Search: Antitrust And The Pursuit Of Privacy Goals, https://www.competitionpolicyinternational.com/assets/Uploads/BurnsideCPI-May-15.pdf

897 Autorité de la Concurrence and Bundeskartellamt, 'Competition Law and Data', p.23, [n4] supra.

898 Case C-32/11 Allianz Hungária [2013] Court of Justice of the European Union, ECLI:EU:C:2013:160, para. 46-47.

individual's rights are better accounted for as well.[899] However, as explained later, data protection is a competence of national authorities, which are limited to their territorial jurisdiction and are the ones that choose which cases to pursue. Even considering that the EU initiates a coordinated action, similar to the one existent in consumer protection, for instance the EU sweeps[900], in order to assess the online marketspace compliance with the new rules, the national authorities would always have the final decision. Consequently, and despite the GDRP, the applicability of data protection will not be fully harmonized. When this is the case, antitrust has intervened before, data protection would not be an exception. For instance, in tax law[901] antitrust has interfered through state aid. It happened, similarly, with the liberalization of the energy and the telecommunication market.[902]

The President of Bundeskartellamt, Andreas Mundt, also defends that competition law can, perhaps, address privacy concerns in a more efficient way considering the fast pace at which these markets evolve:

"Maybe competition law is also a chance to prevent all this kind of regulation [data protection regulations]. (...) Competition law can do a good job here because competition law is so lively. Here competition law is maybe faster, is maybe more adaptive. (...) I'm not going to say that competition law can cure everything there is, but I think we can cure some things."[903]

Data protection and competition law in the USA - The discussion concerning the intersection between competition law and privacy law mainly started in 2007, after the announcement of the acquisition of the internet advertising server, DoubleClick by Google for USD 3.1 billion. The FTC decided to approve the merger without

899 Kennedy, The Myth of Data Monopoly: Why Antitrust Concerns About Data Are Overblown, http://www2.itif.org/2017-data-competition.pdf

900 "The "EU sweep" is an EU-wide screening of websites. It is conducted in a form of simultaneous, coordinated checks to identify breaches of consumer law and to subsequently ensure its enforcement. Following such investigation, the relevant national authorities take proper enforcement actions: they contact companies about suspected irregularities and ask them to take corrective action or face legal action" 'Sweeps - Coordinated Control Actions - European Commission' (Ec.europa.eu, 2017), http://ec.europa.eu/consumers/enforcement/sweeps/index_en.htm

901 European Commission, 'State Aid: Commission Extends Information Enquiry On Tax Rulings Practice To All Member States' (2014), http://europa.eu/rapid/press-release_IP-14-2742_nl.htm. There were also multiple investigations: Apple in Ireland (European Commission, 'State Aid: Ireland Gave Illegal Tax Benefits To Apple Worth Up To €13 Billion' (2016), http://europa.eu/rapid/press-release_IP-16-2923_en.htm Starbucks case in the Netherlands and Fiat in Luxembourg (European Commission, 'European Commission, 'Commission decides selective tax advantages for Fiat in Luxembourg and Starbucks in the Netherlands are illegal under EU state aid rules' (2015), http://europa.eu/rapid/press-release_IP-15-5880_en.htm

902 Burnside A., No Such Thing as a Free Search: Antitrust and the Pursuit of Privacy Goals, May 29, 2015, https://www.competitionpolicyinternational.com/no-such-thing-as-a-free-search-antitrust-and-the-pursuit-of-privacy-goals/

903 Lipman M., Facebook Data Antitrust Case Not Overreach, https://www.law360.com/articles/888145/facebook-data-antitrust-case-not-overreach-enforcer-says

conditions. The cases discussed hereafter are not the only investigations where privacy concerns have been raised, by third parties, but are the ones where privacy was directly referred to by the FTC.

There are some examples, based on Google and Facebook, how there is a relation between competition and data protection laws.

Example 1 – The Google/DoubleClick merger – The case concerned the merger of Google's online advertising and advertisement intermediation service and DoubleClick's advertising serving technology, which could be used in conjugation with other companies' intermediation services. The FTC addressed three theories of harm. The first one concerned the direct elimination of competition, however it was found that Google and DoubleClick were not direct competitors in any relevant market, since DoubleClick was not present neither in the online advertising nor advertisement intermediation market.

Afterwards, it was analysed the elimination of potential competition due to Google's effort to enter third party ad servicing markets. It was found that there is intense competition in this market and even if Google was successful in entering it, it would not have a considerable impact on competition and, thus, the merger did not raise any concerns relating to the elimination of potential competition.

Lastly, FTC scrutinized whether the merger would permit Google to exploit DoubleClick's position in the advertisement serving markets to gain an advantage in the advertisement intermediation market, where Google was present through AdSense. The conclusion reached was that there was no evidence that DoubleClick had market share in the advertisement servicing market and therefore Google could hardly harm competition in the related advertisement intermediation market. It was also mentioned that the gathering of data of Google and DoubleClick would not likely damage competition in the ad intermediation market.[904]

Despite the approval of the merger, the decision was not unanimous. The, at the time, FTC Commissioner Pamela Jones Harbour issued a dissenting statement and called for an analysis of privacy in the merger: "Privacy concerns represent the "other side of the coin" of the exact same merger of datasets. The combination of Google and DoubleClick undeniably raises numerous privacy questions – and these questions, too, beg answers."[905]

She also added that it should not suffice the non-binding statements of both parties ensuring their willingness to protect consumers' privacy. Furthermore, she held that the traditional competition analysis did not capture the interests of all parties affected

904 Federal Trade Commission, 'Statement Of Federal Trade Commission Concerning Google/Doubleclick FTC File No. 071-0170' (2007), https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf

905 Harbour, 'Dissenting Statement Google/Doubleclick', p.9

by the merger. For instance, the web-based publishers and advertisers will be benefitted since it is likely that highly targeted advertisement will create efficiencies capable of cancelling any harm that might exist to competition. Nevertheless, the interests of the consumers whose data will be shared and analysed were not considered, considering that the consumers do not have a business relation with Google nor DoubleClick.[906] "I do not doubt that this merger has the potential to create some efficiencies, especially from the perspective of advertisers and publishers. But it has greater potential to harm competition, and it also threatens privacy. By closing its investigation without imposing any conditions or other safeguards, the Commission is asking consumers to bear too much of the risk of both types of harm."[907]

The Electronic Privacy Information Center ('EPIC')[908] also requested the FTC to analyse privacy in its competition analysis, arguing that the right to privacy is a fundamental right in the United States. It argued that the merger would allow Google to track simultaneously internet searches and website visits. It also added that if the merger was approved, Google would not have almost any obligations to protect the privacy of its users.[909]

Microsoft also presented its views of the case to the FTC. Regarding privacy concerns, it mentioned that allowing the merger would provide only one company with the "largest database of user information in the world". Furthermore, Microsoft drew a parallel between privacy rules in the telecommunication and computer industry: "This country doesn't permit the phone company to listen to what you say and use that information to target ads. The computer industry doesn't permit a software company to record everything we type and use that information to target ads. Yet with this merger, Google seeks to record nearly everything you see and do on the Internet and use that information to target ads."

It was also added that these privacy concerns have, in fact, effects in antitrust. The consumers' data available to Google after the merger will prevent other companies from providing ads in the same lucrative way and, therefore, will not be able to compete. Additionally, he also referred that according to the Sherman Act it is not possible to gain a dominant position in a particular market by purchasing its largest competitor.[910]

---

906 Ibid, p. 10.

907 Ibid, p. 12

908 EPIC is a public interest research center in Washington, D.C. "EPIC routinely files amicus briefs in federal courts, pursues open government cases, defends consumer privacy, organizes conferences for NGOs, and speaks before Congress and judicial organizations about emerging privacy and civil liberties issues" see 'EPIC - About EPIC' (Epic.org, 2017), https://www.epic.org/epic/about.html

909 The Electronic Privacy Information Center, 'Complaint And Request For Injunction, Request For Investigation And For Other Relief' (Federal Trade Commission 2007), para. 7, 27 and 54, https://epic.org/privacy/ftc/google/epic_complaint.pdf

910 Smith B., Brad Smith: Before The Senate Subcommittee On Antitrust, Competition Policy And Consumer Rights, https://news.microsoft.com/2007/09/27/brad-smith-before-the-senate-subcommittee-on-antitrust-competition-policy-and-consumer-rights/#zVhQg6ZZ2QzGQqpC.97

The FTC, in its decision, responded to Microsoft's concerns and disregarded its claims regarding privacy by stating that the real concern was, in fact, that Google would have access to a significantly large database, not available for its competitors. It mentioned that those concerns were not valid since Google does not have access to its competitors' database in the advertisement intermediation market neither, which also comprise unique information. Thus, companies like Microsoft through 'Yahoo!' would still be in a position of actively compete with Google, after the merger.[911]

Peter Swire, who was, at the time, a Professor in Moritz College of Law at the Ohio State University also submitted a testimony to the FTC concerning this case. He argued for the incorporation of privacy concerns in antitrust analysis through the assessment of product quality.[912] This is the theory defended in this thesis and therefore this matter will be discussed in detail in the next chapter.

In its decision, the FTC does seem to leave the door open to the incorporation of privacy in non-price aspects of competition analysis, in the future: "Although such issues may present important policy questions for the Nation, the sole purpose of federal antitrust review of mergers and acquisitions is to identify and remedy transactions that harm competition. Not only does the Commission lack legal authority to require conditions to this merger that do not relate to antitrust, regulating the privacy requirements of just one company could itself pose a serious detriment to competition in this vast and rapidly evolving industry. That said, we investigated the possibility that this transaction could adversely affect non-price attributes of competition, such as consumer privacy. We have concluded that the evidence does not support a conclusion that it would do so. We have therefore concluded that privacy considerations, as such, do not provide a basis to challenge this transaction."[913]

Example 2 – The Facebook/WhatsApp merger – In the merger between Facebook/WhatsApp there was not a formal investigation. The FTC acted within its consumer protection competence[914] and merely reminded WhatsApp that despite the acquisition, it was obliged to maintain its privacy practices. The Bureau Director, Jessica Rich sent a letter[915], to both companies, in which she stressed that

911 FTC, 'Statement (...) Google/Doubleclick', p. 12

912 Swire P., Submitted Testimony To The Federal Trade Commission Behavioral Advertising Town Hall, http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/testimony_peterswire_/Testimony_peterswire_en.pdf

913 Federal Trade Commission, 'Statement (...) concerning Google/Doubleclick', p. 2-3

914 The FTC is not only the US Competition Law Authority but it also comprises consumer protection competences. 'Bureaus & Offices | Federal Trade Commission' (Ftc.gov, 2017), https://www.ftc.gov/about-ftc/bureaus-offices

915 Reich J., Federal Trade Commission, Reminding Both Firms That Whatsapp Must Continue To Honor Its Promises To Consumers With Respect To The Limited Nature Of The Data It Collects, Maintains, And Shares With Third Parties, https://www.ftc.gov/public-statements/2014/04/letter-jessica-l-rich-director-federal-trade-commission-bureau-consumer

if privacy promises are not kept, Facebook will be in breach of Section 5 of the FTC Act, unfair or deceptive acts or practices.[916] Following the merger announcement, Facebook and WhatsApp referred several times that nothing would change in the WhatsApp's privacy policy, which distinguishes itself from neither having advertisement nor selling its users' data for advertisements purposes.[917] In addition, the Bureau Director also pointed that before there was any changing in WhatsApp's privacy policy there would have to be express consent from the consumers and there could not be any misinformation regarding how the data is kept and used. In the letter, it is also advised that in the event of a change of the privacy policy, users should have the possibility of 'opt-out'.[918]

In 2016, there was an alteration of WhatsApp privacy policy which included the share of data with all the Facebook companies. The data transferred included the phone number and the last time users accessed the app which would be used by Facebook to supply "friend suggestions and more relevant ads on Facebook".[919]

WhatsApp did, effectively, allowed its users to 'opt-out' of the data sharing with Facebook by unmarking a box when the privacy policy was altered. After that initial opportunity, the users still had thirty days to 'opt-out' afterwards, however in order to do so, the user needed to go to a different screen within the app and uncheck the box 'share my account details'. Nonetheless, even if the users did this, WhatsApp would still be able to share data with the Facebook family of companies for the purposes of improving infrastructures and systems, fighting spam, etc.[920]

Once again, EPIC issued a complaint before the FTC regarding this merger stating that the alterations of WhatsApp's privacy policy constituted a violation of

916 Facebook has already settled charges that it deceived consumers in 2011 when it failed to keep its privacy promises. With this settlement Facebook became obliged to require user consent for changes in its privacy policy. Federal Trade Commission, Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises, http://facebook-settles-ftc-charges-it-deceived-consumers-failing-keep

917 Guynn J, Mark Zuckerberg: Whatsapp Worth Even More Than $19 Billion, http://articles.latimes.com/2014/feb/24/business/la-fi-tn-mark-zuckerberg-whatsapp-worth-even-more-than-19-billion-20140224

918 Letter From Jessica L. Rich, Director of the Federal Trade Commission Bureau of Consumer Protection, to Erin Egan, Chief Privacy Officer, Facebook, and to Anne Hoge, General Counsel, WhatsApp Inc., Reminding Both Firms That WhatsApp Must Continue To Honor Its Promises To Consumers With Respect to the Limited Nature of the Data It Collects, Maintains, and Shares With Third Parties, April 10, 2014, https://www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappltr.pdf

919 WhatsApp FAQ, I Have Questions About the Updated Terms of Service and Privacy Policy, https://faq.whatsapp.com/general/28030012

920 WhatsApp Security and Privacy, How do I choose not to share my account information with Facebook to improve my Facebook ads and products experience?, https://faq.whatsapp.com/en/general/26000016

Section 5 of the FTC Act, given previous promises by both companies and the lack of express consent from its users at the time of the privacy policy change.[921]

There were other mergers that raised privacy concerns as well which the FTC did not assess. In the 'Assessment of the FTC's Prior Actions on Merger Review and Consumer Privacy',[922] EPIC points out several mergers[923] that represent missed opportunities for the FTC to incorporate privacy concerns in its merger's review.[924] It concludes by stating that the avoidance of analysing non-price factors has permitted companies to dominate data markets and that:

"The FTC should investigate proposed mergers of data aggregators with regard to the companies' ability to dominate the search market and pose unchallenged privacy threats to consumers. Following mergers of data aggregators, the FTC should conduct post-merger reviews to assess whether the companies have honored their commitments, whether formal or informal, to protect the privacy of the users of their services from whom they have obtained detailed, personal information."[925]

To conclude, even if it seems that FTC had left the door open to the incorporation of privacy in non-price factors in antitrust analysis in Google/DoubleClick, the lack of analysis in subsequent decisions[926] casts doubt on whether this is an actual policy objective.

---

921 The Electronic Privacy Information Center and The Center for Digital Democracy, 'Complaint, Request For Investigation, Injunction, And Other Relief' (2016), https://www.democraticmedia.org/sites/default/files/field/public/2016/epic-cdd-ftc-whatsapp-complaint-2016.pdf

922 The Electronic Privacy Information Center, 'Assessment Of The FTC'S Prior Actions On Merger Review And Consumer Privacy' (2015), https://epic.org/privacy/internet/ftc/Merger-Remedy-3-17.pdf

923 It refers to merger cases before the Google/DoubleClick merger in 2007 such as the merger between DoubleClick and Abacus in 1999 and Time Warner and AOL in 2000. After 2007, it mentions the lack of antitrust analysis to the Facebook/WhatsApp merger. Ibid, p.3-21. It also mentions that EPIC alerted the FTC for several other practices that might raise antitrust concerns, for example, it argued that Google's manipulation f YouTube search rankings might constitutes an abuse of dominance position. 'Comments Of The Electronic Privacy Information Center To The Federal Trade Commission In The Matter Of Google, Inc. "FTC File No. File No. 121 0120"' (Federal Trade Commission 2013), https://epic.org/apa/comments/EPIC-FTC-Google-Antitrust-Comments.pdf

924 "Over the last 15 years, there has been growing recognition among consumer privacy organizations and competition experts that data aggregation practices play a significant role in antitrust analysis. (...) it was clear that the practical consequence of the merger [Facebook/WhatsApp] would be to reduce the privacy protections for consumers and expose individuals to enhanced tracking and profiling. The failure of the Federal Trade Commission to take this into account during merger review is one of the main reasons consumer privacy in the United States has diminished significantly over the last 15 years." Ibid, p. 1-2.

925 Ibid, p. 24-25.

926 Unlike the EU the FTC did not consider the merger between Microsoft and LinkedIn despite the expressed concerns of Microsoft's competitor, Salesforce. April Glaser, 'Marc Benioff Says Companies Buy Each Other for the Data, And The Government Isn't Doing Anything About It' Recode (2016), https://www.recode.net/2016/11/15/13631938/benioff-salesforce-data-government-federal-trade-commission-ftc-linkedin-microsoft

In the EU, the approach is quite similar to the US. Thus far, competition law has not been used in any case before the Court of Justice involving companies that hold large databases of consumers' information. The only occasion in which the CJEU made a few comments about the use of competition law to address privacy was in the Asnef case, as mentioned previously. Subsequently, only the Commission has had the opportunity to discuss this controversy.

Example 3 – The Google/DoubleClick merger – As in the US, the Google/DoubleClick merger was also scrutinised by the Commission in 2008. It used the same line of argumentation as the FTC and cleared the merger. Likewise, it found that Google and DoubleClick were not neither direct nor potential competitors and even if DoubleClick entered the advertisement intermediation market, there would be still enough competitors in the market. Regarding the company's non-horizontal relation, it was found that Google would not have the ability to restrict competition in the advertisement serving market since there were other significant competitors such as Microsoft's 'Yahoo!' and AOL. Nonetheless, the potential effects that the integration of both companies' databases would have in their users' privacy were not considered. The Commission mentioned, as a way to justify that lack of analysis, that: "The Commission's decision to clear the proposed merger is based exclusively on its appraisal under the EU Merger Regulation. It is without prejudice to the merged entity's obligations under EU legislation in relation to the protection of individuals and the protection of privacy with regard to the processing of personal data and the Member States' implementing legislation."[927]

Example 4 – The Facebook/WhatsApp merger – In 2014, Facebook disclosed that it was going to acquire WhatsApp for a purchase price of USD 19 billion. The case was also analysed by the Commission which approved the merger without conditions.

The Commission identified three relevant markets: consumer communications services, social networking services and online advertising services.[928]

In the first market, it was acknowledged that privacy was a differentiating factor regarding consumers' choice in the communication market.[929] In respect to this market, the Commission concluded that, despite the fact that both companies operate on it (Facebook through Facebook Messenger), they were not close competitors.[930]

927 European Commission, 'Mergers: Commission Clears Proposed Acquisition Of DoubleClick By Google' (2008), http://europa.eu/rapid/press-release_IP-08-426_en.htm

928 European Commission, 'Mergers: Commission Approves Acquisition Of Whatsapp By Facebook' (2014), http://europa.eu/rapid/press-release_IP-14-1088_en.htm

929 Case No COMP/M7217 - Facebook/ Whatsapp [2014] European Commission Decision, para.87.

930 WhatsApp and Facebook. Facebook/WhatsApp merger case, para. 107

This conclusion was reached despite both companies high market shares.[931] The Commission's arguments were that the apps operate differently since WhatsApp uses the consumers' mobile phone number, while to use Facebook Messenger the user is required to own a Facebook account. Facebook argued that this difference would limit its ability of tying users account in both platforms because it still lacked the technical capacity to do so. The Commission considered that even if that was possible in the future, it would not represent any restraint to competition since there were other significant competitors in the market with different apps offering similar characteristics. There were also other relevant factors for the Commission's conclusion such as consumer's tendency to multi-home[932] and the fact that the network effects that exist are mitigated by a fast-changing market where the barriers to entry are low, which allow competitors to enter the market and expand rapidly.[933]

In the online advertising services market, the Commission referred again to privacy. This time, it established that:

"Any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules."[934]

Therefore, no privacy concerns were accounted for. The Commission established that WhatsApp was not present in the market and it would be necessary a change in its privacy policy in order to enter. This was unlikely, given the "no ads" strategy that WhatsApp had been pursuing.[935] Notwithstanding, it was found that Facebook had a market share of 20-30% in the online advertising market and so it was necessary to assess whether Facebook's position would be strengthened by the merger. The Commission considered two theories of harm: Facebook introducing advertisement in WhatsApp (as it did after acquiring Instagram) or the use of WhatsApp data for targeting advertisements on Facebook. The conclusion reached was that there would be no harm for competition in both case scenarios, mainly because there would still be plenty of providers of targeted advertisement competing with Facebook, as well as a substantial supply of user's data available for advertising purposes under Facebook's absolute control.[936]

The Commission refused, once more, to draw any antitrust consequences from either the exchange of users' information for better advertising targeting or from what that would have represented for their privacy. Despite the initial recognition of privacy as a factor that consumers value in a product, the Commission failed to

931 Ibid, para. 96.
932 Ibid, para. 105.
933 Ibid, para 127-140.
934 Ibid, para. 164.
935 Ibid, para. 173-14.
936 Ibid, para. 174-190.

take it into account in its analysis. It disregarded the ability of Facebook to connect both accounts which actually occurred later, in 2016, when WhatsApp's privacy policy was changed, as explained previously in sub-chapter 4.2.2. The Commission recently announced it would fine Facebook € 110 million for providing misleading information in respect to this, since at the time of the merger, Facebook already had the technical tools to match Facebook and WhatsApp users' accounts.[937] Nonetheless, the Commission clarified that this fine has no impact on the merger authorisation of 2014. It appears that, despite the Commission's recognition that privacy is a non-price factor in competition, its actual influence on the decision was almost irrelevant. WhatsApp had, at the time of the merger, 600 million users[938] to which data Facebook gathered access to, at least to some extent.

Example 5 – The Microsoft/Linked-in merger – In 2016, Microsoft announced that it would acquire LinkedIn for USD 26 billion. The Commission assessed the merger and approved it following a similar reasoning as in Google/DoubleClick, however subject to conditions. The Commission stated expressly that privacy, as a factor considered in consumers' choice, was relevant for competition:

"The results of the market investigation have indeed revealed that privacy is an important parameter of competition and driver of customer choice in the market for PSN [professional social network] services."[939]

It also recognized that companies could compete on the privacy offered to their users,[940] however it did not go further. Thereby, it seems that privacy would only be endangered, if LinkedIn was the only professional social network ('PSN') service provider. However, the Commission had rejected this possibility previously.[941]

Despite considering the importance of competition in the market in order to maintain a certain level of quality and consumer choice, the Commission did not discuss whether the markets analysed[942] was competitive enough to prevent

937 European Commission, 'Mergers: Commission Fines Facebook €110 Million For Providing Misleading Information About Whatsapp Takeover' (2017), http://europa.eu/rapid/press-release_IP-17-1369_en.htm

938 Facebook/WhatsApp merger case, para. 84

939 Case M8124 – Microsoft / LinkedIn [2016] European Commission Decision

940 Ibid, para. 350.

941 The Commission mentioned in paragraph 348 that: "Should the market for PSN services reach such "tipping point", LinkedIn's platform would remain the only PSN service provider in the EEA today and potentially in the coming years. The possible detrimental effect on consumers would be twofold." Later, in paragraph 350, it refers to the impossibility of competing in privacy as one of the consequences of PSN becoming the only provider. Ibid.

942 In this merger case, the Commission considered three different relevant markets: professional social network (PSN) services; customer relationship management software solutions and online advertising services. European Commission, Mergers: Commission Approves Acquisition Of Linkedin By Microsoft, Subject To Conditions, http://press-release_IP-16-4284_en.htm

privacy degradation.[943] Even if this had been analysed, competition would not guarantee by itself that there is not a deterioration of products' quality. Once more, the Commission failed to address the use of data post-merger, namely in the online advertising market, placing exclusively the protection of consumers on data protection rules.

5.3.6. The Digital Services Act package

On 15 December 2020, the European Commission published its Digital Services Act package which proposes two pieces of legislation: the Digital Services Act (DSA)[944] and the Digital Markets Act (DMA)[945]. This package will profoundly change the way companies offer and use digital services in the EU. It affects not just large online platforms but impacts the majority of digital service providers and their business users and customers.

The Digital Services Act will change the rules for handling of illegal or potentially harmful content online, the liability of online providers for third party content, vetting obligations of third-party suppliers and the protection of users' fundamental rights online. This makes the Digital Services Act relevant not only for all digital service providers (social media, online marketplaces, online platforms, etc.) in the EU but also for their business users and customers.

The main provisions of the DSA include:

- Modernised liability regime for online intermediaries. The key principles from the e-Commerce Directive remain generally unchanged, but the DSA adds obligations to address notifications of content considered as illegal. The DSA requires every hosting provider or online platform to put in place user-friendly notice and takedown mechanisms that allow the notification of illegal content. Online platforms will need to establish internal complaint-handling systems, engage with out-of-court dispute settlement bodies to resolve disputes with their users, give priority to notifications of entities that have been qualified as so-called trusted flaggers by the authorities and suspend repeat infringers.
- New and far-reaching transparency obligations for online platforms relating to the measures taken to combat illegal information. If content is removed, an

943 Colangelo G., Maggiolino M., Data Protection In Attention Markets: Protecting Privacy Through Competition?, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2945085

944 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive, 2000/31/EC, Brussels, 15.12.2020, COM(2020) 825 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en

945 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act), Brussels, 15.12.2020, COM(2020) 842 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842&from=en

explanation needs to be provided to the person who uploaded that content. Online platforms must also publish detailed reports on their activities relating to the removal and the disabling of illegal content or content contrary to their terms and conditions.

- Obligation on online intermediaries to include in their terms and conditions information on any restrictions on the use of data provided by the users, with reference to the content moderation mechanisms applied, algorithmic decision-making and human review. This information must be in clear and unambiguous language and publicly available in an easily accessible format.
- Strict requirements for online platforms that allow consumers to conduct distance contracts with traders, to ensure that traders can only offer goods and services via their platforms after strict Know Your Customer procedures. Platforms must keep information about the traders to help track down sellers of illegal goods or services. A platform's interface should facilitate compliance with traders' obligations to inform consumers and provide appropriate product safety information.
- Transparency obligations concerning online advertisements. For each advertisement and to each user, the online platforms must provide, in real time, clear and unambiguous information to users that (i) they are seeing an advertisement, (ii) on whose behalf the ad is displayed, and (iii) provide meaningful information about the main parameters used to determine why a specific user is targeted by this ad.
- Steep fines for non-compliance of up to 6% of the annual income or turnover of the provider of intermediary services and periodic penalty payments for continuous infringements of up to 5% of the average daily turnover of the intermediary in the preceding financial year per day.
- Online intermediaries without establishment in the EU that provide services in the EU must designate a legal representative in the EU who will be required to cooperate with supervisory authorities, the European Commission and the European Board for Digital Services (a new pan-European group of coordinators that will assist with the harmonisation of the DSA) and can be held liable for non-compliance with the DSA.

In addition to the rules set out above, very large platforms must also comply with the rules set out below. Very large online platforms are those platforms which have more than 45 million active monthly users in the EU, and they will have to:

- Analyse any systemic risk stemming from the use of their platforms and put in place effective content moderation mechanisms to address the identified risks (eg illegal content, privacy violations, etc).
- Provide transparency on the main parameters of the decision-making algorithms used to offer content on their platforms (the rankings mechanism) and the options for the user to modify those parameters. They must provide an option

that is not based on profiling. These obligations are clearly inspired by similar obligations in the P2B Regulation and the Omnibus Directive 2019/2161.

- Establish and maintain a public repository, available via application programming interfaces, with detailed information on the online advertisements they served on their platforms in the past year.
- An obligation to designate a dedicated compliance officer responsible for the compliance with obligations under the DSA and undergo an annual independent audit.
- Upon request of the competent authority, very large online platforms must also give access to the data necessary to monitor their compliance with the DSA to the competent authority but also to vetted academic researchers that perform research into the systemic risks.
- In addition, the European Commission will have supervisory and enforcement powers in relation to very large platforms.

The Digital Markets Act regulates the behaviour of core platform services acting as gatekeepers. Gatekeepers are those platforms that serve as an important gateway between business users and their customers and enjoy a significant and durable market position. The Digital Markets Act imposes several prohibitions and obligations on gatekeepers, such as the prohibition to discriminate in favour of own services and obligations to share data that is generated by business users and their customers in their use of the platform.

The DMA will apply only to providers of 'core platforms services': large, online platforms, such as search engines, social networking services, certain messaging services, operating systems and online intermediation services. The European Commission will designate a provider of core platform services as a gatekeeper if the platform provider meets the following cumulative criteria:

1. It has a significant impact on the internal market and is active in multiple EU countries. The DMA indicates that companies with an annual turnover in EEA exceeding EUR 6.5 billion in the last three financial years or having an average market capitalisation of EUR 65 billion or higher and providing a core platform service in at least three Member States are presumed to meet this criterion.
2. It has a strong intermediation position, meaning that it links a large user base to a large number of businesses. A company is presumed to meet this criterion if it operates a core platform service with more than 45 million monthly active end users in the EU and more than 10 000 yearly active business users established in the EU in the last financial year.
3. It has (or is about to have) a stable and durable market position. Companies that have met the other two criteria in each of the last three financial years will be presumed to comply with this criterion.

The notion of 'gatekeeper' under the DMA is different from what the DSA names as 'very large online platforms'. For instance, a platform with more than 45 million monthly active end users established or located in the EU will be considered a very large online platform under the DSA, but it will need to meet all three criteria mentioned above to be designated as the gatekeeper under the DMA.

Providers of core platform services meeting these three criteria must notify the European Commission, who will then decide whether that provider must be designated as a gatekeeper. Based on a market investigation, the European Commission can also designate platforms as gatekeepers even if the above-mentioned presumptions do not apply.

Gatekeeper platforms carry additional responsibilities to facilitate an open online environment that is fair for businesses and consumers. The DMA will attribute new powers to the European Commission to enforce non-compliance, including fines, periodic penalty payments and the power to impose additional tailored remedies on the gatekeepers.

The main points of the Digital Markets Act include:

- Gatekeeper platforms will have to comply with a defined set of prohibitions and obligations to avoid certain unfair practices. These include inter alia: prohibitions to discriminate in favour of own services, obligations to ensure interoperability with its platform, and obligations to share data that is provided or generated by business users and their customers in their use of the platform.
- Gatekeeper platforms must allow their business users to promote their offer and conclude contracts with their customers outside the platform. Gatekeeper platforms may no longer prevent consumers from linking up to businesses outside their platforms.
- The European Commission may conduct market investigations into new services and practices, to update the list of core platform services and to identify new practices that are unfair or may limit the contestability of core platform services. To this end, the European Commission will enjoy a broad array of investigative powers, among which the power to request information, to carry out interviews, and to conduct on-site inspections.
- The European Commission may impose fines of up to 10% of the company's worldwide annual turnover and periodic penalty payments of up to 5% of the company's worldwide annual turnover. In case of systematic infringements, the European Commission can impose additional remedies, including behavioural remedies and, when behavioural remedies do not suffice, structural remedies, e.g., the divestiture of (parts of) a business.

6. SUMMARY AND CONCLUSIONS

6.1. Introduction

We're living through the most profound transformation in our information environment since Johannes Gutenberg's invention of printing in circa 1439. And the problem with living through a revolution is that it's impossible to take the long view of what's happening.[946]

Social Media has furthered changes in our everyday life since the early rumours. The cyber world exploded in the late 1990's with Microsoft's creation of Internet Explorer, a browser and a search engine that allowed Windows computer users to access any existing website, by using a website address.[947] The Internet in the 1990's was primarily used for web browsing and Internet Service Provider e-mail services. Nowadays, the Internet world has been taken by social media. Social media was created by the Internet, which allows people to exchange personal information with one another and designed to be disseminated through social interaction, using highly accessible and scalable publishing techniques.[948]

The human experience is being claimed as free raw material for translation into behavioural data. Although some of these data are applied to service improvement, the rest are declared as a proprietary behavioural surplus, fed into advanced manufacturing processes known as machine intelligence, and fabricated into prediction products that anticipate what you will do now, soon, and later. Finally, these prediction products are traded in a new kind of marketplace that I call behavioural futures markets. Surveillance capitalists have grown immensely wealthy from these trading operations, for many companies are willing to lay bets on our future behaviour.

946 Naughton J., 'The goal is to automate us': welcome to the age of surveillance capitalism, January 20, 2019, https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook

947 Howe W., An anecdotal history of the people and communities that brought about the Internet and the Web, A Brief History of the Internet (Sept. 13, 2012), http://walthowe.com/navnet/history.html.

948 Bodnar K., The Ultimate Glossary: 120 Social Media Marketing Terms Explained, HUBSPOT (Dec 30, 2011) http://blog.hubspot.com/blog/tabid/6307/bid/6126/The-Ultimate-Glossary-120-Social-Media-MarketingTerms-Explained.aspx.

It is certain that personal data has turned into an indispensable new raw material in the Information Age, as multiple business models rely heavily on data.[949] It is nowadays apparent that data and data flows across borders are essential to a modern and future-oriented economy and thus, questions of data governance feature prominently on the policy agendas of many countries, including the EU.[950]

6.2. Summary of main findings

I argue that society today has become totally dependent on technology. It is needed for work (ex. Driver's license databases), to live (ex. Health care databases), and for pleasure (ex. Facebook). Large multinational companies are pinning down consumers' preferences, lifestyle choices and general web behaviour.[951] No matter if we share the information freely or as a legal requirement, we give little thought to it. Very often, we do not see any issues in sharing the most personal details about us, including phone number, home address, etc. on the Internet. Social media pages have tools to encourage us to behave recklessly, for example by giving us more personalization, which leads to emotional attachment to our Internet profiles and consequently to share even more.[952] Companies are collecting data about billions of consumers from various sources, largely without consumers' knowledge.[953] Data collected by observing our lives became extremely valuable to governmental agencies and to private companies.[954] Data is simply a currency in itself, and a source used to analyse and understand selected markets. One way or another, it is not a resource that can or will be easily given up.[955]

In the last 15 years, billions of dollars in venture capital have been poured into funding business models based on the unscrupulous mass exploitation of data, without considering any ethical, societal, cultural, and political implications. Moreover, the

949 Kong L., Data Protection and Transborder Data Flow in the European and Global Context, The European Journal of International Law 21, no. 2,2010, p. 441

950 Burri M., Schär R., The Reform of the EU Data Protection Framework: Outlining Key Changes and AssessingTheir Fitness for a Data-Driven Economy, Journal of Information Policy, vol. 6, 2016, https://www.academia.edu/34683558/The_Reform_of_the_EU_Data_Protection_Framework_Outlining_Key_Changes_and_Assessing_Their_Fitness_for_a_Data-Driven_Economy_Author_s?email_work_card=view-paper, p. 498-499

951 Rowland D., Kohl U., Charlesworth A., Information Technology Law, Fourth Edition, Routledge 2002, p. 4.

952 Barnes S. B., A privacy paradox: Social networking in the United States, First Monday, Volume 11, Number 9 – September 2006, http://firstmonday.org/article/view/1394/1312

953 Christl W., Spiekerman S., Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy, Vienna 2016, p. 121

954 Webster F., Theories of the Information Society, 4th Edition, Routledge 2014, p. 299.

955 Goold B., How Much Surveillance is Too Much? Some Thoughts on Surveillance, Democracy, and Political Value of Privacy, [in:] Schartum D. W. (ed.), Overvåking in en Rettsstat, 2010, p. 45-46.

shortfall of privacy regulation in the US and the absence of its enforcement in Europe has actively impeded the emergence of other kinds of digital innovation - practices, technologies, and business models that preserve autonomy, democracy, social justice, and human dignity. Tech giants and industry groups engage in massive lobbying aiming to actively shape public policy to advance their position.[956]

Key privacy issues - with regards to the corporate collection and utilization of personal data the most urgent issues to be addressed include:

1. the ubiquitous personal data sharing of website, apps, services, and devices with third parties such as data brokers, advertising technology companies, and analytics firms;[957]
2. the availability of third-party data for companies in diverse industries and its use for automated differential treatment of consumers at the individual level;[958]
3. any invasive and de-contextualized use of personal information about everyday life behaviours for judgement, risk assessment or risk-based pricing in essential areas of life such as finance, insurance, education, employment, welfare, or law enforcement;[959]
4. any use of data collected for identity verification, risk assessment, credit rating, fraud detection, and network security for different purposes, e.g. marketing and sales;[960]
5. the use or disclosure of transactional data in telecom, internet access services, banking, and payment for different purposes than to provide these services;[961]
6. the platform and data power of tech giants, under special consideration of their increasingly relevant role as providers of verified identities;[962]

956 Romm T., Tech giants get deeper into D.C. influence game, Politico, 01/21/2015, http://www.politico.com/story/2015/01/tech-lobby-apple-amazon-facebook-google114468, Byers A., How a telecom-tech alliance wiped out FCC's privacy rules, Politico, 03/31/2017, http://www.politico.com/story/2017/03/broadband-data-victory-republicans-236760

957 Christl W., Spiekermann S., Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy, Facultas, Vienna 2016, http://crackedlabs.org/en/networksofcontrol, p. 45-75

958 Christl W., How Companies Use Personal Data Against People. Automated Disadvantage, Personalized Persiasion, and the Societal Ramifications of Commercial Use of Personal Information, 2017, https://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf

959 Christl W., Corporate Surveillance in Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions, June 2017, http://crackedlabs.org/en/corporate-surveillance

960 Christl W., Corporate Surveillance in Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions, June 2017, http://crackedlabs.org/en/corporate-surveillance

961 Christl W., Corporate Surveillance in Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions, June 2017, http://crackedlabs.org/en/corporate-surveillance

962 Christl W., Corporate Surveillance in Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions, June 2017, http://crackedlabs.org/en/corporate-surveillance

7. tech intermediaries aiming to "disrupt" traditional industries that try circumventing regulation and operate in grey legal areas, or whose business plan even includes changing the law,[963] deserve special attention regarding their data practices;

While addressing these issues will be more difficult in the US and other regions with weak legal privacy frameworks, the new European privacy legislation, which includes both the already adopted EU General Data Protection Regulation (GDPR) and the still disputed ePrivacy Regulation, might ban or at least slow down some of the most irresponsible and invasive practices of third-party data collection.[964] Other regulatory instruments such as anti-discrimination, consumer protection, and competition law are equally important in order to challenge unfair discrimination, information asymmetries and power imbalances[965], as well the dominance of certain large players that nobody can escape.[966]

One of the basic challenges for privacy legislation is the problem with consent and choice. Today, myriads of companies collect vast amounts of personal information about individuals without their effectively informed consent and knowledge, although pretending otherwise at a formal level.[967] Better regulating and enforcing the principle of informed consent is certainly crucial in many areas. Technical solutions, such as standardized icons giving consumers a meaningful overview of data processing, standardized privacy exchange protocols, tools supporting semi-automated privacy self-management, so-called "privacy agents", may help, however, today's privacy policies and terms are often misleading, impossible to understand, and not adequately usable for consumers in their daily routine. The problem is that principles of consent and choice unilaterally shift the responsibility of privacy protection to the individual level, which leads to several problems:[968]

1. It is nearly impossible for consumers to comprehend the mechanisms and possible long-term implications of today's data processing.[969]

963 Pollman E., Barry J. M., Regulatory Entrepreneurship, 90 S. Cal. L. Rev. 383 (2017); Loyola Law School, Los Angeles Legal Studies Research Paper No. 2017-29, https://ssrn.com/abstract=2741987

964 IHS Markit, The economic value of behavioural targeting in digital advertising. Analysis on behalf of IAB Europe and EDAA, 2017, https://datadrivenadvertising.eu/wp-content/uploads/2017/09/BehaviouralTargeting_FINAL.pdf

965 Rhoen M., Beyond consent: improving data protection through consumer protection law. Internet Policy Review, 5(1), 2016, https://policyreview.info/articles/analysis/beyond-consent-improving-data-protection-throughconsumer-protection-law

966 Auchard E., Germany takes on Facebook in competition probe, March 2, 2016, https://www.reuters.com/article/us-facebook-germany-dataprotection-idUSKCN0W40Y7

967 Christl W., Spiekermann S., Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy, Facultas, Vienna 2016, http://crackedlabs.org/en/networksofcontrol, p. 121-123

968 Hartzog W., Privacy and the Dark Side of Control. The Institute of Art and Ideas, Sept 4, 2017, https://iainews.iai.tv/articles/privacy-the-dark-side-of-control-auid-882

969 Hartzog W., Privacy and the Dark Side of Control. The Institute of Art and Ideas, Sept 4, 2017, https://iainews.iai.tv/articles/privacy-the-dark-side-of-control-auid-882

2. An issue that is getting increasingly important is that when individuals share data with companies this may also have an impact on the privacy of others.[970]
3. Refusing to agree to data collection is simply not an option in many cases. Consumers can hardly avoid privacy contracts because almost all banks, software and hardware vendors, social networking sites, digital content services, retail loyalty programs, and telecommunications providers employ them.[971]

6.3. Future work

The aim of the future work is to set an ideal model of privacy in the European Union. I argue that privacy is long gone, protection doesn't work, hence, any future project will be focused around regaining privacy. The core element lies in effectively regaining the right to consent, now severely endangered by non-read complex privacy agreements. Data protection legislation alone may not be enough to deal with the consequences a data-driven world has on individuals and society.[972] Education on large scale is one possible solution. Consumers should have a better understanding of the privacy they are losing. "Terms and conditions" and rules on cookies are an example[973]. Not only provisions in GDPR setting rules on what must be included in those are not clear, but companies collecting data are not interested in making it to understand. I propose implementing the idea of Visual Contracts – legal documents, simplified in the form to make them easy to understand and interesting to read.[974] Another solution is new technologies, such as Blockchain. In some cases, it is a tool for data protection.[975] Designing privacy-protecting blockchains is possible.[976]

970 Taylor L., Floridi L., van der Sloot B. (eds.), Group Privacy: new challenges of data technologies. Dordrech 2017, p. 9

971 Rhoen M., Beyond consent: improving data protection through consumer protection law. Internet Policy Review, 5(1), 2016, http://policyreview.info/articles/analysis/beyond-consent-improving-data-protectionthroughconsumer-protection-law, p. 2

972 Christl W., CORPORATE SURVEILLANCEIN EVERYDAY LIFE, How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions, Vienna, June 2017, http://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf, p. 84

973 Commission's Proposal for ePrivacy Regulation admits that rules on giving cookies consent must be completely redesigned. Right now, users do not read the terms, the process became automated and do not serve its purpose.

974 Haapio H., Plewe D. A., De Rooy R., Contract Continuum: From text to images, comics and code, [in:] Schweighofer E., Kummer F., Hotzendorfer W., Ch. Sorge (eds.), Trends and Communities of Legal Informatics, Salzburg 2017, p. 411-418

975 Zyskind G., Nathan O., A. Pentland, Decentralizing Privacy: Using Blockchain to Protect Personal Data, http://ieee-security.org/TC/SPW2015/IWPE/5.pdf

976 What is the impact of blockchains on privacy?, https://theodi.org/blog/impact-of-blockchains-on-privacy

Adoption of blockchain technology can remove the need for large companies to maintain data and provide individuals with complete control over their personal data.[977]

I am aware of significant barriers. When it comes to privacy, the main abusers are powerful actors, such as dominant ICT companies and governments. Some changes may prove to be difficult to implement or even to propose – on the one side there is the ambitious goal of regaining privacy, on the other side there is a huge market for monetizing data that comes from abusing privacy. Another aspect is the problem of privacy as a traditional value bringing strong emotions.

6.4. Final remarks

The idea of "data ownership" is often championed as a solution. However, what is the point of owning data that should not exist in the first place? All that does is further institutionalise and legitimate data capture. Data ownership also fails to reckon with the realities of behavioural surplus. Users might get ownership of the data that they give to surveillance capitalists in the first place, but they will not get ownership of the surplus or the predictions gleaned from it. Certainly, not without new legal concepts built on an understanding of these operations.

Some of the listed ideas on how to deal with dominant ICT companies include breaking them up. There may be sound competition law reasons to break up the largest ICT companies, but this alone will not eliminate surveillance capitalism. Instead, it will simply produce smaller companies and open the field for competitors in the market of "data abuse".

As time goes on and the Internet evolves daily, we need to protect our privacy with greater care. The less care we use, the fewer rights we shall have, and it's a proven fact. There is a growing trend by the courts to rely on old case law and statutes not created for purposes the endless growing Internet. There's not one solution that may best fix this problem, but awareness of your privacy rights while online using social media services or email is a start.[978]

Some ways to protect ourselves:

1. The use of anonymous servers that will allow a blurring of our location information. Instead of using highly accurate location information us as users, can consent to more of a generic location to be broadcasted to others rather than our home address or exact location, such as nearby cities, or landmarks.

977 Blockchains Can Assist EU Regulatory Fight for Personal Data Protection, https://www.law111.com/blockchains-can-assist-eu-regulatory-fight-for-personal-data-protection

978 Sanvenero R., Social Media and Our Misconceptions of the Realities, https://ssrn.com/abstract=2243896, 2013, p. 101

The choice of privacy is left in you as the user of the technology to choose what you broadcast, or allow.[979]

2. We live in a free market society where no one forces us to buy luxury items such as smartphones. What is more, even if we have a smartphone we should limit the date we broadcast. By posting photos, our location, logging to all possible services, including social media, we are diminishing our privacy.
3. Other potential remedies should come from legislatures. As mentioned before the US and EU differ in the approach and scope of legislation. However, it is obvious that legislation is one of the most important ways to protect our privacy.

Major tech companies including Alibaba, Arm, Baidu, IBM, Intel, Google Cloud, Microsoft, and Red Hat today announced the intent to form the Confidential Computing Consortium to improve security for data in use. Established by the Linux Foundation, the organization plans to bring together hardware vendors, developers, open source experts, and others to promote the use of confidential computing, advance common open source standards, and better protect data.[980]

Some of the early contributions include a Microsoft framework[981] that helps you write code to run inside Trusted Execution Environments, an Intel framework for protecting code at the hardware level and a Red Hat tool that abstracts secure environments to the point where you can create and run private "serverless" apps.[982]

Forcing companies to respect a web browser's "Do Not Track"[983] setting – and advocating for such as the default – would probably undercut much of the tracking that pervades today's web. Making it more difficult to use pseudonymous codes and identifiers to constantly link and match digital profiles across companies for purposes other than the provided services would probably disrupt parts of today's "markets of behavioural control".

---

979 Athanasios S. Voulodimos and Charalampos Z. Patrikakis, Quantifying Privacy in Terms of Entropy for Context Aware Services, special issue of the Identity in the Information Society journal, "Identity Management in Grid and SOA", Springer, vol. 2, no 2, December 2009.

980 Khari J., Intel, Google, Microsoft, and others launch Confidential Computing Consortium for data security, August 21, 2019, https://venturebeat.com/2019/08/21/intel-google-microsoft-and-others-launch-confidential-computing-consortium-for-data-security/

981 Russinovich M., Microsoft joins partners and the Linux Foundation to create Confidential Computing Consortium, August 21, 2019, https://cloudblogs.microsoft.com/opensource/2019/08/21/microsoft-partners-linux-foundation-announce-confidential-computing-consortium/

982 Fingas J., Google, Intel and Microsoft form data protection consortium. They want to keep data safe even while you're using it, August 21, 2019, https://www.engadget.com/2019/08/21/confidential-computing-consortium/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmZpLw

983 https://www.eff.org/de/issues/do-not-track

Demanding and enforcing transparency about personal data collection, disclosure, analysis, and use has certainly its limits.[984] It will not always directly empower individuals who already cannot handle the information overload caused by thousands of pages in privacy policies, and it will never be a replacement for solid protection. However, given the extent of opacity and non-transparency currently in place, it empowers individuals indirectly by providing authorities, advocates, journalists, and others with powerful means to address questionable practices and raise awareness. Research, investigation, raising awareness, and legal action are certainly the basis for being able to cope with the market power, resources, and lobbying efforts of today's personal data industries. Single initiatives do have an exceptional impact, as well do coordinated efforts across different kinds of stakeholders, including consumer, digital rights and civil rights organizations, as well as universities, media, privacy and law professionals, data protection authorities, and parts of the industry working on privacy-preserving technologies and business models.

It was only to be hoped that the EU-US Privacy Shield would guarantee adequate protection of data. Commissioner Jourová's stated "when data travels, the protection has to travel with it" should be achieved for EU-US data transfers.[985] However, now we know that Privacy Shield did not meet the expectations placed on it.[986] From a legal point of view, it is essential that the fundamental right to data protection is not compromised for commercial objectives.[987]

There is also increasing evidence of a broader EU assault on US telecommunications and internet companies. The European Parliament has been calling for a breakup of Google, German and French telecoms companies have charged that US internet companies are a tool of US security agencies. Even the relatively free market of UK has just announced a 25 per cent tax (labelled the "Google Tax" by the Financial Times) on multinational high-tech corporations.[988] Back in 2019, France has passed a tax on digital services[989] that was supposed to hit US dominant ICT companies.

---

984 Ananny M., Crawford K., Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability, New Media & Society, 2016, https://doi.org/10.1177/1461444816676645i, Crain M., The limits of transparency: Data brokers and commodification, New Media & Society, 2016, https://doi.org/10.1177/1461444816657096

985 Speech by Commissioner Jourová: The future of U.S.-EU data transfer arrangements at the Brookings Institution, SPEECH/15/6104, http://ec.europa.eu/justice/data- protection/document/review2012/com_2012_11_en.pdf.

986 Read more in 5.1.3.

987 Jaspers R., When data travels - The Commission's objective of making EU data protection travel across the Atlantic, February 2016, https://www.academia.edu/22343341/Robbert_Jaspers_When_data_travels_-_The_Commission_s_objective_of_making_EU_data_protection_travel_across_the_Atlantic?email_work_card=view-paper

988 The Misbegotten 'Right to Be Forgotten', http://www.usnews.com/debate-club/should-there-be-a-right-to-be-forgotten-on-the-internet/the-misbegotten-right-to-be-forgotten

989 Escape Presse, Création d'une taxe sur les services numériques, July 22, 2020, http://www.senat.fr/espace_presse/actualites/201904/creation_dune_taxe_sur_les_services_numeriques.html

Under the bill, tech companies with more than €750 million in global revenue and €25 million in French revenue would be required to pay a 3 percent tax on total annual revenue generated by providing services to French users. The move would affect companies like Google, Facebook, and Amazon, and was made as plans for EU-wide tax changes seemed to stall.[990] However, France had agreed to postpone the tax until the end of 2020.[991]

The assault on behavioural data is so sweeping that it can no longer be circumscribed by the concept of privacy and its contests. This is a different kind of challenge now, one that threatens order defined by principles of self-determination that have been centuries in the making. These principles include but are not limited to, the sanctity of the individual and the ideals of social equality; the development of identity, autonomy, and moral reasoning; the integrity of contract, the freedom that accrues to the making and fulfilling of promises; norms and rules of collective agreement; the functions of market democracy; the political integrity of societies; and the future of democratic sovereignty.

Google's success derives from its ability to predict the future. From the start, Google had collected data on users' search-related behaviour as a by-product of query activity. Back then, these data logs were treated as waste, not even safely or methodically stored. Eventually, the company came to understand that these logs could be used to teach and continuously improve its search engine. Google, Facebook, and others shifted to an advertising model that required the covert capture of user data as the currency for ad sales. Profits rapidly materialized and motivated ever more ruthless and determined data collection. The new science of data mining exploded, driven in part by Google's spectacular success.

ICT companies involved in data collection admit that the goal of everything they do is to change people's actual behaviour at scale. When people use applications, they can capture behaviours, identify good and bad behaviours, and develop ways to reward the good and punish the bad. Eventually, companies can test how profitable it all becomes.

If there is a single word to describe Google, it is „absolute."[992] The „Internet", „Web", and „Google" are referenced interchangeably, as if Goggle's interests stand for the entire Web and Internet. I would argue that same can be used for Facebook and even for Microsoft. This way I would like to go a step further from "Dominant ICT Company" or even super-dominant. "Internet", "Web", "Social media", "Computers",

990 Guarascio F., EU digital tax plan flounders as states ready national moves, November 6, 2018, https://www.reuters.com/article/us-eu-tax-digital/eu-digital-tax-plan-flounders-as-states-ready-national-moves-idUSKCN1NB15F

991 Lecher C., France will delay controversial tech tax, January 23, 2020, https://www.theverge.com/2020/1/23/21078574/france-us-digital-tax-deal-negotiations-tariffs-postponed-trump

992 Zuboff S., Dark Google, April 30, 2014, https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshanna-zuboff-dark-google-12916679.html

these are terms dominated by the companies I used as the most prolific examples of privacy abusers in this dissertation.

The privacy rights have not been eroded, if anything they've multiplied. The difference now is how these rights are distributed. Instead of many people having some privacy rights, nearly all the rights have been concentrated in the hands of a few. On the one hand, we have lost the ability to choose what we keep secret, and what we share.

However, we must remember that we are powerful too. Our demands for self-determination are not easily extinguished. We made Google Facebook and Microsoft, or any other dominant ICT company, perhaps by loving them too much.[993] Perhaps we could "unmake" them. The challenge is to understand what is at stake and how quickly things are moving. In the simplest words, our privacy is at stake and everything that comes from it.

In the 2020 TV series Devs[994] the question is asked: *You know the problem with people who run tech companies? They have too much power.* In my thesis, I listed numbers, names and examples that show the unique, extremely powerful position of the companies that I have chosen. However, everyday we learn more about tech companies, and almost everything we can imagine is influenced by them.

Jeffrey P. Bezos, the founder and chief executive of Amazon, also owns Blue Origin, a rocket company. By reactivating 1970's technology he plans to land on the Moon[995] Without judging that fact, it is worth to mention that Twitter found itself in the position to censor the President of the United States.[996] It is not surprising that US Military runs on Microsoft's Windows XP.[997] But it might be surprising to know that also Russian and Chinese military do the same. And only planning to switch to Linux.[998] As mentioned in the thesis before, Facebook was heavily involved in the US presidential elections. Google, which we know from Chrome and Gmail, works on Quantum computer.[999]

---

993 Zuboff S., Dark Google, April 30, 2014, https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshanna-zuboff-dark-google-12916679.html

994 https://www.imdb.com/title/tt8134186/

995 Levy S., Jeff Bezos Wants Us All to Leave Earth—for Good, 15 October 2018, https://www.wired.com/story/jeff-bezos-blue-origin/#:~:text=03%3A15%20PM-,Jeff%20Bezos%20Wants%20Us%20All%20to%20Leave%20Earth%E2%80%94for%20Good,humanity%20into%20an%20extraterrestrial%20future.

996 Hern A., Twitter hides Donald Trump tweet for 'glorifying violence', 29 May, 2020, https://www.theguardian.com/technology/2020/may/29/twitter-hides-donald-trump-tweet-glorifying-violence

997 Hsu J., Why the Military Can't Quit Windows XP, June 4, 2018, https://slate.com/technology/2018/06/why-the-military-cant-quit-windows-xp.html

998 Cimpanu C., Russian military moves closer to replacing Windows with Astra Linux, Nay 30, 2019, https://www.zdnet.com/article/russian-military-moves-closer-to-replacing-windows-with-astra-linux/

999 Savage N., Hands-On with Google's Quantum Computer, October 24, 2019, https://www.scientificamerican.com/article/hands-on-with-googles-quantum-computer/

Especially the last example has significant importance for this work and for the future of data protection. Why? Cryptography is the cradle of quantum technology. Today's security systems are protected by cryptographic keys that can be decrypted to some extent depending on their complexity and hacker abilities. But quantum technology completely changes the rules of the game, so a new security protocol must be developed to protect data - both future and current. - The problem actually exists and must be taken as soon as possible. Storing data is very cheap, so an intelligent hacker or competitive government can save your encrypted data and, in the future, use a quantum computer to easily decipher past data.

(Super)dominant ICT companies are part of our everyday live. And every day they takeover another field. Either it is military, quantum technology or space technology. We live in a times when companies are hiring sci-fi writers to imagine the future.[1000] After all, Stanisław Lem is known for predicting the Internet, Google and even algorithmic surveillance.[1001] No wonder the law has difficulties in keeping up with the changes.

1000 Underwood K., Why companies are hiring sci-fi writers to imagine the future, 27 February, 2020, https://www.cpacanada.ca/en/news/pivot-magazine/2020-02-27-sci-fi-prototyping

1001 Glinter E., The Future According to Stanisław Lem, September 12, 2014, https://www.theparisreview.org/blog/2014/09/12/the-future-according-to-stanislaw-lem/, Lovaszy L., Alvert D., This brilliant Pole predicted algorithmic surveillance, machine learning and even a virus outbreak in Italy, March 29, 2020, https://rmx.news/article/commentary/this-brilliant-pole-predicted-algorithmic-surveillance-machine-learning-and-even-a-virus-outbreak-in-italy

Finnish Summary

Sosiaalinen media on alkuajoistaan lähtien tuonut muutoksia jokapäiväiseen elämäämme. Kybermaailma laajentui räjähdysmäisesti 1990-luvun lopulla Microsoftin luotua Internet Explorer -selaimen, joka tarjosi Windows-tietokoneiden käyttäjille pääsyn mille tahansa verkkosivulle verkko-osoitetta käyttämällä. Internetiä käytettiin 1990-luvulla pääasiassa verkkoselailuun ja verkkopalveluntarjoajien sähköpostipalveluihin. Nykyään sosiaalinen media on vallannut Internet-maailman. Sosiaalisen median synnytti Internet, joka mahdollistaa henkilökohtaisten tietojen jakamisen ihmisten kesken. Se suunniteltiin leviämään sosiaalisen vuorovaikutuksen avulla ja hyödyntäen erittäin helposti saavutettavia ja skaalautuvia julkaisutekniikoita.

Inhimillisestä kokemuksesta ja henkilötiedoista on tullut korvaamatonta uutta informaatioajan raaka-ainetta, ja monet liiketoimintamallit nojaavat vahvasti dataan. Nykyään on ilmeistä, että data ja rajat ylittävät tietovirrat ovat elinehtoja nykyaikaiselle ja tulevaisuuteen suuntautuneelle taloudelle, ja niinpä tiedonhallintaan liittyvät kysymykset ovat näyttävästi esillä Euroopan unionin poliittisilla asialistoilla.

Väitän, että tämän päivän yhteiskunta on tullut täysin riippuvaiseksi teknologiasta. Sitä tarvitaan työssä (esim. ajokorttitietokannat), elämisessä (esim. terveydenhuollon tietokannat) ja vapaa-ajalla (esim. Facebook). Suuret monikansalliset yritykset selvittävät täsmällisesti kuluttajien mieltymyksiä, elämäntapavalintoja ja yleistä verkkokäyttäytymistä. Riippumatta siitä, jaammeko tietoa vapaaehtoisesti vai lain vaatimusten täyttämiseksi, annamme asialle niukasti huomiota. Useinkaan emme näe mitään ongelmallista siinä, että jaamme Internetissä itsestämme mitä henkilökohtaisimpia yksityiskohtia, kuten puhelinnumeromme, kotiosoitteemme ja muita vastaavia tietoja. Sosiaalisen median sivustoilla on keinonsa, joilla ne rohkaisevat meitä harkitsemattomaan tietojen jakamiseen esimerkiksi tarjoamalla henkilökohtaisempia palveluita, mikä johtaa Internet-profiileihimme kohdistuvaan tunnepohjaiseen kiintymykseen ja saa meidät jakamaan entistä enemmän itsestämme. Yritykset keräävät miljardien kuluttajien tietoja eri lähteistä, paljolti kuluttajien tietämättä. Elämäämme havainnoimalla kerätyistä tiedoista on tullut erittäin arvokkaita viranomaisille ja yksityisille yrityksille. Data on yksinkertaisesti valuuttaa itsessään sekä analyysien ja valittujen markkinoiden ymmärtämisen lähde. Kyse on resurssista, josta ei tulla luopumaan helposti.

Viimeisen 15 vuoden aikana häikäilemättömään datan hyväksikäyttöön pohjautuviin liiketoimintamalleihin on kaadettu miljardeja dollareita riskisijoituspääomaa ilman eettisten, yhteiskunnallisten, kulttuuristen ja poliittisten

vaikutusten huomioimista. Lisäksi yksityisyyssääntelyn puute Yhdysvalloissa ja sen valvonnan ja täytäntöönpanon heikkous Euroopassa ovat aktiivisesti ehkäisseet muunlaisia digitaalisia innovaatioita – autonomiaa, demokratiaa, sosiaalista oikeudenmukaisuutta ja ihmisarvoa tukevia ja säilyttäviä käytäntöjä, teknologioita ja liiketoimintamalleja. Teknologiajättiläiset ja teollisuusryhmittymät harjoittavat laajamittaista lobbaustoimintaa tarkoituksenaan aktiivisesti muotoilla yhteiskuntapolitiikkaa etujensa mukaiseksi.

Miten asiaan tulisi sitten suhtautua? Miten Facebookia, Googlea, Microsoftia ja muita jättiläisiä tulisi käsitellä? Datankeruuta harjoittavat ICT-yritykset myöntävät, että niiden kaiken toiminnan tavoitteena on muuttaa ihmisten käyttäytymistä suuressa mittakaavassa. Kun ihmiset käyttävät sovelluksia, yritykset voivat tallentaa tietoja käyttäytymismalleista, tunnistaa hyvän ja huonon käytöksen sekä kehittää tapoja hyvien palkitsemiseen ja huonojen rankaisemiseen. Lopulta yritykset voivat testata, kuinka kannattavaa siitä kaikesta tuleekaan.

Ratkaisuksi on usein esitetty ajatusta tietojen omistamisesta. On kuitenkin kysyttävä, mikä merkitys on tietojen omistamisella, jos niiden ei olisi alun perinkään pitänyt olla olemassa. Omistajuusajattelu vain institutionalisoi ja legitimoi datankeruuta, eikä se myöskään huomioi ns. käyttäytymiseen liittyvää ylijäämää (behavioural surplus). Käyttäjät saavat ehkä omistajuuden alkuperäisiin valvontakapitalisteille luovuttamiinsa tietoihin, mutta he eivät saa omistajuutta ylijäämään eli ennusteisiin, jotka tehdään näiden tietojen pohjalta. Näin ei tapahdu ainakaan ilman uusia oikeudellisia käsitteitä, jotka on rakennettu näiden toimintojen ymmärryksen pohjalta.

Ongelmien ratkaisuksi on esitetty myös hallitsevassa asemassa olevien ICT-yritysten pilkkomista pienempiin osiin. Olemassa voi olla järkeviä kilpailuoikeudellisia syitä suurimpien ICT-yritysten hajottamiseen, mutta tämä ei yksistään riittäisi eliminoimaan valvontakapitalismia, vaan yksinkertaisesti synnyttäisi pienempiä yrityksiä ja avaisi datan väärinkäytön markkinoita kilpailijoille.

Hallitsevassa tai jopa ylivaltaisessa asemassa olevat ICT-yritykset ovat osa jokapäiväistä elämäämme. Ja joka päivä ne valtaavat uusia aloja, oli kyse sitten sotilaallisesta toiminnasta, kvanttiteknologiasta tai avaruusteknologiasta. Elämme ajassa, jossa yritykset palkkaavat tieteiskirjailijoita kuvittelemaan tulevaisuutta. Tunnetaanhan esimerkiksi Stanisław Lem Internetin, Googlen ja jopa algoritmisen valvonnan ennustamisesta. Ei ihme, että oikeuden on vaikea pysyä muutoksissa mukana.

Polish Summary

Od dnia swojego powstania media społecznościowe przyspieszają zmiany w naszym codziennym życiu. Świat wirtualny w dzisiejszym rozumieniu miał swój początek pod koniec lat 90. XX wieku, kiedy Microsoft stworzył Internet Explorer, przeglądarkę, która umożliwiła użytkownikom komputerów z systemem Windows dostęp do dowolnej istniejącej witryny internetowej. Internet w latach 90. był używany głównie do przeglądania stron internetowych i usług poczty elektronicznej. W dzisiejszych czasach świat wirtualny opanowały media społecznościowe. Są konsekwencją Internetu, który umożliwia ludziom wymianę danych osobowych między sobą i zostały zaprojektowane do rozpowszechniania ich poprzez interakcje społeczne, przy użyciu łatwo dostępnych i zaawansowanych technik publikowania.

Doświadczenia ludzkie i dane osobowe z pewnością stały się nieodzownym nowym surowcem w erze informacyjnej, ponieważ wiele modeli biznesowych w dużym stopniu opiera się na danych. Obecnie jest oczywiste, że dane i ich przepływ przez granice mają zasadnicze znaczenie dla nowoczesnej i zorientowanej na przyszłość gospodarki, a zatem kwestie zarządzania danymi zajmują ważne miejsce w programach politycznych Unii Europejskiej.

Twierdzę, że dzisiejsze społeczeństwo całkowicie uzależniło się od nowoczesnych technologii. Są potrzebne do pracy (np. bazy danych praw jazdy), do życia (np. bazy danych opieki zdrowotnej) i dla przyjemności (np. Facebook). Duże międzynarodowe firmy i ich użyciem określają preferencje konsumentów, wybory dotyczące stylu życia i ogólne zachowania w sieci. Bez względu na to, czy udostępniamy te informacje swobodnie, czy też jest to wymóg prawny, poświęcamy temu niewiele uwagi. Bardzo często nie widzimy problemu z udostępnianiem w Internecie najbardziej osobistych danych o nas, w tym numeru telefonu, czy też adresu domowego. Strony mediów społecznościowych mają narzędzia, które zachęcają nas do lekkomyślnego zachowania, na przykład poprzez zapewnienie nam większej personalizacji, co ma prowadzić do emocjonalnego przywiązania do naszych profili internetowych, a tym samym do jeszcze szerszego udostępniania. Firmy zbierają dane o miliardach konsumentów z różnych źródeł, głównie bez ich wiedzy. Dane zebrane podczas obserwacji naszego życia stały się niezwykle cenne dla agencji rządowych i firm prywatnych. Stały się walutą samą w sobie i źródłem używanym do analizy i zrozumienia wybranych rynków. Nie jest to zasób, z którego można lub będzie łatwo zrezygnować.

W ciągu ostatnich 15 lat miliardy dolarów zostały przelane na finansowanie modeli biznesowych opartych na pozbawionym skrupułów masowym wykorzystywaniu

danych, bez uwzględnienia jakichkolwiek konsekwencji etycznych, społecznych, kulturowych i politycznych. Ponadto niedostatek przepisów dotyczących prawa ochrony prywatności w USA i brak ich wystarczającego egzekwowania w Europie aktywnie zahamował pojawienie się innych rodzajów innowacji cyfrowych - praktyk, technologii i modeli biznesowych, które chronią demokrację, sprawiedliwość społeczną, autonomię i godność człowieka. Giganci technologiczni angażują się w masowy lobbing mający na celu aktywne kształtowanie polityki publicznej w celu wzmocnienia ich pozycji.

Jak więc sobie z tym poradzić? Jak radzić sobie z gigantami takimi jak Facebook, Google, Microsoft i wieloma innymi? Firmy ICT zaangażowane w gromadzenie danych przyznają, że celem wszystkiego co robią, jest zmiana rzeczywistego zachowania ludzi na dużą skalę. Kiedy ludzie używają aplikacji, firmy mogą wychwytywać zachowania, identyfikować te dobre i złe, z ich punktu widzenia, oraz opracowywać sposoby nagradzania tych dobrych i karania za złe. W końcu firmy mogą sprawdzić, jaki ma to wpływ na zyski.

Jako jedno z rozwiązań często promowana jest tak zwana idea własności danych. Jaki jest jednak sens posiadania danych, które w ogóle nie powinny istnieć w obiegu? Wydaje się, że efektem jest dalsza instytucjonalizacja i legalizacja przechwytywania danych. Posiadanie danych również nie uwzględnia realiów tak zwanej „nadwyżki behawioralnej" (ang. behavioural surplus). Co prawda użytkownicy mogą próbować odzyskać własność swoich danych, które na co dzień przekazują tak zwanym „kapitalistom nadzoru" (ang. surveillance capitalists), czyli głównie potężnym firmom z branży ICT, ale nie uzyskają własności nad wspomnianą „nadwyżką" – nie mają nic z tego, że ich dane zostały już użyte. Z pewnością nie jest to możliwe bez nowych rozwiązań prawnych obejmujących tę problematykę.

Niektóre z wymienionych pomysłów, jak radzić sobie z dominującymi firmami ICT, obejmują ich rozbicie. Mogą istnieć uzasadnione powody wynikające z prawa konkurencji, aby rozbić największe firmy ICT, ale samo to nie wyeliminuje problemu. Zamiast tego po prostu stworzy mniejsze firmy i otworzy pole dla konkurentów na rynku „nadużyć danych".

(Super) dominujące firmy ICT są częścią naszego codziennego życia. I każdego dnia rozszerzają swoją działalność. Na technologię wojskową, kwantową, jak również kosmiczną. Żyjemy w czasach, gdy firmy zatrudniają pisarzy science fiction, aby wyobrazić sobie przyszłość. Przecież np. Stanisław Lem znany jest z tego, że przewidział powstanie Internetu, Google, a nawet nadzoru algorytmicznego. Nic dziwnego, że prawo ma tak duże trudności z nadążaniem za zmianami.

Appendix 1:
Changes in General Data Protection Regulation

Right to be Forgotten:

- A Right to be Forgotten helps people better manage data-protection risks online. When they no longer want their data to be processed and there are no legitimate grounds for retaining it, the data will be deleted.
- Whenever consent is required for data processing, it has to be given explicitly, rather than be assumed.
- Easier access to one´s own data and the right of data portability, i.e. easier transfer of personal data from one service provider to another.

Right to Data Portability:

The Regulation gives consumers an unprecedented new economic and human right—the right to data portability. The basic idea of the RDP is that individuals would be able to transfer their electronic information, such as a Facebook friend lists or iTunes music, from Facebook or Apple to a competitor, without hindrance. The biggest problem is that interoperability in practice is often difficult and costly, yet the Regulation appears to mandate new code from software and service providers. In addition, the Regulation ignores years of wisdom from antitrust law about how to address lock-in problems – the high switching costs that the EU is seeking to address. The Regulation applies to small and to large businesses, so long as they sell to any European consumers. It will cause cost and innovation issues. The idea might be one of the most controversial ideas standing behind the GDPR.

Additionally, it also poses serious risks to a long-established EU fundamental right of data protection: the right to security of a person's data. Previous access requests by individuals were limited in scope and format. By contrast, when an individual's lifetime of data must be exported "without hindrance," then one moment of identity fraud can turn into a lifetime breach of personal data.[1002]

Some more details about the changes introduced by the GDPR:

- Companies and organizations will have to notify serious data breaches without undue delay, when feasible within 24 hours.
- A single set of rules on data protection, valid across the EU.
- Companies will only have to deal with a single national data protection authority – in the EU country where they have their main establishment.
- Individuals will have the right to refer all cases to their home national data

1002 What's Wrong with the Proposed EU Right of Data Portability?, https://fpf.org/2012/10/17/whats-wrong-with-the-proposed-eu-right-of-data-portability/

protection authority, even when their personal data is processed outside their home country.
- EU rules will apply to companies not established in the EU, if they offer goods and services in the EU or monitor the online behaviour of citizens.
- Increased responsibility and accountability for those processing personal data.
- Unnecessary administrative burdens such as notification requirements for companies processing personal data will be removed.
- National data protection authorities will be strengthened so they can better enforce the EU rules at home

Definitions introduced or modified by GDPR:

Continuity of many core definitions (such as controller, personal data, data subject, processing, processor), but:

- Child – added definition, anyone under the age of 18. Additional protections apply to children under 13.
- Consent – more detailed, has to be explicit and given by statement or by a clear affirmative action.
- Genetic data – added definition, part of sensitive personal data. Any data that relate to characteristics that are inherited or acquired during early prenatal development.
- Sensitive personal data - more detailed, by adding genetic data and criminal convictions or related security measures.

There is also a broad definition of anonymous data - information that does not relate to an identified or identifiable natural person.[1003]

Changes in jurisdiction:

Directive provision: Applies to an entity established outside the EU if it uses a 'means of processing' (automated or otherwise) located in the EU. A 'means of processing' includes:

I. equipment situated in the EU (e.g., a server) unless that equipment is only used for the purposes of simply transmitting data; or
II. a processor established in the EU.

Change in the Regulation: New test. If an entity is established outside the EU, and it either:

III. offers goods or service to EU residents; or

1003 Wess M., Looking to comply with GDPR? Here's a primer on anonymization and pseudonymization, April 2017, https://iapp.org/news/a/looking-to-comply-with-gdpr-heres-a-primer-on-anonymization-and-pseudonymization/

IV. monitors the behaviour of EU residents, that entity will be subject to the Regulation.

Changes in the enforcement:

- Remedies – under Directive the rights of data subjects differ across Member States. Under Regulation there is Right to a remedy against a SA and Right to a remedy against a controller or processor.
- Compensation – added compensation from processor
- Sanctions - The Directive does not specify the sanctions to be imposed. Regulation include:

a. for individuals and small businesses who commit a first, non-intentional breach of the Regulation, a written warning may be given;
b. for a failure to provide an adequate mechanism for data subjects to exercise their rights, a fine of up to €250,000 or 0.5% of the controller's annual worldwide turnover;
c. for a failure to provide adequate information to data subjects or to allow subject access, or to comply with the right to be forgotten (amongst others), a fine of up to €500,000 or 1% of the controller's annual worldwide turnover; or
d. for processing personal data without a valid processing condition, failure to comply with the conditions relating to Profiling and other more serious breaches of the Regulation, a fine of up to €100 million or 2-5% of the controller's annual worldwide turnover.

Enforcement powers – DPA vs SA. Under Regulation SAs are given wide-ranging powers to enforce compliance with the Regulation (e.g., the power to compel a controller or processor to provide any information relevant to the performance of the SAs duties, and the power to impose a ban on processing).

Changes concerning Supervisory Authorities:

In both Directive and Regulation Each Member State must appoint one or more DPAs/SAs to protect the rights and freedoms of data subjects.

Added One Stop Shop - if a business is established in more than one Member State, it will have a lead authority, determined by the place of its main establishment in the EU.

European Data Protection Board (EDPB) formally replaced the Article 29 Working Party as the European advisory committee on data protection issues. In addition to taking over Article 29 Working Party's responsibilities in issuing guidelines, recommendations and statements of best practice, the EDPB, which operates as an independent body of the European Union with its own separate legal personality, also takes on a far broader set of responsibilities:

- examining – on its own initiative or on the request of one of its members or the European Commission (Commission) – any question covering the application of the GDPR;
- advising the Commission on any issue related to data protection in the EU, including on any proposed amendment of the General Data Protection Regulation (GDPR) and any EU legislative proposal;
- advising the Commission on the format and procedures for the exchange of information in the framework of the Binding Corporate Rules;
- providing the Commission with an opinion on the assessment of the adequacy of the level of protection in a third country;
- providing opinions on draft decisions of the supervisory authorities; and
- issuing binding decisions in certain instances, mostly about dispute resolution among supervisory authorities.[1004]

Consistency - Under the Directive, DPAs can adopt enforcement positions that differ from the positions adopted by other DPAs.

Under the Regulation, where a given processing activity affects data subjects in more than one Member State, the relevant SA must consult with all other affected SAs and the EDPB, to ensure that any enforcement action is consistent across the EU.

Changes concerning Accountability:

Any business that processes the personal data of more than 5000 data subjects in a year must appoint a DPO.

Under the Directive, controllers are required to register their processing activities with the relevant DPA.

Under the Regulation – no registration requirement → obligation to maintain internal records of data processing activities. The Regulation sets out a detailed list of information that must be included in these records and, in many cases, they are more detailed than the equivalent national registration requirements under the Directive.

Privacy by Design and by Default:

Not explicitly addressed in Directive.

Regulation - Whenever a business develops or designs a new technology, product or service, it should do so in a way that ensures compliance with data protection obligations. Businesses are legally required to:

I. Take data protection requirements into account from the inception of any new

1004 O'Donoghue C., Mackay A., European Data Protection Board replaces Article 29 Working Party, July 2, 2018, https://www.technologylawdispatch.com/2018/07/privacy-data-protection/european-data-protection-board-replaces-article-29-working-party/

technology, product or service that involves the processing of personal data[1005]; and

II. Conduct DPIAs where appropriate.

Profiling:

Directive – no explicit definition of Profiling, however there is narrower and similar practice of automated individual decisions

Under the Regulation, data subjects have the right not to be subject to measures based on Profiling that produce legal effects on them, or significantly affect them.

The Directive does not directly address the automated processing of sensitive personal data whereas in Regulation profiling performed solely on the basis of sensitive personal data is prohibited.

Data Breach Reporting:

Businesses that fail to fulfil their data breach reporting obligations may be sanctioned by the SA with a fine of up to €1 million or, up to 2% of annual worldwide turnover, whichever is greater.

Businesses will need to develop and implement a data breach response plan (including designating specific roles and responsibilities, training employees, and preparing template notifications) enabling them to react promptly in the event of a data breach.

Application of Processors:

Under the Directive, the primary obligation to comply with EU data protection law falls on controllers.

The Regulation will impose a number of obligations directly on processors. These direct obligations include:

- maintaining records of processing activities;
- cooperating with the relevant SA;
- implementing appropriate security measures;
- appointing a DPO;
- informing the controller in the event of a data breach;
- performing DPIAs;
- obtaining prior authorisation from, or ensuring prior consultation with, the relevant SA before commencing certain types of processing; and
- complying with the requirements of the Regulation regarding cross-border data transfer.

1005 GDPR, art. 25

The Regulation also explicitly states that a processor is considered a joint controller in the event that it processes personal data other than in accordance with the instructions of the controller.

Deliberate or negligent breach by a processor of its obligations will attract a fine of up to €100 million or 2-5% of annual worldwide turnover, whichever is greater.

Cross-Border Data Transfers:

Under the Directive, businesses are prohibited from transferring personal data out of the EEA unless:

- the transfer is to an Adequate Jurisdiction;
- the transfer is made pursuant to a mechanism that ensures an adequate level of protection (e.g., Model Clauses); or
- A derogation applies.

When businesses rely on Model Clauses or the U.S.-EU Safe Harbor, some DPAs insist upon prior notification.

Under the Regulation, the existing transfer restrictions will be preserved but, importantly, SAs will be prevented from requiring further notification or authorization where the requirements are otherwise satisfied.

Additionally, list of derogations in Commission Text is expanded.

Rights of Data Subject:

Under the Directive:

- The right to certain minimum information,
- The right of access,
- Right to object,
- The right to rectification, erasure or blocking of data

Under the Regulation, the rights of data subjects set out in the Directive continue to apply (subject to minor amendments and clarifications) and the following rights are added:

- The right to be forgotten,
- The right of data portability

Unharmonised areas:

Harmonization introduced by the Regulation is greater than in Directive, yet there will still be several issues that differ from one Member State to another. For example:

- National Security: Data processed for the purposes of the national security of a Member State are exempt from the Regulation. Member States have different conceptions of national security.

- Journalism and freedom of speech: The concepts of 'journalism' and 'freedom of expression' vary from one Member State to another (although Recital 121 of the Regulation states that 'journalism' should be interpreted broadly).
- Employment law: Member States may adopt their own rules regarding the processing of personal data in an employment context.
- Professional secrecy laws: Some Member States have laws on professional secrecy that prevent the processing of certain data, even where the Regulation would otherwise permit that processing.
- Processing and public access to official documents: Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.

Laws on interception of communications: Member States have interception laws under the e-Privacy Directive 2002/58/EC, which are not uniform across the EU.

Appendix 2:
European Commission's GDPR review

The Commission's review of the GDPR stemmed from its obligation, under Article 97 of the GDPR, to submit a report on the evaluation and review of the Regulation to EU law makers within two years of the GDPR taking effect. Its next review is due in 2024. The wide-ranging review looked at a number of important aspects of the data protection regime and how it had operated since the GDPR began to apply on 25 May 2018. As a result, actions planned in response to the findings from the European Commission's GDPR review[1006] underpin its broader aim for greater convergence of data protection standards internationally. These include renewed efforts to drive out differences in the way EU governments and national data protection authorities apply data protection law, a push to expand the network of jurisdictions deemed to offer 'equivalent' data protection to that available in the EU, and the revision of standard contract clauses (SCCs) to help companies transfer personal data around the world more easily. Refining data protection law and guidance to support digital innovation in areas such as use of artificial intelligence (AI) and blockchain technology is also high on the Commission's agenda.

In its report, the Commission noted that all EU member states except Slovenia have adopted new national data protection laws to implement and complement the GDPR. However, it also found that there is a "degree of fragmentation" in how the GDPR has been implemented across the different countries because of the freedom the Regulation provides member states in certain areas to specify their own national rules. Differences in the age of consent and the reconciliation of data protection with freedom of expression and information were highlighted in this regard. This causes uncertainty for data subjects in terms of how their rights apply and causes challenges for cross-border business and innovation. [1007] Also, businesses can expect the EDPB to publish[1008] new guidance on how the GDPR applies to the areas of scientific research, AI, blockchain, and potentially other technological developments too over the coming months.

The Commission pointed out the different approaches to derogations which permit the processing of 'special category data', including for health and research purposes. The Commission is mapping these different approaches and will support

1006 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCI, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, Brussels, 24.6.2020, COM(2020) 264 final, https://ec.europa.eu/info/sites/info/files/1_en_act_part1_v6_1.pdf

1007 Ibid. p. 6-7.

1008 Ibid. p. 17.

the establishment of codes of conduct to facilitate cross-border processing. It will also give feedback to the EDPB in relation to its future guidelines on the processing of personal data for scientific research.[1009]

The adequacy decision mechanism provided for by the GDPR, through which the European Commission endorses other jurisdictions as having equivalent data protection standards to those in place in the EU, has enabled the creation of large areas of free and safe data flows. The adequacy regime is also expected to play an important role in the context of the future, post-Brexit, relationship between the EU and UK in respect of digital trade, law enforcement and security. The need to ensure the continuity of adequacy decisions is an important tool for trade and international cooperation. SCCs are the most widely used data transfer mechanism, for transfers to countries that do not have an adequacy decision.[1010]

The Commission wants the EDPB to clarify the interplay between rules on international data transfers and the territorial scope of the GDPR. The GDPR's territorial scope which covers processing activities of foreign operators that are active in the EU market must also be reflected in the enforcement action by the data protection authorities, it said. In this regard, the Commission said representatives within the EU should be appointed to liaise with data protection authorities of so-called third countries.[1011]

The Commission also plans to establish a Data Protection Academy to facilitate and support exchanges between European and international data regulators.[1012]

In addition to delivering greater alignment of guidance, the Commission has invited the EDPB and national data protection authorities to effectively implement the cooperation and consistency mechanism, and support harmonisation by clarifying key GDPR concepts. The Commission committed to closely monitor the independence of national data protection authorities and to encourage cooperation between regulators, particularly in the fields of communications, competition, and consumer policy. It also called on member states to ensure that data protection authorities are sufficiently resourced.[1013]

Finally, the Commission has identified a number of ways that organisations can be better supported to comply with the GDPR. Examples include:

1) adoption of new, more practical guidelines to avoid ambiguities and to address important specific issues faced by stakeholders – new guidelines on processing children's data and data subject rights, including the exercise of the right of access and the right to erasure, are specifically referenced in the report;

1009 Ibid. p. 15.
1010 Ibid. p. 10, 11, 17.
1011 Ibid. p. 12, 17.
1012 Ibid. p. 13.
1013 Ibid. p. 15-16.

2) helping individuals exercise their right of portability;
3) cooperating with the ENISA on standardisation around cybersecurity issues;
4) financially supporting data protection authorities to help SMEs meet their GDPR obligations.[1014]

1014 Ibid. p. 16-17.

Table of cases

Court of Justice of the European Union

Case 27/76, United Brands Company and United Brands Continentaal BV v Commission of the European Communities. - Chiquita Bananas. ECLI:EU:C:1978:22

Case 322/81 Nederlandsche Banden-Industrie Michelin NV v. Commission, ECLI:EU:C:1983:313

Case 85/76 Hoffmann-La Roche & Co. AG v Commission of the European Communities, Dominant position., ECLI:EU:C:1979:36

Case C-101/01 Bodil Lindqvist, EU:C:2003:596

Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, EU:C:2014:317

Case C-141/12 and C-372/12 YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S, ECLI:EU:C:2014:2081

Case C-18/18 , Eva Glawischnig-Piesczek v Facebook Ireland Limited EU:C:2019:821

Case C-235/08 Asnef-Equifax v Asociación de Usuarios de Servicios Bancarios, ECLI:EU:C:2010:599

Case C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, ECLI:EU:C:2014:238

Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, ECLI:EU:C:2020:559

Case C-317/04 and C-318/04 European Parliament v Council of the European Union (C-317/04) and Commission of the European Communities (C-318/04), ECLI:EU:C:2006:346

Case C-32/11 Allianz Hungária, ECLI:EU:C:2013:160

Case C-333/94 P. Tetra Pak International SA v Commission of the European Communities, ECLI:EU:C:1996:436

Case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650

Case C-465/00, C-138/01, and C-139/01 Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v Österreichischer Rundfunk, EU:C:2003:294.

Case C-468/10 and C-469/10 Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) v Administración del Estado, ECLI:EU:C:2011:777

Case C-473/12 Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert and Others, ECLI:EU:C:2013:715

Case C-486/12 – X Judgment of the Court (Eighth Chamber) of 12 December 2013, Proceedings brought by X, ECLI:EU:C:2013:836

Case C-507/17 Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), EU:C:2019:772

Case C-518/07 European Commission v Federal Republic of Germany, ECLI:EU:C:2009:694

Case C-524/06 Heinz Huber v Bundesrepublik Deutschland, EU:C:2008:724

Case C-553/07 College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer Netherlands, ECLI:EU:C:2009:293

Case C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH, ECLI:EU:C:2019:801

Case C-683/13 Pharmacontinente - Saúde e Higiene SA and Others v Autoridade Para As Condições do Trabalho (ACT), ECLI:EU:C:2014:2028
Case C-73/07 Satakunnan Markkinapörssi and Satamedia, EU:C:2008:727
Case C-92 and C-93/09 Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen, ECR,EU:C:2010:662
Case T-82/09 Gert-Jan Dennekamp v European Parliament, ECLI:EU:T:2011:688
Court of Justice of the European Union PRESS RELEASE No 106/15, Luxembourg, 23 September 2015, http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-09/cp150106en.pdf
Court of Justice of the European Union PRESS RELEASE No 112/19, Luxembourg, 24 September 2019, https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-09/cp190112en.pdf
Court of Justice of the European Union PRESS RELEASE No 117/15, Luxembourg, 6 October 2015, Judgment in Case C-362/14, Maximillian Schrems v Data Protection Commissioner, http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf
Court of Justice of the European Union PRESS RELEASE No 128/19, Luxembourg, 3 October 2019, https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-10/cp190128en.pdf
Court of Justice of the European Union, PRESS RELEASE No 117/15, Luxembourg, 6 October 2015, Judgment in Case C-362/14 Maximillian Schrems v Data Protection Commissioner, http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf
Opinion of Mr Advocate General Fennelly delivered on 29 October 1998, Compagnie maritime belge transports SA (C-395/96 P), Compagnie maritime belge SA (C-395/96 P) and Dafra-Lines A/S (C-396/96 P) v Commission of the European Communities, ECLI:EU:C:1998:518
Opinion of Advocate General Jääskinen delivered on 25 June 2013, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, ECLI:EU:C:2013:424
Opinion of Advocate General Saugmandsgaard Øe delivered on 19 December 2019, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, ECLI:EU:C:2019:1145
Opinion of Advocate General Szpunar delivered on 4 June 2019, Eva Glawischnig-Piesczek v Facebook Ireland Limited, ECLI:EU:C:2019:458
Opinion of Advocate General Bot delivered on 23 September 2015, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:627
Press Release No 91/20, Court of Justice of the European Union, The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield, Luxembourg, 16 July 2020, https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf
Statement on the Court of Justice of the European Union Judgment in Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, 17 July, 2020, https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_en#:~:text=and%20Maximillian%20Schrems-,Statement%20on%20the%20Court%20of%20Justice%20of%20the%20European%20Union,Facebook%20Ireland%20and%20Maximillian%20Schrems&text=The%20EDPB%20identified%20in%20the,decision%20to%20declare%20it%20invalid.

European Court of Human Rights

ECtHR, Weber v Germany, Application no. 54934/00, 29 June 2006
ECtHR, Kennedy v United Kingdom, Application no. 26839/05, 18 May 2010
ECtHR, Von Hannover v. Germany, Application no. 59320/00, 24 June 2004
ECtHR, Malone v United Kingdom, Application no. 8691/79, 2 August 1984

National Courts

United States

Brocke Grp. v. Brown & Williamson Tobacco Corp., 509 U.S. 209 (1993)
Case No. 19-cv-2184, United States of America v. FACEBOOK, Inc., https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf
Case No.: 1:19-cv-2642, https://www.ftc.gov/system/files/documents/cases/youtube_complaint.pdf
Melvin v. Reid, 112 Cal.App. 285, 297 P. 91 (1931)
Riley v. California, 573 U.S. 373 (2014)
Sidis v F-R Publishing Corporation 311 U.S. 711 61 S. Ct. 393 85 L. Ed. 462 1940 U.S
United States v. Verdugo-Urquidez 494 U.S. 259 (1990),
Briscoe v. Reader's Digest Association, Inc. , 4 Cal.3d 529 [L.A. No. 29813. In Bank. Apr. 2, 1971.]
Yahoo! Inc. v. La Ligue Contre Le Racisme, 433 F.3d 1199, 1202–03 (9th Cir. 2006)

Table of statutes and conventions

European Union

Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community, OJ L 29, 31.1.2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12019W/TXT(02)

Article 29 Data Protection Working Party, Opinion 01/2012 on the Data Protection Reform Proposals, 00530/12/EN, WP 191 (Mar. 23, 2012). http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf. See Online Privacy Law: European Union, Library of Congress (May 2014). www.loc.gov/law/help/online-privacy-law/eu.php

Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Article 29 Data Protection Working Party. Opinion 01/2010 on the concepts of "controller" and "processor". Article 21 Data Protection Working Party. February 2010. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

Article 29 Data Protection Working Party. Opinion 05/2012 on Cloud Computing. May 2012. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

Charter of Fundamental Rights of the European Union, proclaimed by the European Council on December 7, 2000 in Nice, O.J., 18.12.2000, C 364/1.

Convention for the Protection of Human Rights and Fundamental Freedoms, CETS No.005, 03/09/1953

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No.108, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37

Council Decision of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, OJ L 195, 27.7.2010, p. 3–4

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, p. 60–71

Data Protection: Europeans Share Data Online, but Privacy Concerns Remain — New Survey. European Commission press release, June 16, 2011. http://europa.eu/rapid/press-release_IP-11-742_en.htm

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 on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016]

DIRECTIVE 2000/31/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

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, p. 37–47

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 [2006]

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 (Text with EEA relevance), OJ L 337, 18.12.2009, p. 11–36

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, OJ L 281, 23.11.1995

EP resolution of 5 July 2018, Adequacy of the protection afforded by the EU-US Privacy Shield, http://www.europarl.europa.eu/doceo/document/TA-8-2018-0315_EN.html?redirect

EU - U.S. Privacy Shield - Second Annual Joint Review, Adopted on 22 January 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/20190122edpb_2ndprivacyshieldreviewreport_final_en.pdf?

General Data Protection Regulation – A Council General Approach At Last!, 17 June 2015, http://www.twobirds.com/en/news/articles/2015/global/general-data-protection-regulation-jha-council

Handbook on European data protection law. 2018 edition, https://publications.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1

Data Protection Commissioner, Facebook Ireland Ltd: Report of Audit, 21 December 2011, 39: http://www.dataprotection.ie/documents.facebook%20report/final%20report/report.pdf

European Data Protection Supervisor – Annual Report 2014, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2014/EDPS_Annual_Report_2014_Web_EN.pdf

European Data Protection Supervisor, Opinion 3/2018, EDPS Opinion on online manipulation and personal data, https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf

Presidential Policy Directive 28 (PPD-28), January 12, 2015, http://fas.org/irp/nsa/nsa-ppd-28.pdf

Press Release: ICT industry joins forces on Data Protection in Europe, http://www.iabeurope.eu/policy/data-protection/press-release-ict-industry-joins-forces-data-protection-euro

Privacy and Self-Regulation in the Information Age, issued by the National Telecommunications and Information Administration, U.S. Department of Commerce, 1997

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, /* COM/2012/010 final - 2012/0010 (COD) */

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), COM/2017/010 final - 2017/03 (COD), http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2017:0010:FIN

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act), Brussels, 15.12.2020, COM(2020) 842 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842&from=en

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive, 2000/31/EC, Brussels, 15.12.2020, COM(2020) 825 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en

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, OJ L 8, 12.1.2001, p. 1–22

Regulation (EU) 2016/679 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 119/1

Resolution on anchoring data protection and the protection of privacy in international law, September 2013, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/13-09-24_International_Law_Resolution_EN.pdf

Statement of the Article 29 Working Party, Brussels, 16 October 2015, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf

The EDRi papers, issue 06, https://edri.org/wp-content/uploads/2013/10/paper06_web_20130128.pdf

Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community [2007] OJ C 326

WP29 Press Release, "Sorry is not enough": WP29 establishes a Social Media Working Group, Brussels, 11 April 2019, https://edps.europa.eu/sites/edp/files/publication/18-04-11_wp29_press_release_en.pdf

European Commission Documents

Attitudes on Data Protection and Electronic Identity in the European Union, European Commission 7 (June 2011). http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

Case M8124 – Microsoft / LinkedIn [2016] European Commission Decision

Case No COMP/M7217 - Facebook/ Whatsapp [2014] European Commission Decision

Commission decides selective tax advantages for Fiat in Luxembourg and Starbucks in the Netherlands are illegal under EU state aid rules (2015) http://europa.eu/rapid/press-release_IP-15-5880_en.htm

COMMISSION DECISION of 24 May 2004 relating to a proceeding pursuant to Article 82 of the EC Treaty and Article 54 of the EEA Agreement against Microsoft Corporation (Case COMP/C-3/37.792 — Microsoft), 2007/53/EC

COMMISSION DECISION of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, C(2010) 593, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32010D0087&from=enhttp://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF

COMMISSION IMPLEMENTING DECISION (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, C(2016) 4176, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016D1250&from=EN

COMMISSION IMPLEMENTING DECISION (EU) 2016/2297, of 16 December 2016, amending Decisions 2001/497/EC and 2010/87/EU on standard contractual clauses for the transfer of personal data to third countries and to processors established in such countries, under Directive 95/46/EC of the European Parliament and of the Council, C(2016) 8471, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016D2297&from=EN

COMMISSION STAFF WORKING PAPER. EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT, Brussels, 25.1.2012, SEC(2012) 73 final

COMMISSION STAFF WORKING PAPER. Impact Assessment, Brussels, 25.1.2012, SEC(2012) 72 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, Brussels, 24.6.2020, COM(2020) 264 final, https://ec.europa.eu/info/sites/info/files/1_en_act_part1_v6_1.pdf

COMMUNICATION FROM THE COMMISSION 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

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/2012/09 final */

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. Towards a common European data space. Brussels, 25.4.2018 COM(2018) 232 final, https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-232-F1-EN-MAIN-PART-1.PDF

COMPARATIVE STUDY ON DIFFERENT APPROACHES TO NEW PRIVACY CHALLENGES, IN PARTICULAR IN THE LIGHT OF TECHNOLOGICAL DEVELOPMENTS, Final Report, January 2010, http://ec.europa.eu/justice/data-protection/document/studies/files/new_privacy_challenges/final_report_en.pdf

Decision of European Commission from 24.03.2004 r. in T-201/04 case, Microsoft

EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield, http://europa.eu/rapid/press-release_IP-16-216_en.htm

European Commission - Press release, Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising, Brussels, 20 March 2019, https://europa.eu/rapid/press-release_IP-19-1770_en.htm

European Commission - Press release, Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service, Brussels, 27 June 2017, https://europa.eu/rapid/press-release_IP-17-1784_en.htm
European Commission - Press release, Antitrust: Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google's search engine, Brussels, 18 July, 2018, https://europa.eu/rapid/press-release_IP-18-4581_en.htm
European Commission - Press release, Antitrust: Commission sends Statement of Objections to Google on comparison shopping service; opens separate formal investigation on Android, Brussels, 15 April 2015, https://europa.eu/rapid/press-release_IP-15-4780_en.htm
European Commission - Press release, http://europa.eu/rapid/press-release_IP-18-4581_en.htm, Brussels, 18 July 2018
EUROPEAN COMMISSION - PRESS RELEASE. Data Protection: Europeans share data online, but privacy concerns remain – new survey, Brussels, 16 June 2011, http://europa.eu/rapid/press-release_IP-11-742_en.pdf
European Commission, European Commission Launches EU-U.S. Privacy Shield: Stronger Protection For Transatlantic Data Flows (2016) http://europa.eu/rapid/press-release_IP-16-2461_en.htm
European Commission, Mergers: Commission Approves Acquisition Of Linkedin By Microsoft, Subject To Conditions (2016), http://press-release_IP-16-4284_en.htm
European Commission, Mergers: Commission Approves Acquisition Of Whatsapp By Facebook (2014), http://europa.eu/rapid/press-release_IP-14-1088_en.htm
European Commission, Mergers: Commission Clears Proposed Acquisition Of DoubleClick By Google (2008), http://europa.eu/rapid/press-release_IP-08-426_en.htm
European Commission, State Aid: Commission Extends Information Enquiry On Tax Rulings Practice To All Member States (2014), http://europa.eu/rapid/press-release_IP-14-2742_nl.htm
Factsheet on ECJ's ruling on the 'right to be forgotten' in relation to online search engines, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf
Fair Taxation: Commission presents new measures against corporate tax avoidance, http://europa.eu/rapid/press-release_IP-16-159_en.htm
Guidelines on Consent under Regulation 2016/679 (wp259rev.01), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051
How does the data protection reform strengthen citizens' rights?, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf
How will the data protection reform affect social networks?, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf
How will the EU's data protection reform benefit European businesses? http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/7_en.pdf
How will the EU's data protection reform make international cooperation easier?, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/5_en.pdf
How will the EU's data protection reform simplify the existing rules? http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/6_en.pdf
How will the EU's data protection reform strengthen the internal market?, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/4_en.pdf
How will the EU's reform adapt data protection rules to new technological developments?, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/8_en.pdf

NEW CHALLENGES TO DATA PROTECTION. FINAL REPORT. Executive Summary, DK/IB 100115, http://ec.europa.eu/justice/data-protection/document/studies/files/new_privacy_challenges/final_report_summary_en.pdf

Notice to stakeholders, Withdrawal of the United Kingdom and EU rules in the field of data protection, Brussels, 6 July 2020, https://ec.europa.eu/info/sites/info/files/brexit_files/info_site/data_protection_en.pdf

RECOMMENDATION No. R (87) 15, OF THE COMMITTEE OF MINISTERS TO MEMBER STATES REGULATING THE USE OF PERSONAL DATA IN THE POLICE SECTOR, Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies, http://ec.europa.eu/justice/data-protection/law/files/coe-fra-rpt-2670-en-471.pdf

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS based on Article 29 (2) of the Council Framework Decision of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, /* COM/2012/012 final */

Report from the Commission, First Report on the implementation of the Data Protection Directive (95/46/EC), COM/2003/0265 ?nal.

Safe Harbour Decision Implementation Study, April 2004, http://ec.europa.eu/justice/data-protection/document/studies/files/safe-harbour-2004_en.pdf

Special Eurobarometer 431, Data Protection. Summary, June 2015, https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_sum_en.pdf

Speech by Commissioner Jourová: The future of U.S.-EU data transfer arrangements at the Brookings Institution, SPEECH/15/6104, http://ec.europa.eu/justice/data- protection/document/review2012/com_2012_11_en.pdf Speech by Commissioner Jourová: The future of U.S.-EU data transfer arrangements at the Brookings Institution, SPEECH/15/6104, http://ec.europa.eu/justice/data- protection/document/review2012/com_2012_11_en.pdf Speech by Commissioner Jourová: The future of U.S.-EU data transfer arrangements at the Brookings Institution, SPEECH/15/6104, http://ec.europa.eu/justice/data- protection/document/review2012/com_2012_11_en.pdf

Speech by Commissioner Jourová: The future of U.S.-EU data transfer arrangements at the Brookings Institution, SPEECH/15/6104, http://ec.europa.eu/justice/data- protection/document/review2012/com_2012_11_en.pdf

Study on the economic benefits of privacy enhancing technologies (PETs), http://ec.europa.eu/justice/data- Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services/q-and-a protection/document/studies/files/final_report_pets_16_07_10_en.pdf

Sweeps - Coordinated Control Actions - European Commission http://ec.europa.eu/consumers/enforcement/sweeps/index_en.htm

The Court of Justice of the EU and the "Right to be Forgotten", http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_rtbf_mythbusting_en.pdf

What Commission proposals on data protection DO and DON'T mean, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_mythbusting_2012_en.pdf

Why do we need an EU data protection reform?, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf

United Nations

International Covenant on Civil and Political Rights, http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

Universal declaration of human rights, http://www.un.org/Overview/rights.html

OECD

Digital Security Risk Management for Economic and Social Prosperity. OECD Recommendation and Companion Document, 2015, http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf

OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, 2007, http://www.oecd.org/internet/ieconomy/38770483.pdf

OECD. Industry Self-Regulation: Role and Use in Supporting Consumer Interests. Organization for Economic Cooperation and Development, March 2015.

THE OECD PRIVACY FRAMEWORK, 2013, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

United States

1974 Privacy Act, 5 U.S.C. § 552a (2000)

Comments Of The Electronic Privacy Information Center To The Federal Trade Commission In The Matter Of Google, Inc. FTC File No. File No. 121 0120 (Federal Trade Commission 2013) https://epic.org/apa/comments/EPIC-FTC-Google-Antitrust-Comments.pdf

Electronic Communications Privacy Act of 1986 (ECPA), An Act to amend title 18, United States Code, with respect to the interception of certain communications, other forms of surveillance, and for other purposes, https://www.govinfo.gov/content/pkg/STATUTE-100/pdf/STATUTE-100-Pg1848.pdf

Federal Trade Commission Summary of Rule 16 CFR Part 312 COPPA: www.ftc.gov/enforcement/rules/rulemaking-regulatory-reformproceedings/childrens-online-privacy-protection-rule

Federal Trade Commission, 'Statement Of Federal Trade Commission Concerning Google/Doubleclick FTC File No. 071-0170' (2007), https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf

Federal Trade Commission. "Protecting Consumers in an Era of Rapid Change." March 2012. www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumerprivacy-era-rapid-change-recommendations/120326privacyreport.pdf

H.R.1428 - Judicial Redress Act of 2015, https://www.congress.gov/bill/114th-congress/house-bill/1428

H.R.3261 – Stop Online Piracy Act; House Judiciary Committee; October 26, 2011, http://www.webcitation.org/63oCICqjh

H.R.387 - Email Privacy Act

Letter From Jessica L. Rich, Director of the Federal Trade Commission Bureau of Consumer Protection, to Erin Egan, Chief Privacy Officer, Facebook, and to Anne Hoge, General Counsel, WhatsApp Inc., Reminding Both Firms That WhatsApp Must Continue To Honor Its Promises To Consumers With Respect to the Limited Nature of the Data It Collects, Maintains, and Shares With Third Parties, April 10, 2014, https://www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappltr.pdf

Press Release: Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises, November 29, 2011, https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep

Report to the Chairman, Committee on Energy and Commerce, House of Representatives, INTERNET PRIVACY - Additional Federal, Authority Could Enhance Consumer Protection and Provide Flexibility, January 2019, https://www.gao.gov/assets/700/696437.pdf

Sherman Act, at 15 U.S.C. § 2.

Summary: H.R.387 — 115th Congress (2017-2018), https://www.congress.gov/bill/115th-congress/house-bill/387

The White House - Office of the Press Secretary, We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online. Internet Advertising Networks Announces Commitment to "Do-Not-Track" Technology to Allow Consumers to Control Online Tracking, February 2012, https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights

UNITED STATES OF AMERICA FEDERAL TRADE COMMISSION, DOCKET NO. C-0923184, https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf

UNITED STATES OF AMERICA FEDERAL TRADE COMMISSION, FILE NO 092 3184, https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf

USA Freedom Act, To reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes, https://www.govinfo.gov/content/pkg/PLAW-114publ23/html/PLAW-114publ23.htm

France

Escape Presse, Création d'une taxe sur les services numériques, July 22, 2020, http://www.senat.fr/espace_presse/actualites/201904/creation_dune_taxe_sur_les_services_numeriques.html

Other Documents

CROSS-BORDER DATA FLOWS AND PROTECTION OF PRIVACY, March 2010, https://assets.hcch.net/upload/wop/genaff2010pd13e.pdf

Guidelines for the Regulation of Computerized Personal Data Files, Adopted by General Assembly resolution 45/95 of 14 December 1990, http://www.refworld.org/pdfid/3ddcafaac.pdf

Hague Conference on Private International Law, Electronic Commerce and International Jurisdiction (Catherine Kessedjian, ed., 2000), http://www.hcch.net/upload/wop/jdgmpd12.pdf

Hague Conference on Private International Law, Electronic Commerce and the Internet (Press Release Including Conclusions and Recommendations) (Sept. 2, 1999), http://www.hcch.net/index_en.php?act=events.details&year=1999&varevent=63

Hague Conference on Private International Law, Geneva Round Table on Electronic Commerce an Private International Law (Sept. 2, 2001), http://www.hcch.net/upload/wop.press01e.html.

NATIONAL ACADEMY OF SCIENCES NATIONAL RESEARCH COUNCIL, GLOBAL NETWORKS AND LOCAL VALUES: A COMPARATIVE LOOK AT GERMANY AND THE UNITED STATES (2001), http://www.nap.edu/catalog/10033.html.

Securities and Exchange Commission , Press Release - Facebook to Pay $100 Million for Misleading Investors About the Risks It Faced From Misuse of User Data, Jul 24, 2019, https://www.sec.gov/news/press-release/2019-140

SIGNALS INTELLIGENCE REFORM 2015. ANNIVERSARY REPORT, http://icontherecord.tumblr.com/ppd-28/2015/overview

Statement by Antonio TAJANI, EP President on the Facebook data crisis, 21/03/2018, https://multimedia.europarl.europa.eu/en/statement-tajani-cambridge-analytica-issue_I152975-V_v

Bibliography

A

Aarnio A., Essays on the Doctrinal Study of Law, Springer 2011

Aarnio A., Legal Point of View. Six Essays on Legal Philosophy, Helsinki 1978

Aarnio A., Reason and Authority. A Treatise on the Dynamic Paradigm of Legal Dogmatics, Cambridge 1997

Aarnio R., Data Protection Reform – are we ready? - 25 years of Data Protection in Finland, a presentation from KnowRight2012, Helsinki

Abrams L., 533 million Facebook users' phone numbers leaked on hacker forum, April 3, 2021, https://www.bleepingcomputer.com/news/security/533-million-facebook-users-phone-numbers-leaked-on-hacker-forum/

Acohido B., Microsoft apologizes for violating EU antitrust order, March 6, 2013, https://eu.usatoday.com/story/tech/2013/03/06/microsoft-eu-antitrust-fine-731-million/1969007/

Aguiló-Regla J., Introduction: Legal Informatics and the Conceptions of the Law, [in:] Benjamins V.R., Casanovas P., Breuker J., Gangemi A. (eds) Law and the Semantic Web. Lecture Notes in Computer Science, vol 3369. Springer, Berlin 2005

Allen A., Coercing Privacy, 40 WILLIAM & MARY L. REV. 723 (1999)

Alvar C.H. Freude & Trixy Freude, Echoes of History: Understanding German Data Protection, Bertelsmann Foundation Newpolitik. October 2016, https://www.bfna.org/research/echos-of-history-understanding-german-data-protection/

Ananny M., Crawford K., Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability, New Media & Society, 2016, https://doi.org/10.1177/14614448166766451

Arrington M., 85% of college students use Facebook, TechCrunch, 2007, http://www.techcrunch.com/2005/09/07/85-of-college-students-use-facebook

Auchard E., Germany takes on Facebook in competition probe, March 2, 2016, https://www.reuters.com/article/us-facebook-germany-dataprotection-idUSKCN0W40Y7

Ausloos, J., The 'Right to be Forgotten' – Worth remembering?, Computer Law & Security Review, Volume 28, Issue 2, April 2012

B

Ball, J. NSA monitored calls of 35 world leaders after US official handed over contacts, 25 October 2013, http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls/

Banisar D., National Comprehensive Data Protection/Privacy Laws and Bills 2019 (August 1, 2019), https://ssrn.com/abstract=1951416

Barbas, The Death of the Public Disclosure Tort: A Historical Perspective, 22 Yale J.L. & Human. 171 (2010) and New York Times Co. v. Sullivan, 376 U.S. 254 (1964)

Barnes, S. B., A privacy paradox: Social networking in the United States, First Monday, Volume 11, Number 9 - 4 September 2006, http://firstmonday.org/ojs/index.php/fm/article/viewArticle/1394/1312%2523

Barzallo, J. Luiz, Valdes, J. Tellez, Olmedo, P. Reyes, Fernandez, Y. Amoroso (ed.), XVI Congreso Iberoamericano de Derecho e Informatica, Quito 2012,

Beaney William M., The Right to Privacy and American Law, 31 Law & Contemp. Probs. 253, 255 (1966)

Beck, U., Sorensen, M. P., Christiansen, A. (editors), An Introduction to the Theory of Second Modernity and the Risk Society, New York 2013
Bellia P. L., Federalization in Information Privacy Law, 118 YALE L.J. 868 (2009).
Benjamins, V. R. (ed.), Law and the Semantic Web, LNAI 3369, Berlin 2005
Bennet, C. J., Regulating Privacy. Data Protection and Public Policy in Europe and the United States, New York 1992
Barret B., WHAT WOULD REGULATING FACEBOOK LOOK LIKE?, March 2018, https://www.wired.com/story/what-would-regulating-facebook-look-like/?CNDID=24507553&mbid=nl_032218_daily_list1_p4
Bhardwaj, K., Right to Privacy. Emerging Dimension of Personal Liberty, New Delhi 2013
Bing J., Computers and Law: Some beginnings, Scherpunktthema, it 2/2007
Bing J., Information Law?, Journal of Media Law and Pratice, 1981, vol. 2, no. 3
Blume, P., Data Protection and Privacy – Basic Concepts in a Changing World, Scandinavian Studies in Law, Volume 56, ICT Legal Issues, October 2010
Blume, P., Protection of Informational Privacy, Copenhagen 2002
Bodnar K., The Ultimate Glossary: 120 Social Media Marketing Terms Explained, HUBSPOT, Dec 30, 2011, http://blog.hubspot.com/blog/tabid/6307/bid/6126/The-Ultimate-Glossary-120-Social-Media-MarketingTerms-Explained.aspx.
Bodoni S., Facebook Quizzed by Watchdog for Listening to Users' Chats, https://www.bloomberg.com/news/articles/2019-08-14/facebook-quizzed-by-privacy-watchdog-for-listening-to-user-audio, August 14, 2019
Bodoni S., Stearns J., Zuckerberg Asked to Explain Himself in European Parliament, April 12, 2018, https://www.bloomberg.com/news/articles/2018-04-12/zuckerberg-asked-to-explain-himself-in-european-parliament
Boyd D. M., Facebook's privacy trainwreck: Exposure, invasion, and social convergence, International Journal of Research Into New Media Technologies, 14, 2009
Braman S., Privacy by design: Networked computing, 1969–1979. New Media & Society, 14(5), 2012, https://doi.org/10.1177/1461444811426741
Brand R. A., Intellectual Property, Electronic Commerce and the Preliminary Draft Hague Jurisdiction and Judgments Convention, 62 U. PITT. L. REV. 581, 594–97 (2001)
Brandimarte L., Acquisti A., Loewenstein G., Privacy concerns and information disclosure: An illusion of control hypothesis. In Proceeding of the 9th Workshop on the Economics of Information Security (WEIS 2010), June 2010.
Brown J. J., From Friday to Sunday: The hacker ethic and shifting notions of labour, leisure and intellectual property. Leisure Studies, 27, 2008
Brustein, J., The Companies' Lines on Prism, June 07, 2013, http://www.businessweek.com/articles/2013-06-07/the-companies-lines-on-prism
Burke M., Marlow C., Lento T., Feed me: Motivating newcomer contribution in social network sites, [in:] Proceedings of the 27th International Conference on Human Factors in Computing Systems (pp. 945–995), 2009, New York, NY: ACM.
Burnside Alec J., 'No Such Thing As A Free Search: Antitrust And The Pursuit Of Privacy Goals' [2015] Competition Policy International https://www.competitionpolicyinternational.com/assets/Uploads/BurnsideCPI-May-15.pdf
Burri M., Schär R., The Reform of the EU Data Protection Framework: Outlining Key Changes and AssessingTheir Fitness for a Data-Driven Economy, Journal of Information Policy, vol. 6, 2016, https://www.academia.edu/34683558/The_Reform_of_the_EU_Data_Protection_Framework_Outlining_Key_Changes_and_Assessing_Their_Fitness_for_a_Data-Driven_Economy_Author_s?email_work_card=view-paper

Busvine D., Facebook's data gathering hit by German anti-trust clampdown, February 2019, https://www.reuters.com/article/us-google-lawsuit-illinois/u-s-judge-dismisses-suit-versus-google-over-facial-recognition-software-idUSKCN1OT001

Buttarelli G., The urgent case for a new ePrivacy law, October 19, 2018, https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_en

Byers A, How a telecom-tech alliance wiped out FCC's privacy rules, Politico, 03/31/2017, http://www.politico.com/story/2017/03/broadband-data-victory-republicans-236760

Bygrave, L. A., Bekken A. G. B., (ed.), Yulex 2004, Oslo

Bygrave, L. A., Privacy and Data Protection in an International Perspective, Scandinavian Studies in Law, Volume 56, ICT Legal Issues, October 2010

Bygrave, L. A., Data Privacy Law. An International Perspective, Oxford 2014

Bygrave, L. A., Data Protection Law. Approaching Its Rationale, Logic and Limits, London 2002

C

Calo R., Digital Market Manipulation, 82 GEO. WASH. L. REV. 995 (2014)

Calo R., Privacy and Markets: A Love Story (August 6, 2015). Notre Dame Law Review, Forthcoming; University of Washington School of Law Research Paper No. 2015-26. Available at SSRN: http://ssrn.com/abstract=2640607 or http://dx.doi.org/10.2139/ssrn.2640607

Calo R., Privacy and Markets: A Love Story (August 6, 2015). Notre Dame Law Review, Forthcoming; University of Washington School of Law Research Paper No. 2015-26. Available at SSRN: http://ssrn.com/abstract=2640607 or http://dx.doi.org/10.2139/ssrn.2640607

Calo R., Rosenblat A., The Taking Economy: Uber, Information, and Power, Columbia Law Review, Vol. 117, 2017; University of Washington School of Law Research Paper No. 2017-08, https://ssrn.com/abstract=2929643

Carey, Peter., Data Protection. A Practical Guide to UK and EU Law, 3rd Edition, Oxford 2011

Casagrande S., WhatsApp with your Facebook data?, February 20, 2014, https://www.dw.com/en/whatsapp-with-your-facebook-data/a-17446624

Casert R., Google Wins Case in E.U. Over 'Right to Be Forgotten' Rules, 24 September, 2019, https://time.com/5684763/google-european-union-right-to-be-forgotten/

Cate, F., Dempsey, J., Rubinstein, I., Systematic government access to private-sector data, International Data Privacy Law, volume 2, number 4, 2012,

Cavoukian A., Privacy as a Fundamental Human Right vs. an Economic Right: An Attempt at Conciliation, 1999, http://www.ontla.on.ca/library/repository/mon/10000/211714.pdf

Cavoukian, A., El Emam, K., Introducing Privacy-Protective Surveillance: Achieving Privacy and Effective Counter-Terrorism, September 2013, http://www.privacybydesign.ca/content/uploads/2013/12/pps.pdf

Cavoukian, A., Privacy by Design. From Rhetoric to Reality, https://www.privacybydesign.ca/content/uploads/2014/01/PbDBook-From-Rhetoric-to-Reality.pdf

Cavoukian, A., Reed, D., Big Privacy: Bridging Big Data and the Personal Data Ecosystem Through Privacy by Design, 2013, https://www.ipc.on.ca/site_documents/PbDBook-From-Rhetoric-to-Reality-ch3.pdf

Cheik-Hussein M., Facebook could be forced to remove content globally in EU ruling, 4 October, 2019, https://www.adnews.com.au/news/facebook-could-be-forced-to-remove-content-globally-in-eu-ruling

Christl W., Corporate Surveillance in Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions, June 2017, http://crackedlabs.org/en/corporatesurveillance

Christl W., How Companies Use Personal Data Against People. Automated Disadvantage, Personalized Persiasion, and the Societal Ramifications of Commercial Use of Personal Information, 2017, https://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf

Christl W., Spiekermann S., Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy, Facultas, Vienna 2016, http://crackedlabs.org/en/networksofcontrol

Cimpanu C., 51 tech CEOs send open letter to Congress asking for a federal data privacy law, September 10, 2019, https://www.zdnet.com/article/51-tech-ceos-send-open-letter-to-congress-asking-for-a-federal-data-privacy-law/

Cimpanu C., GAO gives Congress go-ahead for a GDPR-like privacy legislation, February 15, 2019, https://www.zdnet.com/article/gao-gives-congress-go-ahead-for-a-gdpr-like-privacy-legislation/

Cimpanu C., Russian military moves closer to replacing Windows with Astra Linux, Nay 30, 2019, https://www.zdnet.com/article/russian-military-moves-closer-to-replacing-windows-with-astra-linux/

Ciancaglini V., Balduzzi M., McArdle R., Rösler M., Below the Surface: Exploring the Deep Web, 2015, https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf

Clark M., The Facts on News Reports About Facebook Data, April 6, 2021, https://about.fb.com/news/2021/04/facts-on-news-reports-about-facebook-data/

Colangelo G., Maggiolino M., Data Protection In Attention Markets: Protecting Privacy Through Competition? [2017] The Social Science Research Network Electronic Paper Collection, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2945085

Constine J., Facebook Stops Irresponsibly Defaulting Privacy Of New Users' Posts To "Public", Changes To"Friends", 2014, https://techcrunch.com/2014/05/22/sometimes-less-open-is-more/

Cox J., The Dark Web as You Know It Is a Myth, June 18, 2015, https://www.wired.com/2015/06/dark-web-know-myth/

Cornelius, I., Information policies and strategies, London 2010

Cotterrell, R., The Sociology of Law. An Introduction, 2nd Edition, London 1992

Crane, D. A., Search Neutrality and Referral Dominance, [in:] Journal of Competition Law & Economics, 8(3), p. 459, http://www.theregister.co.uk/2012/05/21/joaquin_almunia_google_statement/

Crain M., The limits of transparency: Data brokers and commodification, New Media & Society, 2016, https://doi.org/10.1177/1461444816657096

Czarnecki J., Blockchains and Personal Data Protection Regulations Explained, https://www.coindesk.com/blockchains-personal-data-protection-regulations-explained/

D

Dallison P., New Danish PM wants Vestager to stay as commissioner, June 26, 2019, https://www.politico.eu/article/new-danish-pm-wants-vestager-to-stay-as-commissioner/

Dallison P., Trump: 'Europe treats us worse than China', June 26, 2019, https://www.politico.eu/article/trump-europe-treats-us-worse-than-china/

Daniels N., Reflective Equilibrium, The Stanford Encyclopedia of Philosophy (Spring 2011 Edition), E. N. Zalta (ed.), http://plato.stanford.edu/archives/spr2011/entries/reflectiveequilibrium

Daskal J., A European Court Decision May Usher In Global Censorship, 3 October, 2019, https://slate.com/technology/2019/10/european-court-justice-glawischnig-piesczek-facebook-censorship.html

Debatin B., Lovejoy J. P., Horn A., Hughes B. N., Facebook and online privacy: Attitudes, behaviors, and unintended consequences, Journal of Computer-Mediated Communication, 15, 2009

De Brusser, E., Data Protection in EU and US Criminal Cooperation, Antwerp 2009

de Búrca G., 'The Drafting of the European Union Charter of Fundamental Rights', 26 European Law Review 1 (2001)

de Búrca G., AFTER THE EU CHARTER OF FUNDAMENTAL RIGHTS: THE COURT OF JUSTICE AS A HUMAN RIGHTS ADJUDICATOR?, p. 169, http://www.maastrichtjournal.eu/pdf_file/ITS/MJ_20_02_0168.pdf

de Búrca, Gráinne, AFTER THE EU CHARTER OF FUNDAMENTAL RIGHTS: THE COURT OF JUSTICE AS A HUMAN RIGHTS ADJUDICATOR?, 2013, http://www.maastrichtjournal.eu/pdf_file/ITS/MJ_20_02_0168.pdf

de Leeuw K., Bergstra J., The History of Information Security. A Comprehensive Handbook, Amsterdam 2007

de Montjoye Y., C. A. Hidalgo, M. Verleysen & V. D. Blondel, Unique in the Crowd: The privacy bounds of human mobility, Scientific Reports 3, Article number: 1376 (2013), http://www.nature.com/articles/srep01376

De Mooy M., Center for Democracy and Technology, Rethinking Privacy Self-Management and Data Sovereignty in the Age of Big Data. Considerations for Future Policy Regimes in the United States and the European Union, 2017, https://cdt.org/files/2017/04/Rethinking-Privacy_2017_final.pdf

Desjardins J., How Google retains more than 90% of market share, April 23, 2018, https://www.businessinsider.com/how-google-retains-more-than-90-of-market-share-2018-4?r=US&IR=T

Dharmapurikar, M. L., Human Rights, Power and Non-Governmental Action, New Delhi 2013

Diffie, W., Landau, S., Privacy on the Line. The Politics of Wiretapping and Encryption. Updated and Expanded Edition, Boston 2007

Dinwoodie G. B., Developing a Private International Intellectual Property Law: The Demise of Territoriality?, 51 WM. & MARY L. REV. 711, 785 (2009)

Dixon, H., Warman, M., Google gets 'right to be forgotten' requests hours after EU ruling, May 14, 2014, http://www.telegraph.co.uk/technology/google/10832179/Google-gets-right-to-be-forgotten-requests-hours-after-EU-ruling.html

Domonoske C., Mark Zuckerberg Tells Senate: Election Security Is An 'Arms Race', April 2018, https://www.npr.org/sections/thetwo-way/2018/04/10/599808766/i-m-responsible-for-what-happens-at-facebook-mark-zuckerberg-will-tell-senate?t=1549538389858

Donlan, Sean Patrick, Urscheler, Lukas Heckendorn (editors), Concepts of Law. Comparative, Jurisprudential, and Social Science Perspectives, Dorchester 2014

Donni D., Machado G., Tsiaras Ch., Stiller B., Schengen Routing: A Compliance Analysis, https://files.ifi.uzh.ch/CSG/staff/doenni/extern/publications/Schengen_Routing_A_Compliance_Analysis_AIMS_2015.pdf

Duggan, M. A., Law and the Computer. A KWIC Bibliography, Macmillan Information, New York 1973.

Dutta, Soumitra, Dutton W.H., Law G., The New Internet World: Perspective on Freedom of Expression, Privacy, Trust and Security. April 2011. http://ssrn.com/abstract=1916005

Dwork C., Differential Privacy, Microsoft Research, http://research.microsoft.com/pubs/64346/dwork.pdf

E

Egwuonwu B., What Is Mass Surveillance And What Does It Have To Do With Human Rights?, April 2016, https://rightsinfo.org/explainer-mass-surveillance-human-rights/

Eliantonio M., Galli F., Schaper M., A Balanced Data Protection in the EU: Conflicts and Possible Solutions: Editorial, Maastricht Journal of European and Comparative Law 2016, https://www.academia.edu/27525378/A_Balanced_Data_Protection_in_the_EU_Conflicts_and_Possible_Solutions_Editorial?email_work_car

Enberg J., Global Digital Ad Spending 2019. Digital Accounts for Half of Total Media Ad Spending Worldwide. March 28, 2019, https://www.emarketer.com/content/global-digital-ad-spending-2019

F

Faull J., Nikpay A., 'The EU Law Of Competition' 6th edn, Oxford University Press 2014

Feiner L., Google cut its lobbying spending nearly in half in 2019, while Facebook took the lead, January 22, 2020, https://www.cnbc.com/2020/01/22/how-much-google-facebook-amazon-and-apple-spent-on-lobbying-in-2019.html

Ferrajoli L., Fundamental Rights, International Journal for the Semiotics of Law, Volume 14 (2001)

Field J. Social Capital, New York 2003

Fingas J., Facebook shared user data with 52 tech companies, June 2018, https://www.engadget.com/2018/06/30/facebook-shared-user-data-with-52-tech-companies/?sr_source=Twitter&guccounter=1

Fingas J., Google, Intel and Microsoft form data protection consortium. They want to keep data safe even while you're using it, August 21, 2019, https://www.engadget.com/2019/08/21/confidential-computing-consortium/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmZpLw

Fischer-Hübner S., Hoofnagle C., Krontiris I., Rannenberg K., Waidner M., Online Privacy: Towards Informational Self-Determination on the Internet (August 29, 2011). Dagstuhl Manifestos, Vol. 1, Issue 1, 2011, https://ssrn.com/abstract=2468200

Fletcher D., Friends (and moms) without borders, Time, 2010, http://www.time.com/time/video/player/0,32068,86888223001_1990764,00.html

Floridi L., (editor),Protection of Information and the Right to Privacy – A New Equilibrium?, Oxford 2014

Fox Ch., Google shuts failed social network Google+, April 2, 2019, https://www.bbc.com/news/technology-47771927

Forbath T., Morey T., Schoop A., Customer Data: Designing for Transparency and Trust, Harvard Business Review, May 2015. https://hbr.org/2015/05/customer-datadesigning-for-transparency-and-trust

Frank H. G. (ed.), KYBERNETISCHE MASCHINEN, 1964.

Frier S., Facebook Paid Contractors to Transcribe Users' Audio Chats, https://www.bloomberg.com/news/articles/2019-08-13/facebook-paid-hundreds-of-contractors-to-transcribe-users-audio, August 13, 2019

Funta R., Facebook from competition law perspective, In. Justičná revue, No. 1., 2018

G

Galindo F. (ed.), El derecho de la sociedad en red, Zaragoza 2013

Gandy Jr. O. H., Engaging Rational Discrimination: Exploring Reasons for Placing Regulatory Constraints on Decision Support Systems, 12 Ethics & Info. Tech. 29, 37-39 (2010).

Garfinkel, S., Database Nation 4-5 (2000)

Gerety T., Redefining Privacy [in:] Harvard Civil Rights-Civil Liverties Law Review, vol 12, number 2, 1977

Gibbs S., Gmail does scan all emails, new Google terms clarify, April 15, 2014, https://www.theguardian.com/technology/2014/apr/15/gmail-scans-all-emails-new-google-terms-clarify

Gilead, A., A Human Argument for Personal Identity, Int Ontology Metaphysics (2008)

Glaser A., Marc Benioff Says Companies Buy Each Other for the Data, And The Government Isn't Doing Anything About It' Recode (2016), https://www.recode.net/2016/11/15/13631938/benioff-salesforce-data-government-federal-trade-commission-ftc-linkedin-microsoft

Glinter E., The Future According to Stanisław Lem, September 12, 2014, https://www.theparisreview.org/blog/2014/09/12/the-future-according-to-stanislaw-lem/

Goldsmith, Jack, Wu, Tim, Who Controls the Internet? Illusions of the Borderless World, Oxford 2008

Gonie J., The EU's Proposed Data Protection Regulation: Microsoft's Position, March 16, 2012, https://blogs.microsoft.com/eupolicy/2012/03/16/the-eus-proposed-data-protection-regulation-microsofts-position/

Gonzalez Fuster G., The Emergence of Personal Data Protection as a Fundamental Right of the EU, Brussels 2014

Goodin D., Facebook suspends tens of thousands of apps in ongoing privacy investigation, 21 September, 2019, https://arstechnica.com/information-technology/2019/09/facebook-suspends-tens-of-thousands-of-apps-in-ongoing-privacy-investigation/

Goold, B. J., Lazarus, L. (editors), Security and Human Rights, Oxford 2007

Graef I., 'Beyond Compliance: How Privacy And Competition Can Be Mutually Reinforcing', Computers, Privacy & Data Protection Conference (2017). https://www.youtube.com/watch?v=Af1qLye_-Ok

Graham, M., Dutton, W. H. (editors), Society & the Internet. How Networks of Information and Communication are Changing our Lives, Oxford 2014

Greenberg A., Meet 'Project Zero,' Google's Secret Team of Bug-Hunting Hackers, July 15, 2014, https://www.wired.com/2014/07/google-project-zero/

Greenstein, S. (editor), Vem reglerar informationssamhallet?, Stockholm 2010

Grossman, L., The Secret Web: Where Drugs, Porn and Murder Live Online, November 11, 2013, http://time.com/630/the-secret-web-where-drugs-porn-and-murder-live-online/

Guarascio F., EU digital tax plan flounders as states ready national moves, November 6, 2018, https://www.reuters.com/article/us-eu-tax-digital/eu-digital-tax-plan-flounders-as-states-ready-national-moves-idUSKCN1NB15F

Guthwirth S., Leenes R., De Hert P. (eds.), Data Protection on the Move. Current Developments in ICT and Privacy/Data Protection, London 2016

Gutwirth, S., Poullet, Y., de Hert, P., de Terwangne, C., Nouwt, S. (editors), Reinventing Data Protection?, Springer 2009

Gutwirth, S., Leenes R., De Hert P. (eds.), Reforming European Data Protection Law, London 2015

Guynn J., Mark Zuckerberg: Whatsapp Worth Even More Than $19 Billion Los Angeles Times (2014), http://articles.latimes.com/2014/feb/24/business/la-fi-tn-mark-zuckerberg-whatsapp-worth-even-more-than-19-billion-20140224

H

Haber S.; Stornetta, Scott (January 1991), "How to time-stamp a digital document", Journal of Cryptology. 3 (2)

Halpin A., The Methodology of Jurisprudence: Thirty Years Off the Point. Canadian Journal of Law and Jurisprudence, Vol. 19, pp. 67-105, 2006. Available at SSRN: http://ssrn.com/abstract=880803

Hart H. L. A., The Concept of Law, 2nd Edition, Oxford 1994
Hartzog W., Privacy and the Dark Side of Control. The Institute of Art and Ideas, Sept 4, 2017, https://iainews.iai.tv/articles/privacy-the-dark-side-of-control-auid-882
Haupt F., Sag mir, wo du stehst und wohin du gehst, FRANKFURTER ALLGEMEINE ZEITUNG, Mar. 20, 2010
Hern A., Twitter hides Donald Trump tweet for 'glorifying violence', 29 May, 2020, https://www.theguardian.com/technology/2020/may/29/twitter-hides-donald-trump-tweet-glorifying-violence
Herrman C. S., Fundamentals of Methodology Part III: The Meaning of Meaning (May 5, 2009). Available at SSRN: http://ssrn.com/abstract=1399550 or http://dx.doi.org/10.2139/ssrn.1399550
Hildebrandt M., Gutwirth S. (eds.), Profiling the European Citizen. Cross-Disciplinary Perspectives, Springer 2008
Hiselius P., ICT/Internet and the Right to Privacy, Scandinavian Studies in Law, Volume 56, ICT Legal Issues, October 2010
Holmes A., 533 million Facebook users' phone numbers and personal data have been leaked online, April 3, 2021, https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4?r=US&IR=T
Howe W., An anecdotal history of the people and communities that brought about the Internet and the Web, A Brief History of the Internet, Sept. 13, 2012, http://walthowe.com/navnet/history.html.
Hsu J., Why the Military Can't Quit Windows XP, June 4, 2018, https://slate.com/technology/2018/06/why-the-military-cant-quit-windows-xp.html
Humphries D., US Attitudes Toward the 'Right to Be Forgotten', Software Advice, September 2014, www.softwareadvice.com/security/industryview/right-to-be-forgotten-2014/
Huxtinx P., 'EU Data Protection Law: The Review Of Directive 95/46/EC And The Proposed General Data Protection Regulation' http://www.statewatch.org/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf

I

Ippel P., de Heij G., Crouvers B. (eds), Privacy Disputed, Den haag 1995

J

Jaspers R., When data travels - The Commission's objective of making EU data protection travel across the Atlantic, February 2016, https://www.academia.edu/22343341/Robbert_Jaspers_When_data_travels_-_The_Commission_s_objective_of_making_EU_data_protection_travel_across_the_Atlantic?email_work_card=view-paper
Jeong S., Zuckerberg struggles to name a single Facebook competitor, April 2018, https://www.theverge.com/2018/4/10/17220934/facebook-monopoly-competitor-mark-zuckerberg-senate-hearing-lindsey-graham
Jones, A., Sufrin, B., EC Competition Law Third Edition, New York 2008

K

Kangas U., Essays in Legal Theory in Honor of Kaarle Makkonen, Vammala 1983
Kanter J., E.U. Parliament Passes Measure to Break Up Google in Symbolic Vote, November 27, 2014, https://www.nytimes.com/2014/11/28/business/international/google-european-union.html
Kelleher D., Murray K., EU Data Protection Law, London 2018
Kemp Ch., 61 Percent of Americans Support the Right to Be Forgotten as California Enacts New Law, September 2014, www.thewhir.com/web-hosting-news/61-percent-americanssupport-right-forgotten-california-enacts-new-law

Kennedy, 'The Myth of Data Monopoly: Why Antitrust Concerns About Data Are Overblown', http://www2.itif.org/2017-data-competition.pdf

Kerr, Orin S., Enforcing Law Online. University of Chicago Law Review, 2007; GWU Law School Public Law Research Paper No. 230; GWU Legal Studies Research Paper No. 230. Available at SSRN: http://ssrn.com/abstract=942859

Kerr, Orin S., The Fourth Amendment and the Global Internet (April 23, 2014). 67 Stanford Law Review 285 (2015); GWU Law School Public Law Research Paper No. 2014-30; GWU Legal Studies Research Paper No. 2014-30. Available at SSRN: http://ssrn.com/abstract=2428042

Kerr, Orin S., Virtual Crime, Virtual Deterrence: A Skeptical View of Self-Help, Architecture, and Civil Liability. Journal of Law, Economics & Policy, Vol. 1, January 2005. Available at SSRN: http://ssrn.com/abstract=605964

Khari J., Intel, Google, Microsoft, and others launch Confidential Computing Consortium for data security, August 21, 2019, https://venturebeat.com/2019/08/21/intel-google-microsoft-and-others-launch-confidential-computing-consortium-for-data-security/

Kirkpatrick D., The Facebook Effect: The Inside Story of the Company That Is Connecting the World, New York 2010

Kirkpatrick M., Facebook's Zuckerberg Says the Age of Privacy is Over, READWRITEWEB, Jan. 9, 2010, http://www.readwriteweb.com/archives/facebooks zuckerberg-says the-age of privacyis ov.php.

Klober R., PERSONLICHKEITSSCHUTZ UND KOMMERZIALISIERUNG, 2007.

Kohnstamm J.: 'Privacy is in motion', https://www.privacyconference2015.org/jacob-kohnstamm-privacy-is-in-motion/

Kokott, Juliane and Sobotta, Christoph, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, http://idpl.oxfordjournals.org/content/3/4/222.full.pdf+html

Kong L., Data Protection and Transborder Data Flow in the European and Global Context, The European Journal of International Law 21, no. 2,2010

Korpisaari, P. (editor), Viestintäoikeuden vuosikurja 2014, Helsinki 2015

Koski H., Solving Structural Competition Problems require Changes in EU Merger Regulation, 23 June 2020, https://www.etla.fi/julkaisut/teknologiajattien-yritysostoihin-puuttuminen-on-rakenteellisten-kilpailuongelmien-ratkaisun-ytimessa/

Krishnamurthy B., Wills C. E., Characterizing privacy in online social networks. In Proceedings of the 1st Workshop on Online Social Networks (WOSN '08), 2008.

Kristol/Montulli, Http State Management Mechanism, RFC Editor, 1997

Kumar M., What is the Deep Web? A first trip into the abyss, May 31, 2012, https://thehackernews.com/2012/05/what-is-deep-web-first-trip-into-abyss.html

L

Lafrance A., Why can't Americans find out what big data knows about them?, May 2014, www.theatlantic.com/technology/archive/2014/05/why-americans-cant-find-outwhat-big-data-knows-about-them/371758/

Lane J., Stodden V., Bender S., Nissenbaum H. (eds.), Privacy, Big Data, and the Public Good: Frameworks for Engagement, Cambridge University Press 2014,https://doi.org/10.1017/CBO9781107590205.004

Langlinais, Alex and Leiter, Brian, The Methodology of Legal Philosophy (September 6, 2013). H. Cappelen, T. Gendler, & J. Hawthorne (eds.), Oxford Handbook of Philosophical Methodology, Forthcoming; U of Chicago, Public Law Working Paper No. 407. Available at SSRN: http://ssrn.com/abstract=2167498

Laudon K. C., Markets and Privacy, Communications of the ACM 39 (9), 1996: 92-104.
Lawler R., Facebook's on-device data sharing program included Huawei, Lenovo. The social network insists any data shared did not go to those companies' servers, June 2018, https://www.engadget.com/2018/06/06/facebook-huawei-lenovo/
Lecher C., France will delay controversial tech tax, January 23, 2020, https://www.theverge.com/2020/1/23/21078574/france-us-digital-tax-deal-negotiations-tariffs-postponed-trump
Lehofer H. P., EuGH: Google muss doch vergessen – das Supergrundrecht auf Datenschutz und die Bowdlerisierung des Internets, E -Comm, 13 May 2014, http://blog.lehofer.at/2014/05/eugh-google-muss-doch-vergessen-das.html
Leiner B. M., Cerf V. G., Clark D., Kahn R. E., Kleinrock L., Lynch D. C., Postel J., Roberts L. G., Wolff S., Brief History of the Internet, 1997, https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf
Leiter, Brian, Beyond the Hart/Dworkin Debate: The Methodology Problem in Jurisprudence. U of Texas Law, Public Law Research Paper No. 34. Available at SSRN: http://ssrn.com/abstract=312781
Leiter, Brian, Why Legal Positivism? (December 10, 2009). U of Chicago, Public Law Working. Available at SSRN: http://ssrn.com/abstract=1521761 or http://dx.doi.org/10.2139/ssrn.1521761
Lenk, C., Hoppe, N., Andorno, R. (editors), Ethics and Law of Intellectual Property. Current Problems in Politics, Science and Technology, Cornwall 2007
Lessig L., CODE: AND OTHER LAWS OF CYBERSPACE, VERSION 2.0 81–82 (2006)
Levmore, S., Nussbaum, M. C. (editors), The Offensive Internet, Cambridge 2010
Levy S., Jeff Bezos Wants Us All to Leave Earth—for Good, 15 October, 2018, https://www.wired.com/story/jeff-bezos-blue-origin/#:~:text=03%3A15%20PM-,Jeff%20Bezos%20Wants%20Us%20All%20to%20Leave%20Earth%E2%80%94for%20Good,humanity%20into%20an%20extraterrestrial%20future.
Liedtke M., Microsoft escalates advertising assault on Google, April 9, 2013, https://news.yahoo.com/microsoft-escalates-advertising-assault-google-131645123--finance.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmZpLw&guce_referrer_sig=AQAAAGD_v63Hkuh55idEUZyaP9mrBfU2e0YtNfUTXe94AB0mBvnOb98DJgzeaA_NrX5sdvEww3VyDBfyWciOydrIjlPK2X6o6UpZRgfFkqm3yvyOEFbNhv_9XYRZaCoUdJlg6ACH3ny4p7WHsL6KKlV5QNt5YkH7nWw0sbwyPJ9hWRel
Liedtke M., Microsoft Skewers Google For Giving Your Personal Data To App Developers, April 9, 2013, https://www.businessinsider.com/microsoft-skewers-google-for-giving-your-personal-data-to-app-developers-2013-4?r=US&IR=T
Lipman M., Facebook Data Antitrust Case Not Overreach, Enforcer Says Law (2017) https://www.law360.com/articles/888145/facebook-data-antitrust-case-not-overreach-enforcer-says
Lloyd, I. J., Information Technology Law, 4th Edition, Oxford 2004
Loevinger, L., Jurimetrics the Next Step Forward. Minnesota Law Review, 33/1949. Wiener, Norbert, The Human Use of Human Beings. Cybernetics and Society, Eyre & Spottiswoode, London 1954.
Lomas N., Europe's top court strikes down flagship EU-US data transfer mechanism, July 16, 2020, https://techcrunch.com/2020/07/16/europes-top-court-strikes-down-flagship-eu-us-data-transfer-mechanism/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAACMjgCXv6mtVr5teCNwNexxrmXPhenHwjs9O4GRUtaMnektTY7jDcaY6E5sLgMSZOsjrsJBamXZqib-KdkdPQ6blpuLEptpE7p0Ue3IssxcIEBRrow0rvvdmTcd5fMEjK9Msu1b7QxMU-GU6mrK9IlKAx8yR3dWXjYt1RtRiVjLc

Lopez-Tarruella, A., Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models, Berlin 2012

Loshin D., Knowledge Integrity: Data Ownership, 2002, http://ori.dhhs.gov/education/products/n_illinois_u/datamanagement/dotopic.html

Lovaszy L., Alvert D., This brilliant Pole predicted algorithmic surveillance, machine learning and even a virus outbreak in Italy, March 29, 2020, https://rmx.news/article/commentary/this-brilliant-pole-predicted-algorithmic-surveillance-machine-learning-and-even-a-virus-outbreak-in-italy

Lucas M., The difference between Bitcoin and blockchain for business, https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-bitcoin-and-blockchain-for-business/

Lumb R., Treat D., Jelf O., EDITING THE UNEDITABLE BLOCKCHAIN. Why distributed ledger technology must adapt to an imperfect world, https://www.accenture.com/t00010101T000000__w__/it-it/_acnmedia/PDF-33/Accenture-Editing-Uneditable-Blockchain.pdf

Lynch M., Predictive Surveillance: Precogs, CATCHEM, and DNA Databases, 18 RISK & REG. 8 (Economic & Soc. Res. Council, London, U.K.), 2009.

Lynskey, O., The Foundation of EU Data Protection Law, Oxford 2015

Lyon, D., The Information Society. Issues and Illusions, Cambridge 1988

M

Mac Sithigh, D., The Mass age of Internet Law, Information & Communications Technology Law, 17:2, 2008

Madden M., Public Perceptions of Privacy and Security in the Post Snowden Era, Pew Research Center, November 2014, www.pewinternet.org/2014/11/12/public-privacy-perceptions/

Magnusson Sjoberg, C. (editor), IT Law for IT Professional – an Introduction, Lund 2005

Majcher, J., Dostęp do urządzeń kluczowych w świetle orzecznictwa antymonopolowego, Warszawa 2005

Makena K., Facebook can be forced to remove content internationally, top EU court rules, 3 October, 2019, https://www.theverge.com/2019/10/3/20896839/facebook-global-takedown-content-ban-austria-modera

Makkonen K., Zur Problematik der juridischen Entscheidung, Turku 1965

Mantelero A., Data protection in a big data society: Ideas for a future regulation, Digital Investigation, November 2015.

Mantelero A., The EU Proposal for a General Protection Regulation and the roots of the 'right to be forgotten', Computer Law & Security Review 29 (2013)

Mantelero A., The Future of Consumer Data Protection in the E.U.: Rethinking the 'Notice and Consent' Paradigm in the New Era of Predictive Analytics, Computer Law & Security Report 30, November 2014.

Markoff J., The tangled history of Facebook. New York Times, 2007, http://www.nytimes.com/2007/08/31/business/worldbusiness/31iht-facebook.5.7340806.html

Markou C., The 'Right to be Forgotten', Ten Reasons Why it Should Be Forgotten, [in:] Gutwirth, S., Leenes, R., de Hert, P. (ed.), Reforming European Data Protection Law, New York 2015

Mathiesen T, Towards a Surveillant Society. The Rise of Surveillance Systems in Europe, Croydon 2013

Matsakis L., THE FTC IS OFFICIALLY INVESTIGATING FACEBOOK'S DATA PRACTICES, March 2018, https://www.wired.com/story/ftc-facebook-data-privacy-investigation/

Maurieni C., Facebook is Deception (Volume One), 2012, http://books.google.fi/books?id=s6TxlJ1v5y4C&printsec=frontcover&dq=Facebook+is+Deception+(Volume+One)&hl=pl&sa=X&ei=7GMKUZDyGInitQaez4DYAQ&ved=0CCwQ6AEwAA

McCullen G., Blockchain & Law in 2017: Finally friends or still foes?, https://medium.com/ipdb-blog/blockchain-and-law-in-2017-f535cb0e06c4

McHangama J., Europe's Freedom of Speech Fail, July 7, 2016, https://foreignpolicy.com/2016/07/07/europes-freedom-of-speech-fail/

Meyer D., EU Parliament calls on Commission to consider Google break-up, November 27, 2014, https://gigaom.com/2014/11/27/eu-parliament-calls-on-commission-to-consider-google-break-up/

Meyer D., Europeans Remain Far from Sold on the Benefits of big data, January 2016. http://fortune.com/2016/01/18/europe-data/

Meyer D., What to Know About 'Freedom From Facebook,' the New Progressive Campaign to Break Up the Social Media Giant, May 2018, http://fortune.com/2018/05/21/facebook-monopoly-breakup-progressive-campaign-ftc/

Meyer-Schonberger V., Delete. The Virtue of Forgetting in the Digital Age, New Jersey 2009

Miąsik D., Skoczny T., Surdek M. (eds), Microsoft – case study. Competition Law on the New Technology Markets, Warsaw 2008

Miles T J., Sunstein C. R., The New Legal Realism. University of Chicago Law Review, Forthcoming; U of Chicago Law & Economics, Olin Working Paper No. 372; U of Chicago, Public Law Working Paper No. 191. Available at SSRN: http://ssrn.com/abstract=1070283

Minkkinen M., Futures of privacy protection: A framework for creating scenarios of institutional change, Futures, Volume 73, October 2015, https://www.sciencedirect.com/science/article/pii/S00163287

Mitchell R., Revised OECD Privacy Guidelines Focus On Accountability, Notification of Breaches, September 16, 2013, http://www.bna.com/revised-oecd-privacy-n17179877087/

Monti G., EC Competition Law (Law in Context), Cambridge 2007

Morozov E., Free Speech and the Internet, INT'L HERALD TRIB., November 2009.

Mozur P., Scott M., Isaac M., Facebook Faces a New World as Officials Rein In a Wild Web, Sept. 17, 2017, https://www.nytimes.com/2017/09/17/technology/facebook-government-regulations.html

Mungan M., Conditional Privacy Rights, April 2016, http://masonlec.org/site/rte_uploads/files/Mungan_Conditional%20Privacy%20Rights.pdf

N

Narayanan A. N., Huey J., Felten E. W., A Precautionary Approach to Big Data Privacy, http://randomwalker.info/publications/precautionary.pdf

Naughton J., 'The goal is to automate us': welcome to the age of surveillance capitalism, January 20, 2019, https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook

Newman L., What Really Caused Facebook's 500M-User Data Leak?, April 6, 2021, https://www.wired.com/story/facebook-data-leak-500-million-users-phone-numbers/

Newton C., The 5 biggest takeaways from Mark Zuckerberg's appearance before the Senate. Congress doesn't understand Facebook — does anyone?, April 2018, https://www.theverge.com/2018/4/10/17222444/mark-zuckerberg-senate-hearing-highlights-cambridge-analytica

Nicoll, C., Prins, J. E. J., van Dellen, M. J. M. (eds), Digital Anonymity and the Law. Tensions and Dimensions, The Hague 2003

Nouwens M., Liccard I., Veale M., Karger D., Kagal L., Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence, 8 January 2020, https://arxiv.org/pdf/2001.02479.pdf

Novak M., Facebook Must Delete Content Globally If It's Considered Defamatory in Europe, Top EU Court Rules, 3 October, 2019, https://gizmodo.com/facebook-must-delete-content-globally-if-its-considered-18387

Nuñez M., FTC Slaps Facebook With $5 Billion Fine, Forces New Privacy Controls, Jul 24, 2019, https://www.forbes.com/sites/mnunez/2019/07/24/ftcs-unprecedented-slap-fines-facebook-5-billion-forces-new-privacy-controls/#3e7bb16a5668

O

Obar J. A., Big Data and The Phantom Public: Walter Lippmann and the Fallacy of Data Privacy Self-Management, 2015, https://ssrn.com/abstract=2239188

O'Donoghue C., Mackay A., European Data Protection Board replaces Article 29 Working Party, July 2, 2018, https://www.technologylawdispatch.com/2018/07/privacy-data-protection/european-data-protection-board-replaces-article-29-working-party/

Olleros Z., Research Handbook on Digital Transformations, Cheltenman 2016

Ong T., Facebook begins privacy push ahead of tough new European law, Jan 29, 2018, https://www.theverge.com/2018/1/29/16944304/facebook-privacy-eu-law-general-data-protection-regulation

O'Reilly C., Finding jurisdiction to regulate Google and the Internet, European Journal of Law and Technology, vol. 2, no. 1, 2011

P

Paliwala A. (ed), A History of Legal Informatics, Zaragoza 2010

Palmer V. V., Mattar M. Y., Koppel A. (eds), Mixed Legal Systems, East and West, Dorchester 2015

Parker C. B., Stanford research finds that computers are better judges of personality than friends and family, January 12, 2015, https://engineering.stanford.edu/magazine/article/stanford-research-finds-computers-are-better-judges-personality-friends-and-family

Perritt Jr. H. H., Sources of Rights to Access Public Information, 4 WM. & MARY BILL RTS. J. 179 (1995)

Perritt Jr. H. H., The Internet at 20: Evolution of a Constitution for Cyberspace, 20 Wm. & Mary Bill Rts. J. 1115 (2012), https://scholarship.law.wm.edu/wmborj/vol20/iss4/5

Phillips S., A brief history of Facebook. Guardian, 2007, www.guardian.co.uk/technology/2007/jul/25/media.newmedia

Pix A., Surveillance Is the Business Model of the Internet - Interview with Bruce Schneier, July 18, 2017, https://www.schneier.com/news/archives/2017/07/surveillance_is_the_.html

Poeter D., EU Slams Microsoft With Record $1.35 Billion Fine, http://www.crn.com/news/applications-os/206900563/eu-slams-microsoft-with-record-1-35-billion-fine.htm,

Pohlmann N., Sparenberg M., Siromaschenko I., Kilden K., Secure Communications and Digital Sovereignty in Europe, ISSE 2014 Securing Electronic Business Processes, Brussels, Belgium, 2014

Pollman E., Barry J. M., Regulatory Entrepreneurship, 90 S. Cal. L. Rev. 383 (2017), Loyola Law School, Los Angeles Legal Studies Research Paper No. 2017-29, https://ssrn.com/abstract=2741987

Polonetsky, Jules and Wolf, Christopher, The US-EU Safe Harbor. An Analysis of the Framework's Effectiveness in Protecting Personal Privacy, December 2013, https://www.scribd.com/embeds/191149678/content?start_page=1&view_mode=scroll&access_key=key-1evmvtd2msnwuqiy2u9u&show_recommendations=true

Post Robert C., Three Concepts of Privacy, 89 Geo. L.J. 2087, 2087 (2001)
Poysti, T., Raman, J., Information Security Law Commentary, 2006
Priest W. C., The Character of Information: Characteristics and Properties of Information Related to Issues Concerning Intellectual Property, Office of Technology Assessment, 1994.
Puccio L., Monteleone S., The Privacy Shield: Update on the state of play of the EU-US data transfer rules, https://www.academia.edu/37345183/The_Privacy_Shield_Update_on_the_state_of_play_of_the_EU-US_d

R

Rainie L., The State of Privacy in America, Pew Research Center, September 2016, www.pewresearch.org/fact-tank/2016/09/21/thestate-of-privacy-in-america/
Ramsey M. D., International Law Limits on Investor Liability in Human Rights Litigation, 50 HARV. INT'L L.J. 271, 296 (2009).
Rantham L., PRISM, Snowden and Government Surveillance: 6 Things You Need To Know, April 19, 2017, https://www.cloudwards.net/prism-snowden-and-government-surveillance/
Rao J. M., Reiley D. H., The Economics of Spam, Journal of Economic Perspectives, vol. 26 (3), 2012
Raul, A. C., Privacy and the Digital State: Balancing Public Information and Personal Privacy, Boston 2002
Rayward, W. B. (editor), European Modernism and the Information Society. Informing the Present, Understanding the Past, Cornwall 2008
Reed, C, Internet Law. Text and Materials, 2nd Edition, Cambridge 2004
Regan P. M., Legislating Privacy. Chapel Hill, 1995, NC: University of North Carolina Press
Reid F., Harrigan M., An Analysis of Anonymity in the Bitcoin System, https://arxiv.org/abs/1107.4524
Reidenberg, Joel R., The Transparent Citizen (October 14, 2015). Loyola University Chicago Law Journal, Vol. 47, 2015; Fordham Law Legal Studies Research Paper No. 2674313. Available at SSRN: http://ssrn.com/abstract=2674313
Reisinger L., Rechtsinformatik, de Gruyter, Berlin 1977.
Rennenberg, K., Royer, D., Deuker, A. (editors), The Future of Indetity in the Information Society. Challenges and Opportunities, New York 2009
Rhoen M., Beyond consent: improving data protection through consumer protection law. Internet Policy Review, 5(1), 2016, http://policyreview.info/articles/analysis/beyond-consent-improving-data-protectionthroughconsumer-protection-law
Rice M., The Deep Web Is the 99% of the Internet You Can't Google, May 22, 2018, https://curiosity.com/topics/the-deep-web-is-the-99-of-the-internet-you-dont-see-curiosity/
Richards, Neil M. and Hartzog, Woodrow, Taking Trust Seriously in Privacy Law (September 3, 2015). Stanford Technology Law Review, Forthcoming. Available at SSRN: http://ssrn.com/abstract=2655719 or http://dx.doi.org/10.2139/ssrn.2655719
Rifkind, M., Porter, H., Henry Porter v Malcolm Rifkind: surveillance and the free society, http://www.theguardian.com/commentisfree/2013/aug/24/rifkind-porter-debate-miranda-surveillance/
Rodrigues, R., Privacy on Social Networks: Norms, Markets, and Natural Monopoly, [in:] S. Levmore, M. C. Nussbaum (ed.), The Offensive Internet, Cambridge, Massachusetts, London 2010
Roessler B., Mokrosinska D., Privacy and social interaction. Philosophy & Social Criticism, 39(8), 2013, https://doi.org/10.1177/0191453713494968
Romm T., Tech giants get deeper into D.C. influence game, Politico, 01/21/2015, http://www.politico.com/story/2015/01/tech-lobby-apple-amazon-facebook-google114468

Romm T., Timberg C., FTC opens investigation into Facebook after Cambridge Analytica scrapes millions of users' personal information, March 2018, https://www.washingtonpost.com/news/the-switch/wp/2018/03/20/ftc-opens-investigation-into-facebook-after-cambridge-analytica-scrapes-millions-of-users-personal-information/?noredirect=on&utm_term=.7f2e14cdafeb

Rosoff M., Here's How Dominant Google Is In Europe, November 29, 2014, https://www.businessinsider.com/heres-how-dominant-google-is-in-europe-2014-11?r=US&IR=T

Rowland, D., Kohl, U., Charlesworth, A., Information Technology Law, 4th Edition, New York 2012

Rubinstein, Ira and Hartzog, Woodrow, Anonymization and Risk (August 17, 2015). Washington Law Review, Vol. 91, No. 2, 2016; NYU School of Law, Public Law Research Paper No. 15-36. Available at SSRN: http://ssrn.com/abstract=2646185

Rubinstein, Ira and Hartzog, Woodrow, Anonymization and Risk (August 17, 2015). Washington Law Review, Vol. 91, No. 2, 2016; NYU School of Law, Public Law Research Paper No. 15-36. Available at SSRN: http://ssrn.com/abstract=2646185

Rücker D., Kugler T. (eds), New European General Data Protection Regulation. A Practitioner's Guide. Ensuring Compliant Corporate Practice, Baden-Baden 2018

Rule, J., Greanleaf, G. (editors), Global Privacy Protection. The First Generation, Cheltenham 2010

Russel L., Blockchains: The legal landscape, https://www.blakemorgan.co.uk/training-knowledge/features-and-articles/blockchains-legal-landscape/

Russinovich M., Microsoft joins partners and the Linux Foundation to create Confidential Computing Consortium, August 21, 2019, https://cloudblogs.microsoft.com/opensource/2019/08/21/microsoft-partners-linux-foundation-announce-confidential-computing-consortium/

S

Saarenpää A. (editor), Legal Privacy, Zaragoza 2008

Saarenpää A., Reading and Comparing Legal Sources

Saarenpää A., Sztobryn K. (eds), Lawyers in the Media Society, University of Lapland, Rovaniemi 2016

Saarenpää A., Wiatrowski A. (eds), Society Trapped in the Network. Does it have a Future?, University of Lapland, Rovaniemi 2016

Samuelson P., A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy, Information Economy, 87 Cal. L. Rev. 751 (1999), https://www.jstor.org/stable/3481032?seq=1#metadata_info_tab_contents

Santolli J., Terrorist Finance Tracking Program: Illuminating the Shortcomings of the European Union's Antiquated Data Privacy Directive, 40 GEO. WASH. INT'L. L. REv. 553 (2008), Federal Constitutional Court, 54 NJW 1921 (2001)

Sanvenero R., Social Media and Our Misconceptions of the Realities, https://ssrn.com/abstract=2243896, 2013

Savage N., Hands-On with Google's Quantum Computer, October 24, 2019, https://www.scientificamerican.com/article/hands-on-with-googles-quantum-computer/

Scally, D.,Time to tell tech firms that private data is 'none of your business' – Max Schrems. Privacy activist is creating a non-profit organisation to fight for data protection, November 30, 2017, https://www.irishtimes.com/business/technology/time-to-tell-tech-firms-that-private-data-is-none-of-your-business-max-schrems-1.3309734

Schaefer L., Deutsche Telekom: 'Internet data made in Germany should stay in Germany', September 2013, https://www.dw.com/en/deutsche-telekom-internet-data-made-in-germany-should-stay-in-germany/a-17165891

Schartum, D. W. (editor), Overvaking i en Rettsstat, Bergen 2010
Schaub, Florian, Balebako, Rebecca, Durity, Adam L. and Cranor, Lorrie F., A Design Space for Effective Privacy Notices, https://www.usenix.org/conference/soups2015/proceedings/presentation/schaub
Schmidt, E., Cohen, J., The New Digital Age. Reshaping the Future of People, Nations and Business, London 2014
Schneier B., Commentary, The Eternal Value of Privacy, WIRED, May 18, 2006, http://www.wired.com/news/columns/1,70886-0.html
Schonfeld E., Facebook closing in on 500 million visitors a month, TechCrunch, 2010, http://techcrunch.com/2010/04/21/facebook-500-million-visitors-comscore/
Schwartz J., Two German Killers Demanding Anonymity Sue Wikipedia's Parent, N.Y. TIMEs, November 2009.
Schwartz P. M., Preemption and Privacy, 118 YALE L.J. 902, 908 (2009).
Schwartz P. M., Privacy and Democracy in Cyberspace, 52 VAND. L. REV. 1609, 1633 (1999)
Schweighofer, E. (editor), Semantisches Web und Soziale Netzwerke im Recht. Tagungsband des 12. Internationalen Rechtsinformatik Symposions, Vienna 2009
Schweighofer, E., Handstanger, M., Hoffman, H., Kummer, F., Primosch, E., Schefbeck, G., Withalm, G. (editors), Zeichen und Zauber des Rechts, Bern 2014
Schweighofer, E., Kummer, F., Hötzendorfer, W. (ed.), Transparency, Proceedings of the 17th International Legal Informatics Symposium IRIS 2014, Salzburg 2014,
Schweighofer, E., Kummer, F., Hotzendorfer, W. (editors), Abstraction and Application. Proceedings of the 16th International Legal Informatics Symposium, Vienna 2013
Schweighofer, E., Kummer, F., Hotzendorfer, W. (editors), Transparency. Proceedings of the 17th International Legal Informatics Symposium, Vienna 2014
Schweighofer, E., Kummer, F., Hotzendorfer, W., Borges, G. (eds.), Networks. IRIS 2016. Proceedings of the 19th International Legal Informatics Symposium, Vienna 2016
Schweighofer, E., Saarenpää, A., Boszormenyi, J. (editors), KnowRight 2012. Knowledge Rights – Legal, Societal and Related Technological Aspects. 25 Years of Data Protection in Finland. OCG Forum Privacy 2013. IT Enterprises Between Surveillance State and Consumer Responsibility, Vienna 2013
Scott M., Google details requests in Europe „to be forgotten", International New York Times (10 October 2014) 16
Scott M., Larger T., To take on Big Tech, US can learn antitrust lessons from Europe, August 25, 2019, https://www.politico.eu/article/europe-us-big-tech-competition-antitrust-apple-google-facebook-amazon/
Seiffert J., Weighing a Schengen zone for Europe's Internet data, February 2014, https://www.dw.com/en/weighing-a-schengen-zone-for-europes-internet-data/a-17443482
Seipel, P., Computing Law. Perspectives on a New Legal Discipline, Stockholm 1977
Seipel P., IT Law in the Framework of Legal Informatics, Stockholm Institute for Scandinavian Law 1957-2010
Sevignani S., The commodification of privacy on the Internet, Science and Public Policy 40, 2013
Shapiro A., A Closer Look At EU Parliament's Vote To Break Up Google, November 28, 2014, https://www.kgou.org/post/closer-look-eu-parliaments-vote-break-google
Sharma, D. (editor), Social Security and Human Rights, New Delhi 2014
Sherr I., Facebook lost control of our data. Now it's paying a record $5 billion fine, Jul 24, 2019, https://www.cnet.com/news/facebook-lost-control-of-our-data-now-its-paying-a-record-5-bill

Simitis S., Datenschutz - Rfickschritt oder Neubeginn?, 51 NJW 2473, 2477 (1998).
Simitis S., Privacy - An Endless Debate, December 2010, California Law Review vol. 98, issue 6.
Simitis S., Reviewing Privacy in an Information Society, University of Pennsylvania Law Review 135, 1987
Simmons D., 6 Countries with GDPR-like Data Privacy Laws, January 17, 2019, https://insights.comforte.com/6-countries-with-gdpr-like-data-privacy-laws
Simpson J., Restore 'Privacy by Obscurity', December 4, 2014, https://www.usnews.com/debate-club/should-there-be-a-right-to-be-forgotten-on-the-internet/restore-privacy-by-obscurity
Singer N., Conger K., Google Is Fined $170 Million for Violating Children's Privacy on YouTube, 4 September, 2019, https://www.nytimes.com/2019/09/04/technology/google-youtube-fine-ftc.html
Słojewska, A. , Bruksela nie kończy walki z Microsoftem, „Rzeczpospolita", 13.07.2006.
Smith B., Brad Smith: Before The Senate Subcommittee On Antitrust, Competition Policy And Consumer Rights (Washington D.C., 2007), https://news.microsoft.com/2007/09/27/brad-smith-before-the-senate-subcommittee-on-antitrust-competition-policy-and-consumer-rights/#zVhQg6ZZ2QzGQqpC.97
Smith I., Before you lament the end of your internet privacy, read this, Mar 31, 2017, https://www.pbs.org/newshour/politics/lament-end-internet-privacy-read
Solove Daniel J., Schwartz Paul M., Information Privacy Law, Fourth Edition, New York 2011,
Solove Daniel J., Hoofnagle Chris J., A Model Regime of Privacy Protection (Version 3.0). GWU Law School Public Law Research Paper No. 132; University of Illinois Law Review, Vol. 2006, No. 2, 2006. Available at SSRN: http://ssrn.com/abstract=881294
Solove Daniel J., Schwartz Paul M., Privacy Law Fundamentals. D. Solove & P. Schwartz, PRIVACY LAW FUNDAMENTALS, International Association of Privacy Professionals, 2011; GWU Law School Public Law Research Paper No. 542; UC Berkeley Public Law Research Paper No. 1790262; GWU Legal Studies Research Paper No. 542. Available at SSRN: http://ssrn.com/abstract=1790262
Solove Daniel J., A Brief History of Information Privacy Law. PROSKAUER ON PRIVACY, PLI, 2006; GWU Law School Public Law Research Paper No. 215. Available at SSRN: http://ssrn.com/abstract=914271
Solove Daniel J., A Brief History of Information Privacy Law. PROSKAUER ON PRIVACY, PLI, 2006; GWU Law School Public Law Research Paper No. 215. Available at SSRN: http://ssrn.com/abstract=914271
Solove Daniel J., Access and Aggregation: Public Records, Privacy, and the Constitution, 86 MINN. L. REV. 1137 (2002)
Solove Daniel J., Conceptualizing Privacy. California Law Review, Vol. 90, 2002. Available at SSRN: http://ssrn.com/abstract=313103
Solove Daniel J., Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75 S. CAL. L. REV. 1083 (2002)
Solove Daniel J., 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. San Diego Law Review, Vol. 44, p. 745, 2007; GWU Law School Public Law Research Paper No. 289. Available at SSRN: http://ssrn.com/abstract=998565
Solove Daniel J., Nothing to Hide: The False Tradeoff between Privacy and Security (May 1, 2011). Daniel J. Solove, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY, Chapter 1, Yale University Press, 2011; GWU Law School Public Law Research Paper No. 571; GWU Legal Studies Research Paper No. 571. Available at SSRN: http://ssrn.com/abstract=1827982

Solove Daniel J., Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 STAN. L. REV. 1393 (2001)
Solove Daniel J., Privacy Self-Management and the Consent Dilemma, 126 HARV. L. REV. 1880, 1883-88 (2013)
Solove Daniel J., Reconstructing Electronic Surveillance Law. George Washington Law Review, Vol. 72, 2004. Available at SSRN: http://ssrn.com/abstract=445180 or http://dx.doi.org/10.2139/ssrn.445180
Solove Daniel J., Schwartz Paul M., Information Privacy Law, 4th Edition, New York 2011
Solove Daniel J., The Future of Reputation. Gossip, Rumor, and Privacy on the Internet, London 2007
Solove Daniel J., The Origins and Growth of Information Privacy Law. PLI/PAT, Vol. 748, p. 29, 2003. Available at SSRN: http://ssrn.com/abstract=445181 or http://dx.doi.org/10.2139/ssrn.445181
Solove Daniel J., Understanding Privacy. Daniel J. Solove, UNDERSTANDING PRIVACY, Harvard University Press, May 2008; GWU Legal Studies Research Paper No. 420; GWU Law School Public Law Research Paper No. 420. Available at SSRN: http://ssrn.com/abstract=1127888
Sparrow, A., The Law of Virtual Worlds and Internet Social Networks, Surrey 2010
Standish R., Why Is Finland Able to Fend Off Putin's Information War? Helsinki has emerged as a resilient front against Kremlin spin. But can its successes be translated to the rest of Europe?, March 2017, https://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war/
Stewart Daxton R. (editor), Social Media and the Law. A Guidebook for Communication Students and Professionals, New York 2013
Stolton S., Facebook to Irish data body: 533 million user breach took place before GDPR, April 6, 2021, https://www.euractiv.com/section/data-protection/news/facebook-to-irish-data-body-533-million-user-breach-took-place-before-gdpr/
Stone Geoffrey R., Commentary, Freedom and Public Responsibility, CHI. TRIB., May 21, 2006
Stupp C., Cambridge Analytica harvested 2.7 million Facebook users' data in the EU, Apr 6, 2018, https://www.euractiv.com/section/data-protection/news/cambridge-analytica-harvested-2-7-million-facebook-user
Sunstein Cass R., Vermeule A., Interpretation and Institutions (July 2002). U Chicago Law & Economics, Olin Working Paper No. 156; U Chicago Public Law Research Paper No. 28. Available at SSRN: http://ssrn.com/abstract=320245 or http://dx.doi.org/10.2139/ssrn.320245
Susskind R., The Future of Law. Facing Challenges of Information Technology, Oxford 1996
Swire P. P, Litan R. E., None of Your Business: World Data Flows, Electronic Commerce and the European Privacy Directive (1998)
Svatesson Dan Jerker B., Bad news for the Internet as Europe's top court opens the door for global content blocking orders, October 3, 2019, https://www.linkedin.com/pulse/bad-news-internet-europes-top-court-opens-door-global-svantesson/
Svantesson Dan Jerker B., Extraterritoriality in Data Privacy Law, Copenhagen 2013
Svantesson Dan Jerker B., Greenstein S. (editors), Nordic Yearbook of Law and Informatics 2010-2012. Internationalisation of Law in the Digital Information Society, Copenhagen 2013
Swire P. (Testimony, Senate Judiciary Committee Hearing, July 8, 2015), Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy, http://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Swire%20Testimony.pdf

Sykes C. J., The End of Privacy 6-9 (1999)
Szyszczak E., Controlling Dominance in European Markets, [in:] Fordham International Law Journal, Volume33, Issue 6, 2011

T

Taraszow T., Arsoy A., Shitta G., Laoris Y, How much personal and sensitive information do Cypriot teenagers reveal in Facebook?, [in:] Proceedings From 7th European Conference on E-Learning, 2008, Reading, England
Taylor K., What is the Surface Web?, https://www.hitechnectar.com/blogs/introduction-surface-web-deep-dark-web/
Taylor L., Floridi L., van der Sloot B. (eds.), Group Privacy: new challenges of data technologies, Dordrech 2017
Tene O., Wolf Ch., The Draft EU General Data Protection Regulation: Costs and Paradoxes of Explicit Consent, January 2013, https://www.scribd.com/embeds/121642539/content?start_page=1&view_mode=scroll
Tene O., Wolf Ch., Overextended: Juristiction and APplicable Law under the EU General Data Protection Regulation, January 2013, https://www.scribd.com/embeds/121642254/content?start_page=1&view_mode=scroll
Tene O., Wolf Ch., The Definition of Personal Data: Seeing the Complete Spectrum, January 2013, https://www.scribd.com/embeds/121642913/content?start_page=1&view_mode=scroll
Thanjagari V., Deep Web & Dark Web Explained, May 7, 2019, https://hackernoon.com/deep-web-dark-web-explained-dd3b1e6855e
Thoren-Peden D.S, Meyer C.D., Data Protection 2018: USA, June 26, 2018, https://www.pillsburylaw.com/en/news-and-insights/data-protection-2018-usa.html
Tranberg, Ch. B., Proportionality and data protection in the case law of the European Court of Justice, International Data Privacy Law 1, no. 4 (2011)
Tufekci Z., Facebook's Surveillance Machine, March 19, 2018, https://www.nytimes.com/2018/03/19/opinion/facebook-cambridge-analytica.html
Turow J., Hoofnagle C. J., Mulligan D. K., Good N., Grossklags J., The federal trade commission and consumer privacy in the coming decade. I/S: A Journal of Law & Policy for the Information Society, (723)

U

Underwood K., Why companies are hiring sci-fi writers to imagine the future, 27 February, 2020, https://www.cpacanada.ca/en/news/pivot-magazine/2020-02-27-sci-fi-prototyping
Utz Ch., Degeling M., Fahl S., (Un)informed Consent: Studying GDPR Consent Notices in the Field, 22 October 2019, https://arxiv.org/pdf/1909.02638.pdf

V

Van Alsenoy B., Verdoodt V., Heyman R., Ausloos J., Wauters E., Acar G., From social media service to advertising network. A critical analysis of Facebook's Revised Policies and Terms, March 31, 2015, https://www.law.kuleuven.be/citip/en/news/facebook-1/facebooks-revised-policies-and-terms-v1-2.pdf
Van Bael, Bellis (editor), Competition Law Of The European Community, The Hague 2005
Van Calster G., Steady now. Eva Glawischnig-Piesczek v Facebook. The CJEU on jurisdiction and removal of hate speech, Conflict of Laws /Private international law, EU law - General, October 10, 2019, https://gavclaw.com/tag/c-13617/
Van Dijk, J., The Network Society, 3rd Edition, London 2012
van Loon, S., Chapter 2. The Power of Google: First Mover Advantage or Abuse of a Dominant Position, [in:] A. Lopez-Tarruella (editor), Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models, The Hague 2012

Vara V., Europe versus Google, November 29, 2014, https://www.newyorker.com/business/currency/europe-versus-google
Vincent J., Google fined a record €2.4 billion by the EU for manipulating search results, 27 June, 2017, https://www.theverge.com/2017/6/27/15872354/google-eu-fine-antitrust-shopping
Vincent J., Google hit with €1.5 billion antitrust fine by EU, 20 March, 2019, https://www.theverge.com/2019/3/20/18270891/google-eu-antitrust-fine-adsense-advertising
Vincenti D., EU urged to choose transatlantic convergence on data protection, December 2012, https://www.euractiv.com/section/digital/news/eu-urged-to-choose-transatlantic-convergence-on-data-protection/
Von Drehle D., The Surveillance Society, 2013, http://nation.time.com/2013/08/01/the-surveillance-society/
Voorhees, J., Obama Defends NSA Surveillance: "Nobody Is Listening to Your Telephone Calls.", June 7 2013, http://www.slate.com/blogs/the_slatest/2013/06/07/obama_defends_nsa_surveillance.html/
Voulodimos A. S.,Patrikakis C. Z., Quantifying Privacy in Terms of Entropy for Context Aware Services, special issue of the Identity in the Information Society journal, "Identity Management in Grid and SOA", Springer, vol. 2, no 2, December 2009

W

Wadham, J., Human Rights and Privacy - The Balance, speech given at Cambridge (March 2000), http://www.liberty-human-rights.org.uk/mhrp6j.html
Wahlgren P., Automation of Legal Reasoning. A Study on Artificial Intelligence and Law, Stockholm 1992
Wahlgren P. (ed.), Scandinavian Studies in Law Volume 65. 50 Years of Law and IT. The Swedish Law and Informatics Research Insitute 1968-2018, Stockholm 2018
Wahlgren P., The Quest for Law, Stockholm 1999
Waldo J., Lin H. S., Millett L. I., (eds.), Engaging Privacy and Informational Technology and a Digital Age, Washington DC 2007
Walters J., Steve Bannon on Cambridge Analytica: 'Facebook data is for sale all over the world', March 2018, https://www.theguardian.com/us-news/2018/mar/22/steve-bannon-on-cambridge-analytica-facebook-data-is-for-sale-all-over-the-world
Warren S. D., Brandeis, L. D., The Right to Privacy, Harvard Law Review, 4(5), 1890,
Warren T., Microsoft finally admits Windows Phone is dead, October 9, 2017, https://www.theverge.com/2017/10/9/16446280/microsoft-finally-admits-windows-phone-is-dead
Warzel Ch., These Confidential Charts Show Why Facebook Bought WhatsApp, Mac R., December 5, 2018, https://www.buzzfeednews.com/article/charliewarzel/why-facebook-bought-whatsapp
Webster F., Theories of the Information Society, 4th Edition, New York 2014
Wess M., Looking to comply with GDPR? Here's a primer on anonymization and pseudonymization, April 2017, https://iapp.org/news/a/looking-to-comply-with-gdpr-heres-a-primer-on-anonymization-and-pseudonymization/
Westby J. R. (editor), International Guide to Privacy, Chicago 2004
Westby J. R., Project Chair (ed.), International Guide to Privacy. American Bar Association Privacy & Computer Crime Committee Section of Science & Technology Law, ABA Publishing 2004,
Whish R., Competition Law 6th Edition, New York 2009
Whitman J. Q., The Two Western Cultures of Privacy: Dignity Versus Liberty, 113 YALE L.J. 1151 (2004).

Whittaker Z., Microsoft fined $731m by EU in browser choice screw-up, March 6, 2013, https://www.zdnet.com/article/microsoft-fined-731m-by-eu-in-browser-choice-screw-up/
Wieduwilt H., Gesucht: Mdnnlich, liiert, heterosexuell, aus Berlin, FRANKFURTER ALLGEMEINE ZEITUNG, Dec. 22, 2009
Wiener J. B., Rogers M. D., Comparing precaution in the United States and Europe, Journal of Risk Research 5 (4), 2002
Wiener N., CYBERNETICS: OR CONTROL AND COMMUNICATION IN THE ANIMAL AND THE MACHINE (2d. ed. 1961).
Wiese Schartum D. (editor), Overvaking I en rettsstat. Boken utgis I serien Nordisk arbok I rettsinformatikk, Bergen 2010
Wilke S., Krings D., Blockchain from a perspective of data protection law. A brief introduction to data protection ramifications, https://www2.deloitte.com/dl/en/pages/legal/articles/blockchain-datenschutzrecht.html
Willinger M., March 2012, Context and Legitimate Basis: US-EU approaches to data processing, https://fpf.org/2012/03/27/context-and-legitimate-basis-us-eu-approaches-to-data-processing/
Willinger M., October 2012, What's Wrong with the Proposed EU Right of Data Portability?, https://fpf.org/2012/10/17/whats-wrong-with-the-proposed-eu-right-of-data-portability/
Witzleb N., Lindsay D., Moira P., Rodrick S. (editors), Emerging Challenges in Privacy Law. Comparative Perspectives, Cambridge 2014
Wong P., Conversations about the Internet #5: Anonymous Facebook Employee, 2010, http://therumpus.net/2010/01/conversations-about-the-internet-5-anonymousfacebook-employee/3/
Woolgar S. (ed), Virtual Society? Technology, Cyberbole, Reality, Oxford 2002
Wright D., De Hert P. (eds), Privacy Impact Assesment, London 2012
Wright T. D., UK gives search engines time to comply with 'right to be forgotten', May 23, 2014, https://www.lexology.com/library/detail.aspx?g=ad5225dc-5e52-45fe-b3b0-6681681bee3a
Wyatt E., A Victory for Google as F.T.C. Takes No Formal Steps, January 3, 2013, https://www.nytimes.com/2013/01/04/technology/google-agrees-to-changes-in-search-ending-us-antitrust-inquiry.html

Y

Yahnke K., A Practical Guide to Data Privacy Laws by Country. Improve your knowledge of (and compliance with) data protection laws around the world with this introductory guide, November 5, 2018, https://i-sight.com/resources/a-practical-guide-to-data-privacy-laws-by-country/

Z

Zittrain J., Europe's Bad Solution to a Real Problem, December 5, 2014, https://www.usnews.com/debate-club/should-there-be-a-right-to-be-forgotten-on-the-internet/europes-bad-solution-to-a-real-problem
Zittrain J., Future of the Internet and How to Stop it, London 2008
Zuboff S., Dark Google, April 30, 2014, https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshanna-zuboff-dark-google-12916679.html
Zuboff S., The Age of Surveillance Capitalism. The Fight for Human Future at the New Frontier of Power, London 2019
Zuboff S., The Secrets of Surveillance Capitalism, March 5, 2016, https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html

Zyskind G., Nathan O., Pentland A., Decentralizing Privacy: Using Blockchain to Protect Personal Data, http://ieee-security.org/TC/SPW2015/IWPE/5.pdf

Zywica J., Danowski J., The faces of Facebookers: Investigating social enhancement and social compensation hypotheses; predicting Facebook™ and offline popularity from sociability and self-esteem, and mapping the meanings of popularity with semantic networks, Journal of Computer-Mediated Communication 14, 2008

TITLED LINKS

2016 Data Protection and Breach Readiness Guide. Providing prescriptive advice to help business optimize privacy and security practices, reducing the risk and impact of data loss incidents, Online Trust Alliance 2016, https://otalliance.org/system/files/files/resource/documents/2016-ota-breachguidehr.pdf

"Anonymized" data really isn't—and here's why not, http://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/

"Fundamental Rights are Fundamental", https://www.privacyinternational.org/sites/default/files/NGOStatement.pdf

87% of Android devices are vulnerable, Nexus models most secure, http://www.tweaktown.com/news/48002/87-android-devices-vulnerable-nexus-models-secure/index.html

A Brief History of Safe Harbor, https://iapp.org/resources/article/a-brief-history-of-safe-harbor/

A Closer Look At EU Parliament's Vote To Break Up Google, http://www.npr.org/2014/11/28/367244283/a-closer-look-at-eu-parliaments-vote-to-break-up-google

A closer look at Yandex's market share in Russia, http://marketrealist.com/2014/03/yandex-market-share-increase-powered-search/, http://connect.icrossing.co.uk/a-closer-look-at-yandexs-market-share-in-russia_12575

Ad Tech Surveillance on the Public Sector Web. A special report on pervasive tracking of EU citizens on government and health service websites, Report by Cookiebot, March 2019, https://www.cookiebot.com/media/1121/cookiebot-report-2019-medium-size.pdf

AG James: Google And Youtube To Pay Record Figure For Illegally Tracking And Collecting Personal Information From Children, 4 September, 2019, https://ag.ny.gov/press-release/2019/ag-james-google-and-youtube-pay-record-figure-illegally-tracking-and-collecting

A manifesto for the future of the 'right to be forgotten' debate, http://www.theguardian.com/technology/2014/jul/22/a-manifesto-for-the-future-of-the-right-to-be-forgotten-debate

Actually, Facebook Changed Its Terms To Cover That Experiment After It Was Over, http://www.consumerwatchdog.org/story/actually-facebook-changed-its-terms-cover-experiment-after-it-was-over

AltaVista: A Brief History of the AltaVista Search Engine, http://www.websearchworkshop.co.uk/altavista_history.php

American Chamber of Commerce to the European Union, http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=5265780509-97

An update on kids and data protection on YouTube, 4 September, 2019, https://youtube.googleblog.com/2019/09/an-update-on-kids.html

An Update on Our App Developer Investigation, 20 September, 2019, https://newsroom.fb.com/news/2019/09/an-update-on-our-app-developer-investigation/

Android dominates 81 percent of world smartphone market, http://www.cnet.com/uk/news/android-dominates-81-percent-of-world-smartphone-market/

Announcing Project Zero, July 2014, https://googleonlinesecurity.blogspot.fi/2014/07/announcing-project-zero.html

Antitrust: Commission probes allegations of antitrust violations by Google, http://europa.eu/rapid/press-release_IP-10-1624_en.htm
AOL releases search data on 500,000 users, http://arstechnica.com/uncategorized/2006/08/7433/
Apple and Google sign letter urging Obama to support encryption, http://www.theguardian.com/technology/2015/may/19/apple-google-letter-president-obama-encryption-fbi-surveillance
Apple defies FBI and offers encryption by default on new operating system, http://www.theguardian.com/technology/2014/oct/17/apple-defies-fbi-encryption-mac-osx
Apple's encryption means it can't comply with US court order, http://www.theguardian.com/technology/2015/sep/08/apple-encryption-comply-us-court-order-iphone-imessage-justice
Apple's encryption means it can't comply with US court order, September 2015, http://www.theguardian.com/technology/2015/sep/08/apple-encryption-comply-us-court-order-iphone-imessage-justice
Apple responds to FBI iPhone hack: 'This case should never have been brought', http://thenextweb.com/apple/2016/03/29/apple-responds-fbi-iphone-hack-case-never-brought/
Arguments for and against EU data protection rules, http://www.debatingeurope.eu/focus/infobox-arguments-for-and-against-eu-data-protection-rules/#.VMi3bmh4rh4
As U.S. Tech Companies Scramble, Group Sees Opportunity in Safe Harbor Decision, October 2015, http://www.nytimes.com/2015/10/21/technology/as-us-tech-companies-scramble-group-sees-opportunity-in-safe-harbor-decision.html?smid=fb-share
As U.S. Tech Companies Scramble, Group Sees Opportunity in Safe Harbor Decision, http://www.nytimes.com/2015/10/21/technology/as-us-tech-companies-scramble-group-sees-opportunity-in-safe-harbor-decision.html?smid=fb-share&_r=0
Austrian activist launches consumers' digital rights group, November 28, 2017, https://www.apnews.com/18a537b8b234445fa4eab2633a4a516d
Austria court considers Facebook privacy case, http://www.bbc.com/news/technology-32229285
Austrian student's lawsuit vs Facebook bogged down in procedure, http://www.reuters.com/article/2015/04/09/us-facebook-austria-lawsuit-idUSKBN0N019420150409
Bad Google DMCA Takedown is Hurting Us, Hosting Site Says, https://torrentfreak.com/bad-google-dmca-takedown-is-hurting-us-hosting-site-says-140330/
Before you post your next Lumia selfie on Facebook or tweet something clever, here are some social-media guidelines to help keep your online reputation safe. http://lumiaconversations.microsoft.com/2015/01/28/stop-think-connect-safeguarding-online-reputation/
Belgian court orders Facebook to stop tracking non-members, http://www.theguardian.com/technology/2015/nov/10/belgian-court-orders-facebook-to-stop-tracking-non-members
Benefits Of Participation | Privacy Shield (Privacyshield.gov, 2017) https://www.privacyshield.gov/article?id=Benefits-of-Participation
Bitcoin Anonymity - Is Bitcoin Anonymous?, https://www.buybitcoinworldwide.com/anonymity/
Blockchains Can Assist EU Regulatory Fight for Personal Data Protection, https://www.law111.com/blockchains-can-assist-eu-regulatory-fight-for-personal-data-protection
Blockchain technologies and the EU 'right to be forgotten' – an insurmountable tension?, http://www.ibtimes.co.uk/blockchain-technologies-eu-right-be-forgotten-insurmountable-tension-1580166
Book Discussion: Marko Milanovic's Extraterritorial Application of Human Rights Treaties, November 2011, http://www.ejiltalk.org/book-discussion/
Brazil and Germany draft anti-spy resolution at UN, http://www.bbc.com/news/world-europe-24781417
Chinese Search Engine Market: Stats, Trends and Insights, http://www.chinainternetwatch.com/category/search-engine/

CJEU Judgment - First Statement, Jul 16, 2020, https://noyb.eu/en/cjeu
Class action privacy lawsuit filed against Facebook in Austria, http://www.theguardian.com/technology/2015/apr/09/class-action-privacy-lawsuit-filed-against-facebook-in-austria
Coming Together to Combat Online Piracy and Counterfeiting, https://www.whitehouse.gov/blog/2013/07/15/coming-together-combat-online-piracy-and-counterfeiting
Commission to issue formal statement of objections. Letter sent to European Commissioners on February 24th, 2014, http://www.beuc.org/publications/beuc-x-2014-021_ama_antitrust_investigation_abuse_of_dominance_in_google_vertical_search.pdf
Computers may soon know you better than your spouse, http://www.pcworld.idg.com.au/article/563737/computers-may-soon-know-better-than-your-spouse/
Console Operating System Market Share Worldwide, March 2020, https://gs.statcounter.com/os-market-share/console/worldwide
Consumer Advocates Seek a 'Do-Not-Track' List, http://www.nytimes.com/2007/10/31/technology/31cnd-privacy.html
CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY, https://www.whitehouse.gov/sites/default/files/privacy-final.pdf
Consumer Watchdog Calls on Justice Department to Launch Antitrust Action Against Google, Including Possible Breakup, http://www.consumerwatchdog.org/newsrelease/consumer-watchdog-calls-justice-department-launch-antitrust-action-against-google-includ
Consumer Watchdog Urges European Parliament To Approve Call To Break Up Google, http://www.consumerwatchdog.org/newsrelease/consumer-watchdog-urges-european-parliament-approve-call-break-google
Context and Legitimate Basis: US-EU approaches to data processing, https://fpf.org/2012/03/27/context-and-legitimate-basis-us-eu-approaches-to-data-processing/
Court: Cops Need a Warrant to Open Your Phone, Even Just to Look at the Screen, http://motherboard.vice.com/read/court-cops-need-a-warrant-to-open-your-phone-even-just-to-look-at-the-screen
Court troubled by surveillance excesses at FBI, NSA, http://www.politico.com/blogs/under-the-radar/2016/04/government-surveillance-fbi-nsa-violations-222162
Cyber criminals hide in the 'dark web' to remain anonymous, May 2 2019, https://economictimes.indiatimes.com/tech/internet/cyber-criminals-hide-in-the-dark-web-to-remain-anonymous/articleshow/69139795.cms?from=mdr
Data Privacy Day 2015 – Putting people in control, http://blogs.microsoft.com/on-the-issues/2015/01/28/data-privacy-day-2015-putting-people-control/
Data privacy isn't dead with the internet of things, just different, https://gigaom.com/2015/01/12/data-privacy-isnt-dead-with-the-internet-of-things-just-different/
Data privacy law: the top global developments in 2018 and what 2019 may bring, February 25, 2019, https://www.dlapiper.com/en/finland/insights/publications/2019/02/data-privacy-law-2018-2019/
Data protection in the EU: the certainty of uncertainty, http://www.theguardian.com/technology/blog/2013/jun/05/data-protection-eu-anonymous
Data protection in the EU: the certainty of uncertainty, http://www.theguardian.com/technology/blog/2013/jun/05/data-protection-eu-anonymous
Data protection in United States: overview, http://uk.practicallaw.com/6-502-0467
Data Protection: companies must bear their responsibility, http://www.eppgroup.eu/press-release/Data-Protection%3A-companies-must-bear-their-responsibility

Denmark's Vestager reappointed EU competition commissioner, September 11, 2019, https://www.thelocal.dk/20190911/denmarks-vestager-reappointed-eu-competition-commissioner

Digital records could expose intimate details and personality traits of millions, http://www.cam.ac.uk/research/news/digital-records-could-expose-intimate-details-and-personality-traits-of-millions#sthash.KgR9ynWT.Wf96PXdg.dpuf

Does Obama privacy push have oomph?, http://www.politico.com/story/2015/01/obama-cybersecurity-privacy-initiatives-114184.html

Don't Force Google to 'Forget', http://www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html

Don't Strike Down the Safe Harbor Based on Inaccurate Views About U.S. Intelligence Law, https://iapp.org/news/a/dont-strike-down-the-safe-harbor-based-on-inaccurate-views-on-u-s-intelligence-law/

Don't Strike Down the Safe Harbor Based on Inaccurate Views About U.S. Intelligence Law, https://iapp.org/news/a/dont-strike-down-the-safe-harbor-based-on-inaccurate-views-on-u-s-intelligence-law/

EC Announces Privacy Shield Timeframe, Conditions, http://www.forbes.com/sites/lisabrownlee/2016/02/08/ec-announces-privacy-shield-timeframe-conditions/#462e0134284c

EDITING THE UNEDITABLE BLOCKCHAIN. Why distributed ledger technology must adapt to an imperfect world, https://www.accenture.com/fi-en/insight-editing-uneditable-blockchain

Email Hosting, March 2020, https://www.datanyze.com/market-share/email-hosting--23

EPIC - About EPIC (Epic.org, 2017) https://www.epic.org/epic/about.html

E.U. Parliament Passes Measure to Break Up Google in Symbolic Vote, http://www.nytimes.com/2014/11/28/business/international/google-european-union.html?_r=0

E.U. Parliament Passes Measure to Break Up Google in Symbolic Vote, http://www.nytimes.com/2014/11/28/business/international/google-european-union.html?_r=0

ECJ Rules: Decision 2000/520/EC on U.S./EU Safe Harbor Framework Invalid, https://www.hollandhart.com/safe-harbor-framework-invalid

Entrepreneurs at the heart of economic recovery in Europe, http://www.robert-schuman.eu/en/european-issues/0284-entrepreneurs-at-the-heart-of-economic-recovery-in-europe

EU court backs 'right to be forgotten' in Google case, May 2014, http://www.bbc.com/news/world-europe-27388289

EU court ruling opens door for 'right to be forgotten' on the Internet, http://www.euractiv.com/sections/infosociety/eu-court-ruling-opens-door-right-be-forgotten-internet-302094

EU court strikes down Cisco complaint against Microsoft-Skype merger, http://www.dw.com/en/eu-court-strikes-down-cisco-complaint-against-microsoft-skype-merger/a-17287569

EU Data Protection Regulation. EU Data Protection Legislation, http://www.eudataprotectionregulation.com/data-protection-design-by-default

EU Google investigation: Adequate answers still not found. BEUC files complaint asserting consumer interest, http://www.beuc.org/publications/beuc-pr-2014-010_eu_google_investigation-beuc_complaint.pdf

EU lawmaker warns of data protection rules delay till 2016, http://www.euractiv.com/sections/infosociety/eu-lawmaker-warns-data-protection-rules-delay-till-2016-311100

EU lawmaker warns of data protection rules delay till 2016, http://www.euractiv.com/sections/infosociety/eu-lawmaker-warns-data-protection-rules-delay-till-2016-311100

EU lawmaker warns of data protection rules delay till 2016, http://www.euractiv.com/sections/infosociety/eu-lawmaker-warns-data-protection-rules-delay-till-2016-311100

EU Privacy regulations subject to 'unprecedented lobbying', http://www.telegraph.co.uk/technology/news/9070019/EU-Privacy-regulations-subject-to-unprecedented-lobbying.html
EU privacy watchdogs give Google guidelines to change privacy practices, http://www.euractiv.com/sections/infosociety/eu-privacy-watchdogs-give-google-guidelines-change-privacy-practices-308740
EU Rejects 3rd Google Antitrust Deal; It's Time For Formal Complaint, http://www.consumerwatchdog.org/blog/eu-rejects-3rd-google-antitrust-deal-it's-time-formal-complaint
EU urged to choose transatlantic convergence on data protection, http://www.euractiv.com/infosociety/eu-urged-choose-data-protection-news-516449
EU urged to choose transatlantic convergence on data protection, http://www.euractiv.com/infosociety/eu-urged-choose-data-protection-news-516449
EU wants to divide and conquer Google, http://bgr.com/2014/11/28/eu-vs-google-search/
Europe turns against Google, http://www.politico.eu/article/when-europe-turned-against-google/
Europe-v-Facebook, Response to Audit by the Irish Office of the Data Protection Commissioner on Facebook Ireland Ltd., Vienna, 4 December 2012, 42: http://www.europe-v-facebook.org/report.pdf
Europe Versus Google, http://www.newyorker.com/business/currency/europe-versus-google
Europe Wants to Censor America's Internet, http://www.usnews.com/debate-club/should-there-be-a-right-to-be-forgotten-on-the-internet/europe-wants-to-censor-americas-internet
Europe's court should know the truth about US intelligence, http://www.ft.com/intl/cms/s/90be63f4-6863-11e5-a57f-21b88f7d973f,Authorised=false.html?siteedition=uk&_i_location=http%3A%2F%2Fwww.ft.com%2Fcms%2Fs%2F0%2F90be63f4-6863-11e5-a57f-21b88f7d973f.html%3Fsiteedition%3Duk&_i_referer=http%3A%2F%2Fblogs.cfr.org%2Fc5a52a1175b96da3ad2f95a79beaf0fa&classification=conditional_standard&iab=barrier-app#axzz3x2GajVs1
European Action Focuses Debate On Right To Be Forgotten, http://www.consumerwatchdog.org/blog/european-action-focuses-debate-right-be-forgotten
European Antitrust Chief Takes Swipe at Privacy Issue, http://www.nytimes.com/2016/01/18/technology/european-antitrust-chief-takes-swipe-at-privacy-issue.html?smid=fb-share
European Union Parliament Backs Break Up of Google, November 28, 2014, https://www.medianews4u.com/european-union-parliament-passes-measure-to-break-up-google-in-symbolic-vote/
European Regulators Hit Microsoft With $731 Million Fine, http://www.consumerwatchdog.org/story/european-regulators-hit-microsoft-731-million-fine
Europe's Bad Solution to a Real Problem, http://www.usnews.com/debate-club/should-there-be-a-right-to-be-forgotten-on-the-internet/europes-bad-solution-to-a-real-problem
Europe's top court just gave U.S. tech firms a huge headache, http://fortune.com/2015/10/06/safe-harbor-facebook-data/
Europe's top court just gave U.S. tech firms a huge headache, Octover 2015, http://fortune.com/2015/10/06/safe-harbor-facebook-data/
Extraterritoriality and the Fundamental Right to Data Protection, http://www.ejiltalk.org/extraterritoriality-and-the-fundamental-right-to-data-protection/
F.T.C. Says Internet-Connected Devices Pose Big Risks, http://bits.blogs.nytimes.com/2015/01/27/f-t-c-calls-for-strong-data-and-privacy-protection-with-connected-devices/
Facebook & Co. ignore fundamental rights, http://www.dw.com/en/facebook-co-ignore-fundamental-rights/a-16927866
Facebook Changes Privacy Policy, BBC, Aug. 27, 2009, http://news.bbc.co.uk/2/hi/8225338.stm

Facebook Faces Criticism on Privacy Change, BBC, Dec. 10, 2009, http://news.bbc.co.uk/2/hi/8405334.stm
Facebook Gives Users More Control of Privacy, BBC, Dec. 9, 2009, http://news.bbc.co.uk/2/hi/technology/8404284.stm
Facebook is eating the world, except for China and Russia: World map of social networks, http://thenextweb.com/socialmedia/2012/06/10/facebook-is-eating-the-world-except-for-china-and-russia-world-map-of-social-networks/
Facebook Is Quietly Making Friends With State Lawmakers Across The Country, http://www.consumerwatchdog.org/story/facebook-quietly-making-friends-state-lawmakers-across-country
Facebook leak: Irish regulator probes 'old' data dump, April 6, 2021, https://www.bbc.com/news/technology-56639081
Facebook may know you better than your friends and family, study finds, http://www.washingtonpost.com/news/the-intersect/wp/2015/01/12/facebook-may-know-you-better-than-your-friends-and-family-study-finds/
Facebook reads private messages to boost "Likes," lawsuit claims, https://gigaom.com/2014/01/02/facebook-reads-private-messages-to-boost-likes-lawsuit-claims/
Facebook Secret Research On Users' Emotions Is Unethical, Consumer Watchdog Says, http://www.consumerwatchdog.org/newsrelease/facebook-secret-research-users'-emotions-unethical-consumer-watchdog-says
Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises, November 2011, https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep
Facebook. Statistics of Facebook. Palo Alto, CA: Facebook, 2012, http://newsroom.fb.com/content/default.aspx?NewsAreaId=22
Facebook to Acquire WhatsApp, February 2014, http://newsroom.fb.com/news/2014/02/facebook-to-acquire-whatsapp/
Facebook tracks logged-out users in 'violation' of EU law, study says, http://thenextweb.com/facebook/2015/03/31/facebook-tracks-logged-out-users-in-violation-of-eu-law-belgian-privacy-commission-says/
Facebook Wins a Round in Austrian Court Case, http://bits.blogs.nytimes.com/2015/07/01/facebook-wins-a-round-in-austrian-court-case/?smid=fb-share&_r=0
Facebook, a 'data monopolist'?, http://www.dw.com/en/facebook-a-data-monopolist/a-17788350
Facebook's new headquarters is located at 1 Hacker Way, http://www.zdnet.com/article/facebooks-new-headquarters-is-located-at-1-hacker-way/
FACT SHEET: Safeguarding American Consumers & Families, January 2015, https://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families
First SOPA, Now Your Privacy: Facebook, Google Flex Lobbying Muscle in Europe, http://www.motherjones.com/politics/2013/03/google-facebook-sopa-privacy
Foreign Surveillance and Human Rights, Part 1: Do Foreigners Deserve Privacy?, http://www.ejiltalk.org/foreign-surveillance-and-human-rights-part-1-do-foreigners-deserve-privacy/
Foreign Surveillance and Human Rights: Introduction, http://www.ejiltalk.org/foreign-surveillance-and-human-rights-introduction/
From social media service to advertising network. A critical analysis of Facebook's Revised Policies and Terms, March 2015, http://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-2.pdf

FTC report recommended suing Google for anti-competitive practices, http://www.theguardian.com/technology/2015/mar/20/google-anti-competitive-ftc-report

GDPR: noyb.eu filed four complaints over "forced consent" against Google, Instagram, WhatsApp and Facebook, Vienna 2018, https://noyb.eu/wp-content/uploads/2018/05/pa_forcedconsent_en.pdf

General Elections in Finland, a round up one week before the election, http://www.robert-schuman.eu/en/eem/1138-general-elections-in-finland-a-round-up-one-week-before-the-election

Germany's highest court rules Facebook 'friend finder' is unlawful, http://www.theguardian.com/world/2016/jan/14/germany-highest-court-facebook-friend-finder-unlawful?CMP=share_btn_fb

Germany, Brazil Turn to U.N. to Restrain American Spies, http://foreignpolicy.com/2013/10/24/exclusive-germany-brazil-turn-to-u-n-to-restrain-american-spies/

Global Networks and Local Values, COMPUTER SCI. & TELECOMM. BD., http://sites.nationalacademies.org/CSTB/CompletedProjects/CSTB_042333

Google: A Brief History of the Google Search Engine, http://www.websearchworkshop.co.uk/google_history.php

Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law. FTC, New York Attorney General allege YouTube channels collected kids' personal information without parental consent, 4 September, 2019, https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations

Google attacks Brussels antitrust case in 100-page response, http://www.theguardian.com/technology/2015/aug/27/google-attacks-brussels-antitrust-case-european-commission-shopping-price-comparison

Google attacks Brussels antitrust case in 100-page response, http://www.theguardian.com/technology/2015/aug/27/google-attacks-brussels-antitrust-case-european-commission-shopping-price-comparison

Google case. Questions and Answers, http://www.beuc.org/publications/beuc-x-2014-025_ama_google_questions_and_answers_april_2014.pdf

Google faces antitrust action from EU competition watchdog, http://www.theguardian.com/technology/2015/apr/15/google-faces-antitrust-action-from-eu-competition-watchdog

Google faces antitrust action from EU competition watchdog, http://www.theguardian.com/technology/2015/apr/15/google-faces-antitrust-action-from-eu-competition-watchdog

Google Gets Search Take-Down Requests After European Court Ruling, http://www.nbcnews.com/tech/tech-news/google-gets-search-take-down-requests-after-european-court-ruling-n105496

Google History, http://www.google.com/about/corporate/company/history.html

Google Inc.: Is Microsoft Corporation Right, and Will This Affect Gmail Use?, http://www.consumerwatchdog.org/story/google-inc-microsoft-corporation-right-and-will-affect-gmail-use

Google Is Doing A New Thing To Tick Off Microsoft: Exposing Bugs In Windows 8, http://uk.businessinsider.com/googles-new-way-to-tick-off-microsoft-2015-1?r=US

'Google is not like any other average company', http://www.dw.com/en/google-is-not-like-any-other-average-company/a-17753047

Google Opens Privacy Web Form For 'Right To Be Forgotten' Requests, http://www.nbcnews.com/news/world/google-opens-privacy-web-form-right-be-forgotten-requests-n118211

Google 'Right To Be Forgotten' Ruling Unlikely to Repeat in U.S., http://www.nbcnews.com/tech/internet/google-right-be-forgotten-ruling-unlikely-repeat-u-s-n114731

Google 'Right To Be Forgotten' Ruling Unlikely to Repeat in U.S., http://www.nbcnews.com/tech/internet/google-right-be-forgotten-ruling-unlikely-repeat-u-s-n114731

Google Spends Record $16.83 Million On 2014 Lobbying, Topping 15 Tech And Communications Companies; Facebook, Amazon, Apple Also Post Records, http://insidegoogle.com/

Google to extend 'right to be forgotten' to all its domains accessed in EU, http://www.theguardian.com/technology/2016/feb/11/google-extend-right-to-be-forgotten-googlecom?CMP=share_btn_fb

Google vs the EU: Will Google Shut Down It's Search Engine Services in EU?, http://anonhq.com/dont-evil-eu-attempts-make-google-accountable-filling-statement-objections/

Google's right to be forgotten – industrial scale misinformation?, https://edri.org/forgotten/

Hacker releases new purported personal data for top CIA, DHS officials, October 2015, http://arstechnica.com/tech-policy/2015/10/hacker-releases-new-purported-personal-data-for-top-cia-dhs-officials/

Hand over our code to China? We're no commie patsies, Apple cries, http://www.theregister.co.uk/2016/04/19/apple_denies_giving_beijing_user_info/

How Does Data Protection Differ Between China and The West?, http://blog.maytech.net/blog/how-does-data-protection-differ-between-china-and-the-west

How We'll Know the Wikimedia Foundation is Serious About a Right to Remember, http://concurringopinions.com/archives/2014/08/how-well-know-the-wikimedia-foundation-is-serious-about-a-right-to-remember.html

IHS Markit, The economic value of behavioural targeting in digital advertising. Analysis on behalf of IAB Europe and EDAA, 2017, https://datadrivenadvertising.eu/wp-content/uploads/2017/09/BehaviouralTargeting_FINAL.pdf

Improving quality isn't anti-competitive, http://googlepolicyeurope.blogspot.co.uk/2015/08/improving-quality-isnt-anti-competitive.html

In Europe-U.S. Clash on Privacy, a Longstanding Schism, http://www.nytimes.com/2015/10/08/technology/in-europe-us-clash-on-privacy-a-longstanding-schism.html?_r=1

In Europe-U.S. Clash on Privacy, a Longstanding Schism, October 2015, http://www.nytimes.com/2015/10/08/technology/in-europe-us-clash-on-privacy-a-longstanding-schism.html?_r=0

Industry Coalition for Data Protection, http://www.euroispa.org/industry-coalition-for-data-protection/

Informal Comment on the Draft General Data Protection Regulation and Draft Directive on Data Protection Law Enforcement Investigations, https://edri.org/files/US_lobbying16012012_0000.pdf

Interference-Based Jurisdiction Over Violations of the Right to Privacy, http://www.ejiltalk.org/interference-based-jurisdiction-over-violations-of-the-right-to-privacy/

International privacy law and technology scholars recommend practical steps in improving protection for EU and US Internet Users, https://privacybridges.mit.edu/news/international-privacy-law-and-technology-scholars-recommend-practical-steps-improving

Is Facebook the enemy of truth and civic unity?, http://www.theguardian.com/technology/2016/jan/01/facebook-truth-trump-obama?CMP=share_btn_fb

Japan recognises 'right to be forgotten' of man convicted of child sex offences, https://www.theguardian.com/technology/2016/mar/01/japan-recognises-right-to-be-forgotten-of-man-convicted-of-child-sex-offences?CMP=share_btn_fb

Kela website user data ended up with Google, Facebook, February 1, 2020, https://yle.fi/uutiset/osasto/news/paper_kela_website_user_data_ended_up_with_google_facebook/11187895

Let Europeans sue America for slurping their data – US Senate, http://www.theregister.co.uk/2016/02/10/europeans_can_sue_us_government/
Life In The Digital Crosshairs, http://www.microsoft.com/security/sdl/story/#chapter-1
Limit 'Right to Be Forgotten' to Europe, Panel Tells Google, http://bits.blogs.nytimes.com/2015/02/06/limit-right-to-be-forgotten-to-europe-panel-says/?ref=technology
Mark Zuckerberg should spend $45 billion on undoing Facebook's damage to democracies, https://www.washingtonpost.com/opinions/mark-zuckerberg-could-spend-45-billion-on-undoing-facebooks-damage/2015/12/10/4b7d1ba0-9e91-11e5-a3c5-c77f2cc5a43c_story.html
Meet 'Project Zero,' Google's Secret Team of Bug-Hunting Hackers, http://www.wired.com/2014/07/google-project-zero/
Microsoft Admits Windows 10 Automatic Spying Cannot Be Stopped, http://www.forbes.com/sites/gordonkelly/2015/11/02/microsoft-confirms-unstoppable-windows-10-tracking/#174f9bb42f4a
Microsoft escalates ad assault on Google, April 9, 2013, https://eu.usatoday.com/story/tech/2013/04/09/microsoft-google-advertising/2066991/
Microsoft fuels advertising assault against Google, April 9, 2013, https://www.cbsnews.com/news/microsoft-fuels-advertising-assault-against-google/
Microsoft Puts Data Privacy on Its Branding Agenda, http://www.edweek.org/ew/articles/2014/07/09/36microsoft_ep.h33.html
Microsoft Should Act Now To Protect Online Privacy, http://www.consumerwatchdog.org/blog/microsoft-should-act-now-protect-online-privacy
Microsoft Skewers Google For Giving Your Personal Data To App Developers, http://www.consumerwatchdog.org/story/microsoft-skewers-google-giving-your-personal-data-app-developers
Microsoft, Google & friends urge passage of USA Freedom Act, https://gigaom.com/2014/11/17/microsoft-google-friends-urge-passage-of-usa-freedom-act/
Microsoft's plan to avoid a 'return to the digital dark ages' in wake of Safe Harbor decision, October 2015, https://www.washingtonpost.com/news/the-switch/wp/2015/10/20/microsofts-plan-to-avoid-a-return-to-the-digital-dark-ages-in-wake-of-safe-harbor-decision/
Microsoft's plan to avoid a 'return to the digital dark ages' in wake of Safe Harbor decision, https://www.washingtonpost.com/news/the-switch/wp/2015/10/20/microsofts-plan-to-avoid-a-return-to-the-digital-dark-ages-in-wake-of-safe-harbor-decision/
NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE, Appendix A – Fair Information Practice Principles (FIPPs), http://www.nist.gov/nstic/NSTIC-FIPPs.pdf
Netflix Spilled Your Brokeback Mountain Secret, Lawsuit Claims, http://www.wired.com/2009/12/netflix-privacy-lawsuit/
Network Society as a Paradigm for Legal and Societal Thinking (NETSO),
http://www.ulapland.fi/InEnglish/Units/Faculty-of-Law/Institutes/Institute-for-Law-and-Informatics/NETSO-Project
New leaks say NSA can see all your online activities, 31 July 2013, http://net-security.org/secworld.php?id=15328
New Stanford research finds computers are better judges of personality than friends and family, http://news.stanford.edu/news/2015/january/personality-computer-knows-011215.html
New study: Google manipulates users into constant tracking, 27 November 2018, https://www.forbrukerradet.no/side/google-manipulates-users-into-constant-tracking
NSA spying on Europe reflects the transatlantic culture gap by Jan Philipp ALBRECHT, http://www.respect-my-privacy.eu/en/blog/jan-albrecht/nsa-spying-europe-reflects-transatlantic-culture-gap

NSA: our analogue spying laws must catch up with the digital era, http://www.theguardian.com/commentisfree/2013/nov/10/nsa-analogue-spying-laws-surveillance-digital-era
Obama finds bipartisan support for first 'Big Data' privacy plan, http://www.reuters.com/article/2015/02/05/us-usa-privacy-exclusive-idUSKBN0L90D320150205?feedType=RSS&feedName=technologyNews
Once again, the government finds a way to crack an iPhone without Apple's help, https://www.washingtonpost.com/business/justice-department-drops-another-demand-for-apples-help-with-passcode/2016/04/23/4fedbfd8-090c-11e6-bdcb-0133da18418d_story.html
Online privacy will still be a mess a decade from now, experts say, https://gigaom.com/2014/12/18/online-privacy-will-still-be-a-mess-a-decade-from-now-experts-say/
Online Privacy: Who Writes the Rules?, http://www.nytimes.com/2015/01/01/opinion/online-privacy-who-writes-the-rules.html?_r=0
Op-Ed: Restore 'Privacy by Obscurity', http://www.usnews.com/debate-club/should-there-be-a-right-to-be-forgotten-on-the-internet/restore-privacy-by-obscurity
Open Social Networks, http://www.europe-v-facebook.org/EN/Objectives/objectives.html
Overview on Binding Corporate rules, http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm
Parliament seeks global application of EU online privacy rules, http://www.euractiv.com/infosociety/parliament-seeks-tighter-global-news-516943
Preserving Privacy in Belgium, http://cosic-be.blogspot.be/2015/10/preserving-privacy-in-belgium.html
Preserving Security in Belgium, https://www.facebook.com/notes/alex-stamos/preserving-security-in-belgium/10153678944202929
Presidential Policy Directive -- Signals Intelligence Activities, https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities
Presidential Policy Directive -- Signals Intelligence Activities, https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities
Privacy, http://plato.stanford.edu/entries/privacy/
Privacy advocates say NSA reform doesn't require 'technological magic', http://www.csmonitor.com/World/Passcode/2015/0116/Privacy-advocates-say-NSA-reform-doesn-t-require-technological-magic
Privacy Bridges report presented to International Data Protection Commissioner's conference, https://internetpolicy.mit.edu/blog/privacy-bridges-report-presented-international-data-protection-commissioners-conference
Privacy Commission takes Facebook to court, http://deredactie.be/cm/vrtnieuws.english/News/1.2367528?devicetype=mobile
Privacy International, Data Is Power: Profiling and Automated Decision-Making in GDPR, 2017, https://privacyinternational.org/sites/default/files/2018-04/Data%20Is%20Power-Profiling%20and%20Automated%20Decision-Making%20in%20GDPR.pdf
Privacy Matters, http://www.respect-my-privacy.eu/privacy-matters
Privacy shield's future: five things to know, http://www.politico.eu/article/privacy-shields-future-five-things-to-know/
Privacy Shield List, https://www.privacyshield.gov/list
Privacy Shield: Our Concerns with the Data Transfer Agreement, http://www.pastemagazine.com/articles/2016/02/privacy-shield-our-concerns-with-the-data-transfer.html
Privacy Shield Program Overview | Privacy Shield (Privacyshield.gov, 2017) https://www.privacyshield.gov/Program-Overview
Privacy, http://www.consumerwatchdog.org/focusarea/privacy

Project Zero, http://googleprojectzero.blogspot.fi/
ProPublica Launches the Dark Web's First Major News Site, http://www.wired.com/2016/01/propublica-launches-the-dark-webs-first-major-news-site/
Protect your privacy on the Internet, http://www.microsoft.com/security/online-privacy/prevent.aspx
Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers, https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers
Protection Of Personal Data (Ec.europa.eu) http://ec.europa.eu/justice/data-protection/
Recommendation Assessment Report January 29, 2015, https://www.pclob.gov/library/Recommendations_Assessment-FactSheet.pdf
Reform Government Surveillance, http://reformgs.tumblr.com/post/102821955852/open-letter-to-the-us-senate
Report of the Advisory Committee to Google on the Right to be Forgotten, https://drive.google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNbDA/view
Safe Harbor 2.0: Judges to keep NSA spying in check – EU justice boss, October 2015, http://www.theregister.co.uk/2015/10/28/nsa_spying_on_eu_subject_judicial_review/
Safe Harbor 2.0: Judges to keep NSA spying in check – EU justice boss, http://www.theregister.co.uk/2015/10/28/nsa_spying_on_eu_subject_judicial_review/
Safe Harbor ripped and replaced with Privacy Shield in last-minute US-Europe deal, http://www.theregister.co.uk/2016/02/02/safe_harbor_replaced_with_privacy_shield/
Search Engine Market Share Worldwide, March 2020, https://gs.statcounter.com/search-engine-market-share
Secretary's Advisory Committee on Automated Personal Data Systems. Records, Computers, and the Rights of Citizens. Dept. of Health, Educ. and Welfare, July 1973, www.epic.org/privacy/hew1973report/
SIGNALS INTELLIGENCE REFORM. 2015 ANNIVERSARY REPORT, http://icontherecord.tumblr.com/ppd-28/2015/overview
Snowden: FBI's claim that it requires Apple's help to unlock iPhone is 'bullshit', http://thenextweb.com/insider/2016/03/09/snowden-fbis-claim-that-it-requires-apples-help-to-unlock-iphone-is-bullshit/#gref
Staff technologist at the Electronic Frontier Foundation, https://www.eff.org/
Tech giants at war: Changing fortunes of Microsoft and Google, April 10, 2013, https://economictimes.indiatimes.com/corporate-industry/tech-giants-at-war-changing-fortunes-of-microsoft-and-google/slideshow/19470298.cms
TechRadar: Big Data, www.forrester.com/report/TechRadar+Big+Data+Q1+2016/-/E-RES121460
Teenagers under 16 will need parental consent to use Facebook and email under EU laws, http://www.telegraph.co.uk/technology/internet/12049927/Teenagers-under-16-face-being-banned-from-Facebook-and-email-under-EU-laws.html
The Boston Consulting Group, The Value of Our Digital Identity, 2012: 4. www.libertyglobal.com/PDF/public-policy/The-Value-ofOur-Digital-Identity.pdf
The Case For Apple, Facebook, Microsoft Or Google Buying Yahoo Now, http://www.forbes.com/sites/ericjackson/2014/07/21/the-case-for-apple-facebook-microsoft-or-google-buying-yahoo-now/
The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, January 2019, https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

The collapse of the US-EU Safe Harbor: Solving the new privacy Rubik's Cube, http://blogs.microsoft.com/on-the-issues/2015/10/20/the-collapse-of-the-us-eu-safe-harbor-solving-the-new-privacy-rubiks-cube/

The Court of Justice of EU's Judgment on the "Right to be Forgotten": An International Perspective, http://www.ejiltalk.org/the-court-of-justice-of-eus-judgment-on-the-right-to-be-forgotten-an-international-perspective/

The Electronic Privacy Information Center, Complaint And Request For Injunction, Request For Investigation And For Other Relief' (Federal Trade Commission 2007), https://epic.org/privacy/ftc/google/epic_complaint.pdf

The Electronic Privacy Information Center, Assessment Of The FTC'S Prior Actions On Merger Review And Consumer Privacy (2015), https://epic.org/privacy/internet/ftc/Merger-Remedy-3-17.pdf

The Electronic Privacy Information Center and The Center for Digital Democracy, Complaint, Request For Investigation, Injunction, And Other Relief (2016), https://www.democraticmedia.org/sites/default/files/field/public/2016/epic-cdd-ftc-whatsapp-complaint-2016.pdf

The EU's Proposed Data Protection Regulation: Microsoft's Position, http://www.microsoft.eu/2012/03/16/the-eus-proposed-data-protection-regulation-microsofts-position/

The Evolution of Privacy on Facebook, http://mattmckeon.com/facebook-privacy/

The Implications of the European Safe Harbor Decision, http://blogs.cfr.org/cyber/2015/10/07/the-implications-of-the-european-safe-harbor-decision/

The Implications of the European Safe Harbor Decision, October 2015, http://blogs.cfr.org/cyber/2015/10/07/the-implications-of-the-european-safe-harbor-decision/

The Linux Foundation, New Cross-Industry Effort to Advance Computational Trust and Security for Next-Generation Cloud and Edge Computing, August 21, 2019, https://www.linuxfoundation.org/press-release/2019/08/new-cross-industry-effort-to-advance-computational-trust-and-security-for-next-generation-cloud-and-edge-computing/

The Misbegotten 'Right to Be Forgotten', http://www.usnews.com/debate-club/should-there-be-a-right-to-be-forgotten-on-the-internet/the-misbegotten-right-to-be-forgotten

The Misbegotten 'Right to Be Forgotten', http://www.usnews.com/debate-club/should-there-be-a-right-to-be-forgotten-on-the-internet/the-misbegotten-right-to-be-forgotten

The International Organization for Standardization/the International Electrotechnical Commission standard 2382-8: 1998(en), Information technology — Vocabulary, https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en:term:2126318

The right to be forgotten and the global reach of EU data protection law, http://concurringopinions.com/archives/2014/06/the-right-to-be-forgotten-and-the-global-reach-of-eu-data-protection-law.html

The Right to Be Forgotten Becomes Possible on the Blockchain, http://cryptotimes.org/blockchain/right-forgotten-becomes-possible-blockchain/

The Right to Privacy Is Global, http://www.usnews.com/debate-club/should-there-be-a-right-to-be-forgotten-on-the-internet/the-right-to-privacy-is-global

The Search for Harm, https://googleblog.blogspot.co.uk/2015/04/the-search-for-harm.html

The Slow Death of 'Do Not Track', http://www.nytimes.com/2014/12/27/opinion/the-slow-death-of-do-not-track.html?module=Search&mabReward=relbias&

The Top 10 Blockchain Takeaways From Europe's Trustech Conference, https://www.forbes.com/sites/laurashin/2016/12/05/the-top-10-blockchain-takeaways-from-europes-trustech-conference/#6bb7a0e97ba6

The USA Freedom Act: A Partial Response to European Concerns about NSA Surveillance, http://peterswire.net/wp-content/uploads/gtjmce2015-1-swire.pdf

The US Will Cede Control of the Internet for the First Time, http://motherboard.vice.com/read/the-us-will-cede-control-of-the-internet-for-the-first-time-1
The value of data, 22 September 2017, https://www.weforum.org/agenda/2017/09/the-value-of-data/
Thomson Reuters Practical Law. Data Protection in the United States. July 1, 2015. http://us.practicallaw.com/6-502-0467
Tor Anonymity: Things Not to Do, January 4, 2016, https://news.ycombinator.com/item?id=10833629
Transparency Report. Requests to delist content under European privacy law, https://transparencyreport.google.com/eu-privacy/overview?hl=en
US Companies Are Throwing a Fit Because They're Losing Control Over the Internet, http://motherboard.vice.com/read/us-companies-are-throwing-a-fit-because-theyre-losing-control-over-the-internet
U.S. Attitudes Toward the 'Right to Be Forgotten' IndustryView, 2014, http://www.softwareadvice.com/security/industryview/right-to-be-forgotten-2014/
U.S. attorney general criticizes Apple, Google data encryption, http://www.reuters.com/article/2014/09/30/us-usa-smartphones-holder-idUSKCN0HP22P20140930
U.S. to Back Privacy Resolution It Knee-Capped, http://foreignpolicy.com/2013/11/23/u-s-to-back-privacy-resolution-it-knee-capped/
US Attorney Gen latest to roast Apple, Google mobe encryption, http://www.theregister.co.uk/2014/10/01/us_attorney_general_piles_on_phone_encryption_criticism/
US claim on the world's servers at a crossroads, September 2015, http://arstechnica.com/tech-policy/2015/09/us-claim-on-the-worlds-servers-at-a-crossroads/
US Government just unlocked the San Bernadino iPhone, tells Apple 'never mind', http://thenextweb.com/apple/2016/03/29/us-government-just-unlocked-the-san-bernadino-iphone-tells-apple-never-mind/
US lobbying waters down EU data protection reform, http://www.euractiv.com/specialreport-data-protection/us-lobbying-waters-eu-data-prote-news-510991
US lobbying waters down EU data protection reform, http://www.euractiv.com/specialreport-data-protection/us-lobbying-waters-eu-data-prote-news-510991
We Are All Foreign Nationals — Even Orin Kerr, https://www.justsecurity.org/2817/foreign-nationals-orin-kerr/
We Are All Foreigners: NSA Spying and the Rights of Others, https://www.justsecurity.org/2668/foreigners-nsa-spying-rights/
Weighing a Schengen zone for Europe's Internet data, http://www.dw.com/en/weighing-a-schengen-zone-for-europes-internet-data/a-17443482
What are the odds for Europe-v-Facebook's latest challenge over personal data?, http://www.dw.com/en/what-are-the-odds-for-europe-v-facebooks-latest-challenge-over-personal-data/a-17847438
What does the end of Safe Harbour mean for you?, http://www.wired.co.uk/news/archive/2015-10/06/what-does-the-end-of-safe-harbour-mean
What is Facebook doing with my data?, http://www.bbc.com/news/magazine-34776191
What is the impact of blockchains on privacy? https://theodi.org/blog/impact-of-blockchains-on-privacy
What's Wrong with the Proposed EU Right of Data Portability?, https://fpf.org/2012/10/17/whats-wrong-with-the-proposed-eu-right-of-data-portability/

WhatsApp and iMessage could be banned under new surveillance plans, http://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-and-snapchat-could-be-banned-under-new-surveillance-plans-9973035.html
WhatsApp Blog, Facebook, https://blog.whatsapp.com/499/Facebook?
WhatsApp FAQ, I Have Questions About the Updated Terms of Service and Privacy Policy, https://faq.whatsapp.com/general/28030012
WhatsApp Security and Privacy, How do I choose not to share my account information with Facebook to improve my Facebook ads and products experience?, https://faq.whatsapp.com/en/general/26000016
WhatsApp with your Facebook data?, http://www.dw.com/en/whatsapp-with-your-facebook-data/a-17446624
When the right to be forgotten becomes possible on the Ethereum blockchain, https://www.newsbtc.com/press-releases/bcdiploma-right-to-be-forgotten-ethereum-blockchain/
Which tech companies back SOPA? Microsoft, Apple, and 27 others, http://thenextweb.com/insider/2011/11/17/which-tech-companies-back-sopa-microsoft-apple-and-27-others/
Why a Facebook 'Sympathize' Button Is a Terrible Idea, http://time.com/3632244/facebook-dislike-sympathize-like/
Why it's time for Facebook to offer a "pay for privacy" feature, https://gigaom.com/2014/11/13/why-its-time-for-facebook-to-offer-a-pay-for-privacy-feature/
Windows 10 Worst Secret Spins Out Of Control, http://www.forbes.com/sites/gordonkelly/2016/02/09/windows-10-data-tracking-spying-levels/#492e2f287aa9

UNTITLED LINKS

http://blogs.microsoft.com/on-the-issues/2015/01/28/data-privacy-day-2015-putting-people-control/
http://codebutler.com/
http://definitions.uslegal.com/m/mass-surveillance/
http://digital-era.net/active-surveillance-program-xk-eyscore/
http://ec.europa.eu/justice/news/consulting_public/0003/contributions/citizens/kilian_wolfgang_en.pdf
http://edri.org/files/holder.pdf
http://en.wikipedia.org/wiki/List_of_government_mass_surveillance_
http://europa.eu/transparency-register/
http://faculty.fordham.edu/jreidenberg/
http://freedomfromfb.com/
http://github.com/10se1ucgo/DisableWinTracking
http://globetrotter.berkeley.edu/people/Castells/castells-con4.html
http://googleonlinesecurity.blogspot.fi/2014/07/announcing-project-zero.html
http://ipdb.io/
http://lumiaconversations.microsoft.com/2015/01/28/stop-think-connect-safeguarding-online-reputation/
http://net-security.org/secworld.php?id=15328
http://networksociety.org/about
http://research.microsoft.com/en-us/projects/privacy_in_metering/3
http://unstats.un.org/unsd/snaama/Index
http://www.aclu.org/about-aclu-0
http://www.brunswickgroup.com/

http://www.civic.com/intel
http://www.eff.org/de/issues/do-not-track
http://www.ethereum.org/
http://www.export.gov/safeharbor/index.asp
http://www.hrw.org/sites/default/files/related_material/UNGA_upload_0.pdf
http://www.informationshield.com/
http://www.informationshield.com/usprivacylaws.html
http://www.internet-sicherheit.de/?L=2
http://www.internetworldstats.com/stats.htm
http://www.microsoft.com/security/online-privacy/prevent.aspx
http://www.oecd.org/sti/ieconomy/privacy.htm
http://www.oed.com/view/Entry/151596?redirectedFrom=privacy
http://www.pewinternet.org/
http://www.privacyinternational.org/
http://www.staysafeonline.org/
http://www.staysafeonline.org/
http://www.staysafeonline.org/data-privacy-day/
http://www.teamliquid.net/forum/general/229525-nsfw-exploring-the-hidden-internet-deep-web/
http://www.torproject.org/
http://www.ulapland.fi/InEnglish/Units/Faculty-of-Law/Institutes/Institute-for-Law-and-Informatics/NETSO-Project
http://www.vbprofiles.com/companies/3e122f809e597c10032cd724
http://ycharts.com/companies/