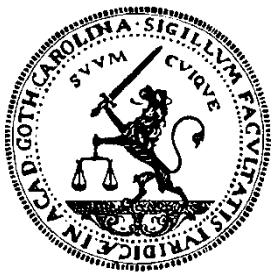

FACULTY OF LAW
Lund University

Beatrice Edler

Sustainable Data Privacy Protection in Commercial Practices

Commercial Aspects on the Data Privacy Protection of Individuals in the European Union Compared to the United States, and Technical Implications

JURM02 Graduate Thesis

Graduate Thesis, Master of Laws program
30 higher education credits

Supervisor: Professor Karol Nowak

Semester of graduation: First Period, Spring Semester 2017

Contents

Summary

Individuals as consumers in the EU and the U.S. are increasingly utilizing data collecting solutions on a daily basis to benefit from smart and efficient lifestyles. By providing personal data directly or indirectly to data service providers, processors or controllers; commercial actors have advantageous possibilities to track, obtain, process, monitor, transmit, and store personal data to improve businesses based on consumer behavior.

The processing of personal data in and between the EU and the U.S. is a critical issue that threatens the fundamental right to privacy and data privacy. Individuals lack the ability to control personal data, and are not fully able to consent to what functionalities or operators that can obtain the personally attributed information. The commercial data practices for processing personally attributed data need more sustainable solutions in order to maintain an appropriate exchange of personal data, and the prospering of innovation and economical growth in and between the EU and the U.S.

In this thesis I argue that commercial actors, as in data providers, processors and controllers, shall consider a sustainable and eco-system thinking strategy when conducting or developing data practices in the EU and/ or the U.S. I also argue that individuals as data subjects must correspondingly be better informed and aware of their right to data privacy. In order to formulate sustainable data processing practices and compliance within the commercial sector, there are three major underlying factors that must be analyzed. (1) In order to protect data privacy, individuals and commercial actors must understand why it is important to protect privacy, and the importance of sustainable data development. Secondly, (2) the legal protection of data privacy in and between the EU and the U.S. must be evaluated whether they are protecting individuals' privacy sufficiently. Finally, (3) to implement practically applicable data compliance practices among commercial actors, the technical solutions must be adjusted and analyzed in order to see how sustainable data privacy protection best can be managed.

International frameworks and policy-making, national regulators, and law enforcement mechanisms can serve as guidelines and supervising entities. I argue, however, that the best protection of data privacy is a matter of the relationship between the individuals and the commercial actors. Sustainable data privacy protection must derive from incentives among business actors, and be addressed on a narrow scale with understanding of the importance of sustainable values in the future data development.

Sammanfattning

Individer i egenskap av konsumenter och dataanvändare inom EU och USA använder datalösningar i en allt större utsträckning. Detta för att använda och kontrollera personliga ägodelar och ekonomiska medel, engagera i sociala nätverk samt få tillgång till platstjänster och vardaglig effektivitet. Kommersiella aktörer som exempelvis erbjuder datasortering samt systemvaror eller hårdvaror tillhandahåller digitalt anpassade lösningar mot att få tillgång till personlig data från individer. Företag som säljer eller kontrollerar data, marknadsföretag samt andra aktörer anpassade för IT lösningar får därmed goda förutsättningar att registrera, använda, vidarebefordra samt lagra personlig data för olika kommersiella ändamål och framförallt i marknadsföringssyfte.

EU och USA är de mest utvecklade IT-regionerna i världen. Databehandling av personlig data inom och mellan EU och USA är en kritisk fråga och den transnationella databehandlingen är ansedd vara ett hot mot den fundamentala rättigheten till privatliv och framförallt rätten till personlig data. Individers möjlighet till att samtycka och kontrollera spridning av personlig data är av särskild betydelse, där kommersiella aktörer har ett försprång i både kunskap och ekonomiska förutsättningar. Datahanteringen mellan EU och USA måste därför präglas av innovativa och hållbara lösningar, för att skapa balans mellan individers rätt till personlig data och kommersiella ekonomiska intressen och tillväxt.

I den här uppsatsen argumenterar jag för att dataföretag som behandlar, säljer eller kontrollerar data för kommersiella ändamål måste överväga hållbart strategiska lösningar när de driver eller utvecklar företagsverksamhet i och mellan EU och USA. Ämnet ”data privacy” är synnerligen nytt och kräver regulativ vägledning, inte minst i egenskap av branchpraxis. Följaktligen måste även individer få större förståelse och mer kvalitativ information om datahantering i EU och USA.

För att utveckla en hållbar strategi för kommersiella aktörer i datahantering måste tre huvudsakliga områden analyseras: (1) företag och individer måste få kunskap om bakomliggande sociala värderingar i benämningen ”privatliv”, och förstå vikten av att skydda individers rätt till privatliv inom data. Rätten till privatliv måste också balanseras gentemot andra intressen, varav teorier om hållbarhet belyser en potentiell lösning för detta. Vidare, (2) det juridiska perspektivet i och mellan EU och USA måste beaktas för hur rätten till privatliv regleras och huruvida rätten till privatliv är tillräckligt skyddad. Slutligen (3) måste praktiska datalösningar där personlig data förekommer utvärderas för att utveckla fungerande strategier där både personlig data och ekonomiska incitament kan respekteras och få utrymme. Lösningen för hållbar datahantering inom IT-företag där både individers rätt till privatliv och ekonomiska intressen kan utvecklas finns i interaktionen mellan individer och kommersiella aktörer. Det är där förändring kan ske, med rätt initiativ, i en hållbar riktning.

Acknowledgements

I would like to direct my gratitude to my supervisor and mentor, Karol Nowak, for the support when conducting the research and work with this graduate thesis in Masters of Laws, Lund University. Further, I would like to thank all of my previous professors at Lund University, Sheffield University and Columbia University in the City of New York for supporting my interest in the IT legal perspective, and for excellent tutoring during my studies. Also, I am grateful for all fellow students I have met during my studies at all faculties that I have learned much from, and will hopefully be my friends for life. Further, my family and friends for supporting me during my studies.

Finally, I would like to thank my internship supervisors and fellow colleagues at Unacast Inc., New York, for taking me under their wings and letting me experience IT law in practice. I hope to further specialize in the field and to contribute to the developing technology in a legal perspective in the future.

Beatrice Edler, May 21, 2017.

Abbreviations

CCPR	Human Rights Committee of the United Nations
CIA	Central Intelligence Authority of the United States
DoC	Department of Commerce of the United States
DPA	Data Protection Authority
ECPA	The Electronic Communications Privacy Act of 1986
EUCJ	European Union Court of Justice
FCC	Federal Communications Commission (U.S.)
FTC	Federal Trade Commission (U.S.)
GDPR	General Data Protection Regulation (EU)
IoT	Internet-of-Things; Internet-based information architecture programmed in products such as cars, thermometers etc, facilitating digital exchange of goods and information infrastructure
NSA	National Security Authority of the United States
OECD	Organization for Economic Co-operation and Development
PII	Personally Identifiable Information (U.S.)
UN	United Nations

1 Introduction

1.1 Background

The implication of privacy is a subject in disarray in the academic and legal history. The concept of privacy has historically been understood as the dichotomy of privacy between individuals versus privacy between the state and citizens. In the past decades we have witnessed antagonism for governmental surveillance, such as the NSA, and the necessity to protect individuals from public interference. Thus, privacy concerns between private commercial actors versus individuals as consumers is a growing concern, emphasizing how businesses and individuals should interact in the IT environment on a daily basis.

This thesis focuses on the commercial perspective of data privacy and how individuals' daily lives are affected by commercialization of personal information. As IT is becoming a crucial apparatus for businesses purposes, individuals' privacy is vulnerable to commercial personalization. IT has facilitated enormous technical advantages for businesses to find, retain, and evaluate consumers by profiling, targeting, monitoring, transmitting, and storing individuals' personal data. In a commercial perspective, "personal data" in EU definition, or "personally identifiable information"[1] in the U.S., has become the new monetization of commercial purposes.

Philosophers, lawyers, justices and privacy experts have concluded that the current research status of data privacy is challenged by individuals' demands for transparency, efficiency, accessibility, and security. Simultaneously, individuals and regulators on national and international level demand higher privacy protection in innovation due to the imbalanced power between commercial actors and individuals as consumers.

In order to shape solutions between the commercial interests and the individuals' privacy concerns, benefiting economical growth for businesses as well as safer practices to protect individuals' privacy; the solutions must be sustainable. In this thesis I refer to "sustainability" as the long-term balancing interest in social and economical values between individuals and commercial actors. This thesis outlines a practical eco-system thinking model for how commercial interests and privacy are able to align in a sustainable direction for commercial development.

[1] [Hereinafter: "PII"].

1.2 Purpose

The purpose of this thesis is to present fundamental factors for commercial actors to take into account when implementing a strategic compliance model for data practices, to develop more sustainable data processing practices. Focus will be on commercial services implying processing, collecting, monitoring, transmitting and storing of personally attributed data in and between the EU and the U.S. Focus will further more be on the individual's right to data privacy. The strategy presented in this thesis highlights the necessity to take into account social values of privacy, the legal status in the EU and the U.S., and the practical implication of regulative compliance in innovation.

1.3 Research Question

The research question in this thesis is *how data privacy protection can be more sustainable in commercial data processing practices*. The question captures what social, legal and technical factors must be taken into account for developing more sustainability in commercial data processing of personally attributed data. Further, how commercial sustainability practically impact businesses engaging in processing, monitoring, transmitting and storing of data containing personal attributes to consumers. The question will be addressed to the relationship between the EU and U.S. as two of the most IT developed economies in the world.

1.4 Theory

The central theory of this thesis is that in order to economically benefit commercial actors and innovators in IT, and simultaneously ensure safer practices to protect consumers' privacy; data services, products, and functionalities must be implemented and adjusted to sustainable data privacy solutions. The relationship between individuals' privacy and commercial interests must be better balanced, where individuals' data privacy must be stronger positioned in commercial values.

The term privacy has shaped several recognized fundamental human rights in conventions, EU directives and regulations, U.S. national legislation, transnational collaborations, and best practices among companies.[2] Data privacy as a democratic value is setting new history in commercial, social, and legal aspects in the current time frame. Due to commercial, social and legal development of the notion of data privacy, this thesis emphasizes that sustainable data privacy protection must be studied based on (1) social underlying values behind data privacy, (2) the legal and regulative status of

[2] The critical regulations supporting this aspect, for instance article 8 of the European Convention and precedents from the U.S. Supreme Court, will be exclusively presented in chapter 5.

data privacy, and (3) practical capabilities to comply with sustainable data practices in technological perspectives.

In order to strengthen data privacy in commercial aspects, commercial data actors must initiate awareness of data privacy in their business models. Pressure must derive from regulators, law enforcement mechanisms, and individuals, but also from other commercial actors. By strengthening the understanding and importance of data privacy among regulators, commercial actors, and individuals, the laws and judicial powers will be able to create better guidelines resulting in better compliance among data companies. There has to be a systematic symbiosis between federal States/ EU Member State regulators, judicial powers, and corporate governance promoting early steps towards incentivizing data privacy and compliance inhibited in business models. Additionally, individuals as consumers must be better informed and involved in data processing practices and their right to data privacy. When commercial actors and innovators are aware and comprehend the importance of protecting data privacy, they can develop sustainable data products and services.

1.5 Method and Material

This thesis has a comparative aspect, focusing on the EU and the U.S., in order to highlight how two of the largest IT-economies impact the status of the transnational data privacy protection.[3] The two economies are currently representing approximately 50 % of the world's GDP and have established an extensive trade and business relationship, where data solutions are becoming a crucial component.

This thesis has a cross-disciplined research approach. First, it is examining a philosophical spectrum on privacy and underlying values of sustainable development.[4] Thereafter, a legal dogmatic method analyzing the legal current standpoint of data privacy in the EU on interstate level and on federal level in the U.S. Finally, standpoints and research from a technical perspective is presented regarding how the conclusions from the philosophical and legal sections impacts the practical compliance among commercial actors.[5] The cross-disciplined method is utilized due to the disarray and undetermined regulative research status of the topic. The right

[3] Compare to theorists such as Bogdan, Michael, *Komparativ rätt: Comparative Law*, Juridiska föreningen, Lund 1978; and Thomason, Sara Grey and Kaufman, Terrence, *Language Contact, Creolization, and Genetic Linguistics*, University of California Press, 1988 (note: this thesis will not explain comparative law as part of the thesis. This thesis will be limited to privacy and data privacy as the notions for comparison in regulations in the EU and the U.S.).

[4] Philosophers, metaphysicians and privacy theorists such as Ruth Gavison, Judith D. Thomson, Helen Nissenbaum, Judith DeCew, Richard Posner, Charles Fried, Jeffrey Reiman, Allan Westin, and Daniel Solove are mentioned; see chapter 3 and 4.

[5] Data privacy and security experts or organizations such as Bruce Schneier, Edward Snowden, Professor Monica Lam, FTC Commissioners and institutional organizations representing the EU or the U.S.

to data privacy and how it will affect future commercial compliance is a new phenomenon and is constantly changing in the current time frame.

The reader of this thesis should be aware of that the descriptive and analyzing parts are merged to better connect the cross-disciplined approach. Additionally, as the topic is under regulative change and development, it is required to discuss *potential* outcomes, however based on existing regulations and guidelines.

The sources referred to in this thesis derive from varying aspects. Due to graduate studies in English, and the majority of sources are written in English, this thesis is written in English. Conventions, regulations, directives, case law and institutional documents from EU legislators are analyzed. The U.S. Constitution, federal laws, precedents, and sectorial data branch practices are evaluated. The transnational data transfer framework EU-U.S. Privacy Shield is presented. In order to understand the starting points and incentives for the regulations in the EU and the U.S., reports and research undertaken by global organizations such as the UN and OECD are evaluated. For critically analyzing the current level of protection; stakeholder consultations from organizations as well as individuals are presented. Furthermore; interviews, reports, webinars and conferences presented by IT experts, data companies, and privacy lawyers are analyzed. Literature, reports, and journals written by privacy theorists in the U.S. as well as the EU are presented to emphasize discussions related to data privacy.

1.6 Limitations

This thesis focuses on data privacy of individuals interacting as consumers in commercial aspects, called “data subjects”. The analysis of data privacy is based on discussions of the “traditional” right to privacy. This thesis presents discussions of privacy starting in late 1700 until today, and the term “data privacy” is considered introduced in the 1960s due to the information technology boom, which influenced the legal protection of privacy extensively.

This thesis recognizes the different definitions of “personal data” in the EU privacy laws, and “personally identifiable information” in the federal U.S. privacy laws.[6] In this thesis, the definitions imply data with personal attributes that can be related to a natural person, and focus will be on the aspect of consent and control over personal information. Each country in the EU is not presented due to the limitation of this thesis. The same applies to each Federal State in the U.S., which are not analyzed.

The terms “data privacy” and “data protection” are diligently associated with each other in this thesis. The term “data protection” implies the

[6] Both definitions; ”personal data” and ”personal identifiable information”, will be presented exclusively in chapter 5.

regulative aspect of data privacy, whilst "data privacy" is presented as the general understanding of privacy in the context of data and IT. The term "data security" will not be analyzed as data security mainly focuses on the protection of data systems, or the right to privacy for other non-natural persons.

Data privacy practices analyzed in this thesis will be limited to two types of commercial services implying processing, monitoring, using and storing of personal data. The first type of data processing highlights the concerns over transmitting of personal data in social networks, such as Facebook Inc., to third parties. The second type of concern is the complexity of data processing and the interconnectedness when attempting to control personal data between hardware and software systems, as in Internet-of-things.

This thesis will not analyze governmental liabilities to data subjects in the EU and the U.S. Privacy of employees, data privacy in financial services, and data privacy regarding medical records are not analyzed.

1.7 Outline

This thesis is explaining sustainable data privacy in three major parts. Each part has its own conclusions and entails embedded analyses, in order to benefit the understanding of the intersectional approach and tie them together. The first part includes the philosophy and underlying values of privacy that is presented in chapter *two*. Chapter t*wo* is necessary in order to understand the context of data privacy, which is presented in chapter *three*. The implication of sustainable development will be analyzed in chapter *four*. The first part assists to better understand the social values underlying the legal protection of privacy.

The second part and chapter *five* presents and analyzes the legal status of data privacy in the EU and the U.S. Chapter *six* complements by presenting and analyzing the transatlantic data transfer framework between the EU and the U.S.

In the third part, technical implications and how data privacy is impacting practical solutions is analyzed in chapter *seven*. Chapter *eight* will present concluding remarks in sustainable protection of personal data and data privacy, by presenting earlier conclusions in this thesis.

2 The Right to Privacy

2.1 Introductionary Notes

What is privacy and why should we express concern over privacy? According to extensive research undertaken by numerous privacy experts starting in the 1960's until today, experts argue that privacy is threatened, diminishing, at stake, crucial for humanity and a growing interest in society. Furthermore, experts express concern over the unawareness, or perhaps ignorance, of individuals in society and the absence of privacy in our priorities. Citizens are unaware of the importance of protecting privacy and laws are failing in recognizing sufficient consistency in privacy protection.[7]

The legal right to privacy derives from social values and norms in society, and must reach a sufficient level of ethical standard in society to be subject to legal protection. Privacy is a legal right and freedom and recognized as a basic human right according to several human rights declarations worldwide, such as article eight in the European Convention of Human Rights and precedents in the U.S. Supreme Court.[8] Thus, legal frameworks are countering difficulties on a transatlantic scale regarding the right to privacy, especially in terms of its meaning, scope and functions. It is therefore evident to determine what privacy entails. Continuously, this chapter discusses the social core elements of privacy from a philosophical perspective.

This chapter presents varying aspects from privacy experts on privacy and its meaning and scope. The presented authors in this chapter emphasize the differentiating ideas of privacy in the individual's perspective of social values, and are the most referred authors and experts in privacy. This chapter set forth the initial argument that privacy has several different shapes depending on the context. Although, privacy must be stronger positioned as a moral and ethical norm among individuals, corporations and governmental institutions in order to be protected fully.

2.2 The Definition of Privacy

The definition of privacy is a widely attempted challenge and has been analyzed and formulated by several legal and philosophical experts. Despite several intellectual attempts to find common denominators, theorists have failed to develop an exhaustive definition of privacy. A problematized core factor is the difficulty to determine the status and characteristics of privacy.[9]

---

[7] Solove, Daniel J., *Understanding Privacy*, Harvard University Press, Cambridge Massachusetts, London, England, 2008 [Solove, 2008], p. 6.
[8] These frameworks and laws will be explicitly presented in chapter 5.
[9] Gavison, 1980, p. 424.

Privacy is encompassing several components that can be associated to the human nature and mental as well as physical state. The term includes individual's control over personal information and body, freedom of thought, and the freedom to be let alone in one's personal sphere.[10] Further, it could be associated with personal relationships, integrity, and personhood.[11] Privacy enables individuals to create and manage boundaries and barriers towards other people, and is essential to autonomy, dignity and serves as a ground stone for other human rights and freedoms.[12]

Modern theorists have developed a methodology that captures two ways of determining the definition of privacy; a descriptive definition of privacy, and a normative concept of privacy.[13] A descriptive concept of privacy refers to its independent implication without positioning privacy in a context, situation or associated with other values. A descriptive definition implies that privacy is worthy to protect as a right itself. Although, several theorists argue that privacy must be positioned in different contexts and has to be evaluated in its protected interest and underlying values. Such attempt to define privacy is a normative explanation.[14] Privacy experts have extensively argued both aspects.[15] A selection of the most referred authors and experts in privacy below clarifies the different approaches to define privacy.

2.2.1 Limited Access to Private Information

Privacy expert Ruth Gavison has predominantly argued in favor of a descriptive concept of privacy. Gavison argues that our interest of privacy is due to "*our interest of accessibility to others*". Further, that "*[w]e accept the need for privacy as an indication of the limits of human nature"*.[16] Gavison explains that protection of privacy entails the limitation of access for someone to another individual's personal information.[17]

Gavison depicts that there must be a descriptive concept of privacy in order to determine when there has been a loss of privacy. However, a loss of privacy is not necessarily a violation or intrusion of privacy since the loss

[10] Solove, 2008, p. 1.
[11] Gavison, 1980, p. 424.
[12] Privacy International, Explainers, *What is Privacy?*, April 6, 2017.
[13] See for instance Nissenbaum, Helen, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford Law Books, November 2009 [Nissenbaum, 2009], p. 68; and Judith DeCew, Stanford Encyclopedia of Philosophy, *Privacy*, May 14, 2002; substantive revision August 9, 2013 [DeCew, 2002 (revision 2013)].
[14] Nissenbaum, 2009, p. 68; compare with DeCew, 2002 (revision 2013).
[15] Gavison, 1980; DeCew, 2002 (revision 2013); Solove, 2008; Fried, Charles, *Privacy*, The Yale Law Journal, Vol. 77, No. 3 (Jan., 1968), pp. 475-493 [Fried, 1968]; Reiman, Jeffrey, *Privacy, Intimacy and Personhood*, Philosophy and Public Affairs, Vol. 6, No. 1 (Autumn 1976), publ. Wiley, pp. 26-44 [Reiman, 1976]; Thomson, Judith Jarvis, *The Right to Privacy*, Philosophy and Public Affairs, Vol. 4, No 4 (Summer, 1975), publ. by Wiley, pp. 295 – 314 [Thomson, 1975]; and further on, see theories presented below.
[16] Gavison, 1980, 452.
[17] *Ibid*., p. 424.

could be "waived" by an individual with consent.[18] Gavison describes a state where there is no privacy as;

> "[…] *Total lack of privacy is full and immediate access, full and immediate knowledge, and constant observation of that individual […]".*

A person who would have his or her thoughts constantly analyzed and processed would develop an un-personal lifestyle, attempting to compress thoughts that he or she would not want to be disclosed. Such behavior would be devastating for human nature and would force individuals to give up uniqueness and personality. However, full disclosure and transparency could also make citizens safer, decrease criminality, and enemies could be detected sooner.[19] By the time Gavison published her article in 1980, the world appeared different in terms of information flows and especially in terms of digital-based services. The scenario Gavison describes as a state of "full lack of privacy" would not differ significantly from our current state, where we are witnessing more transparency than ever.

Gavison's theory and the descriptive definition of privacy is questionable. A descriptive approach is lacking the flexibility that privacy requires in order to address privacy and all its different scenarios in the human social life. Privacy is not only encompassing an individual's right to limit access by others to one's private information, but privacy could also be freedom from being harassed, sexual and family life, or being subject to tolerate noise by a neighbor next door.[20]

Argued by privacy expert Daniel J. Solove, privacy is dependent on social structures and norms developed and dynamically changing in society, and a descriptive concept of privacy tends to be objective. Privacy is highly subjective, a difficult characteristic when formulating a definition for privacy. A descriptive definition of privacy is therefore ignorant to several evident components of human life, and important factors explaining privacy.[21] Unlike Solove, Nissenbaum refers to Gavison as having the most suitable concept of privacy, as it facilitates the ability to discuss different levels of privacy without having any values or interests prevailing one another.[22] However, without a normative approach to privacy one cannot presume the situations for when privacy must be protected, and why we must protect privacy. Additionally, the values behind the term "privacy" are not taken into account in a descriptive definition.[23]

---

[18] Gavison, 1980, p. 424.
[19] *Ibid.*, p. 443.
[20] Compare to Solove, 2008, p. 21.
[21] Solove, Daniel J., *Conceptualizing Privacy*, California Law Review, Vol. 90, No. 4 (Jul., 2002), pp. 1087-1155 [Solove, 2002], p. 1129-1132.
[22] Nissenbaum, 2009, pp. 62-63.
[23] *Ibid.*, pp. 68-70.

Gavison's theory that privacy would be descriptive and be defined as the limitation of access to other's personal information falls short. With support from Nissenbaum, Gavison argue that privacy must be defined isolated from other values and contexts. However, in order to successfully isolate the right attributes of privacy, one must be certain of what values and factors that comprise the term "privacy", and Gavison does not persuade that her definition is exhaustive. With support in Solove's argument, privacy cannot solely be objectively defined as a limitation of access to someone's personal information. Continuously, privacy must be placed in context to other social values, interests and situations, as in a normative definition.[24]

2.2.2 Personhood, Intimacy and Integrity

Privacy has been argued as "moral capital" when creating or developing relationships, friendships and trust between people. As moral capital, Charles Fried explains that the intangible character of privacy, as our closest and most intimate capital, facilitates the development of our inner connection with other people. Privacy is also connected to intimacy and integrity, a part of human nature to fulfill self-respect, the ability to fully live an intimate life with oneself as well as with others, and the ability to love, care and be spontaneous.[25]

Fried's comprehension of privacy is deeply influenced by moral grounds, as in rights and values that all people should be equally entitled to as a result of human personhood.[26] Fried's theory is that privacy is not simply an interest or value that serves to protect other values or interests, but the fundamental factor for humanity. Human integrity, personhood and intimacy would diminish without protection of privacy.[27]

Even though Fried analyses privacy abstract as an intangible moral value and therefore difficult to apply to practical legal claims, he problematizes how to protect the components that occur in a state of love, trust or friendship; components that are therefore difficult to protect legally. Fried's analysis is therefore promoting the idea of privacy as an ultimate value, evaluating privacy as a higher value that cannot be described materially.

Fried's theory of privacy falls short in terms of explaining when a state of relationship, trust, love, care, and self-respect is occurring, and when privacy is lost, violated or intruded, and will be difficult to establish in objective legal aspects. Further, it falls short in capturing other attributes in personal lives such as unwanted access to personal property, or disclosure of personal information other than personal relationships.

---

[24] Solove, Daniel J., *Conceptualizing Privacy*, California Law Review, Vol. 90, No. 4 (Jul., 2002), pp. 1087-1155 [Solove, 2002], p. 1129-1132.
[25] Fried, 1968, p. 482.
[26] *Ibid.,* p. 478.
[27] *Ibid.*, 1968, p. 477.

2.2.3 Privacy as an Economic Interest

The difficulty to determine any loss of privacy if there is no concrete method to measure the term "privacy" has been problematized by the American former judge and economist Richard Posner. According to Posner, there are three aspects of privacy; the concealment of information, the wish to be left alone without invasion of others in one's private sphere, and the sense of autonomy and freedom.[28]

Posner argues that the aspect of privacy is an economic interest, and that higher economical incitement is related to the wish for increased privacy. For instance, the wish to be left alone could be argued as an economic incitement for why certain individuals in chief positions would have private offices, and other employees do not. Further, he argues that for the same reason workers and consumers develop particular behavior for protecting their economic interests, individuals develop the interest to shield their private information connected to their economic interest.[29]

Concealment involves an element of secrecy, where an individual wants to hide particular information that could harm the individual if the information would be disclosed. In terms of a consumer and vendor relationship, the vendor is dependent on information obtained by the consumer in order to maximize the efficiency on his or her market. By reducing access of information of the consumer for the vendor, the consumer will not be completely exposed to the vendor.[30]

Posner's theory is arguing that privacy is normative, and if certain kind of information could be hidden, it could reduce market efficiency.[31] Posner's theory is mainly focusing on the economical incitement for businesses when collecting personal information about consumers. By taking Posner's perspective, privacy becomes an obstacle for developing profitable businesses.

Privacy as an undesirable value in economic terms should be criticized. Posner's theory is falling short in terms of valuing other efficiency incitements of privacy in the economical perspective; such as trust, goodwill, good consumer relations, social dignity and integrity, and safeguarding fundamental democratic rights and freedoms of individuals. There are risks associated with the concept of privacy as an economic incentive since privacy encompasses other intangible aspects of values such as dignity, intimacy and personhood.[32]

---

[28] Posner, Richard A., *The Economics of Privacy*, The American Economic Review, Vol. 71, No. 2, Papers and Proceedings of the Ninety-Third Annual Meeting of the American Economic Association (May, 1981) [hereinafter: Posner, 1981], pp. 405-409, p. 405.
[29] Posner, 1981, p. 405.
[30] *Ibid.*, p. 405.
[31] Posner, 1981, p. 407.
[32] Compare to Fried, 1968.

2.2.4 Privacy Clustered to Other Rights

As several privacy theorists have argued that the definition of privacy is normative, it becomes evident to establish to what extent privacy is normative and dependent on other values and contexts. Moral philosopher and metaphysician Judith J. Thomson explains that the right to privacy is a right dependent on other rights and not existing itself. Thomson argues that the right to privacy has a plausible effect, where a violation of privacy also consists a violation of another value or right. Her theory captures situations where privacy coexists with other typical legal interests and the protection of interests, such as the right to own your property or to keep something confidential.[33]

Thomson explains that by spreading confidential information without consent would be a violation of privacy, but also a violation of confidentiality. [34] If the right to privacy always is dependent on other rights, there is no need to determine boundaries for the right to privacy. In that perspective, it implies that a violation of privacy always constitute a violation of another right.

Thomson is critical to the concept of privacy as a stand-alone right or value in itself, and would therefore argue in favor of a normative concept of privacy. Thomson describes the limit of privacy violations as:

> "*[Y]ou may violate a man's right to privacy by looking at him or listening to him; there is no such thing as violating a man's right to privacy by simply knowing something about him […]".*[35]

However, Thomson's theory can be criticized as it abandons the human sense of dignity; the personhood and intangible loss of personality when privacy is deprived. Lost property could also generate a similar feeling, however the loss is not only giving the individual the concrete missing property and economical loss, but a disappointing sense of having something in your personal sphere taken away without permission or control.[36]

Moral and privacy expert Jeffrey Reiman is criticizing Thomson and argues that even if privacy is relatable to other rights, Reiman suggests that it is helpful to distinguish certain components in the interest of privacy and where from they derive. Any social right or value is rooted in other interests, but that does not imply that all social values should be protected in connection to other rights. Therefore, privacy should be protected as its own individual legal right.[37]

---

[33] Thomson, 1975, pp. 296-297.
[34] *Ibid.*, pp. 295-296.
[35] *Ibid.*, p. 307.
[36] Compare to Reiman, 1976, pp. 26-44.
[37] *Ibid.,* pp. 26-29.

Thomson's statement; "[…] *there is no such thing as violating a man's right to privacy by simply knowing something about him […]"* could be an intrusion of privacy, if the personal information is obtained unauthorized and being used in a further process; as in sharing the information to a third party. If an individual has taken the necessary steps in order to avoid privacy interference and further usage of personal information, Thomson's theory is lacking perspective on the aspect of controlling further dissemination and processing of personal information, both in physical and viral environments.

2.2.5 Control over Personal Information

Privacy defined as control over personal information towards others is considered as the most predominant definition among privacy theorists.[38] The control over personal information entails the individual's power to determine what others can know about him or her. Supreme Court judges Samuel Warren and Louis Brandeis are considered formers of the concept of control over information. Warren and Brandeis introduced the concept of privacy as "*the right to be let alone*"[39]; a definition that received extensive attention in privacy discussions during the nineteenth century, and was recognized as legitimate grounds to protect privacy in four tort actions in U.S. courts.[40]

The concept of a "right to be left alone" is successful in terms of the protective interest of privacy in today's spectrum, where IT is dominating individuals' daily routines and also captures the concerns over third party data processing. Also privacy expert Alan Westin affiliates to the concept of control, that privacy protects our ability to determine for ourselves when, how and to what extent information about us is communicated to others. Westin explain that privacy is;

> "*[T]he claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others*".[41]

Theorists promoting "control over information" emphasize unwanted information disclosure, scrutinized personal life, threats to our ability to maintain control over our bodies and mental state, and threats to our autonomy and decision-making. The moral value in these theories embraces human independence and particularly indicates a negative right or value; the

[38] Solove, 2008, pp. 24-25.
[39] See Warren, Samuel and Brandeis, Louis, *The Right to Privacy,* Harvard Law Review, Vol. 4, No. 5, December 15, 1890 [Warren and Brandeis, 1890]; compare to: Solove, 2008, p. 15.
[40] *Ibid.*
[41] Westin, Allan F., *Privacy and Freedom*, Antheneum for the Assoc. of the Bar of the City of New York, 1967 [Westin, 1967], p. 7.

freedom from being pressured to conform, exploitation and freedom from being socially judged.

The control of personal information towards others captures the subjectivity problem that other theorists have failed to seize when attempting to define privacy. By giving the restricting power to the individual to set limitations for information disclosure, privacy can be seen in the light of different social values and contexts depending on the individual's preferences. The "control over information" concept is too narrow according to Solove since it only focuses on information. However, with support in arguments that privacy should have a normative definition and be dependent on different contexts, control over information concepts aligns with the current society and social behavior, and particularly the IT society regarding control and consent. [42]

2.3 Privacy as a Contextual Right

As can be concluded from the theories presented above, the current status of privacy is scattered and entails several attempts to define privacy. However, they all encompass crucial components and aspects of privacy that have been depicted depending on different contexts and cannot be evaluated separately. Privacy must therefore be comprehended as several different aspects of individuals' social life.

The different approaches presented by privacy theorists clarify the puzzle of defining privacy and according to privacy expert Solove, the theories presented are either too narrow or too broad. Solove argues that; "*merely being more contextual about privacy, however, will not be sufficient to develop a fruitful understanding of privacy*", and that privacy must also serve the underlying core values it protects.[43]

Since data and IT is a growing vital component of individual's lives, it would be relevant to evaluate privacy in the light of IT contexts. However it would also be, aligned with Solove's argument, necessary to deepen our understanding of all affected core values when processing data. For instance the safeguarding of individuals' private information, but also the appropriate quality of data and accuracy balanced to privacy.[44] Continuously, it would be evident to not only include the context, such as IT and processing of personal information, but also what other interests are affected.

The question remains how to stipulate an appropriate level of privacy that can be enjoyed equally by individuals in society. As argued by Warren, Brandeis and Westin, the individual is able to set his or her own limitations by "controlling personal information" towards others.[45] In a democratic

[42] Solove, 2008, pp. 28-29.
[43] *Ibid.*, p. 6.
[44] Nissenbaum, 2009, pp. 127.
[45] See chapter 2.2.5.

society, the citizens would determine to what extent privacy should be protected. If individuals subjectively determine the necessary level of privacy protection in each context, there would be a risk of unequal application of privacy laws.[46] One individual's perspective of the level of privacy protection might differ from another's, and that dilemma cannot justify which perspective of privacy that should prevail.

In order to strengthen privacy as a legal right for all individuals, privacy must be equally protected in similar and objective situations. Certain rights and freedoms are necessary in order to ensure citizens to set their own preferences and values in the first place. Privacy is more than an adjustable prerequisite in a democratic society; it is a vital ingredient and ground stone to form rights, freedoms, duties and moral values in a legitimate democratic system.[47] As Gavison argues; the courts should make "*an explicit commitment to privacy"*.[48] An "ultimate idea" of privacy is not vulnerable to subjective standpoints; it is an overriding value itself that would be determined collectively.[49] If we mislay the idea of importance of privacy, we will start questioning how much protection we truly need in society.

Therefore, in order to establish objective grounds for equal protection of privacy and simultaneously find sufficient protection for underlying values, and strengthening privacy; privacy must be interpreted extensively among regulators, law enforcement mechanisms and even among commercial practices and individuals. Privacy must be seen as an overriding and ultimate value, scrutinizing the interaction between individuals and commercial actors. [50]

Strengthening privacy in context could either require a decrease in required requisites for when a violation of privacy should be considered, or clearer and more requisites included for the term "violation". Gavison mentions that loss of privacy not necessarily implies an intrusion or violation. Though, loss of privacy could be unwanted or unsolicited towards a third party, and the line between a violation and loss of privacy is vague.[51]

Thomson depicts that a person can "waive" the right to privacy by giving consent or show ignorance to someone listening to a private conversation, for instance.[52] The critical issue to address is the grey zone between a consented waived right to privacy and when there is an unsolicited intrusion of privacy. Third parties could easily misuse a "waived" right to privacy. For instance, a waived right to privacy by giving personal information to a medical institution would not necessarily mean that the individual consent

[46] Compare to Nissenbaum, 2009, pp. 65-66, regarding "subjective approaches".
[47] *Ibid.*, pp. 65-66.
[48] Gavison, 1980, 459.
[49] Nissenbaum, 2009, pp. 71-75.
[50] See opposing theories from Thomson, 1975 and Posner, 1981 and their theories of economic interests and privacy as an associated interest to property rights, for instance, making privacy measurable and tangible.
[51] Gavison, 1980, p. 425.
[52] Thomson, 1975, p. 295-296.

to that the medical center give, or accidently transmit, the personal information to insurance companies. Thomson argues that individuals must take necessary steps to avoid other's involvement or interference of his or her privacy.[53] However in IT contexts, the individual does not necessarily have the control to take such measurements to avoid other's interference or actions upon obtaining such personal information.

2.4 Concluding Notes

Various privacy experts have established several approaches to define privacy and what it implies for individuals' social lives. By presenting various different perspectives of the definition of privacy, it can be concluded that the term "privacy" should encompass all theories and be seen in the light of the actual social context. By applying a wide definition of privacy, it is possible to find broader legal basis for protecting privacy. Privacy should be defined in its context, but be protected explicitly as an ultimate underlying fundamental human right.

The predominant understanding of privacy among theorists is the "control over information" concept. By observing today's society, it is evident that IT and data is expanding, and positions privacy in a critical state in the commercial sector. In terms of privacy in the context of IT and commercialization, the "control over information" concept would capture several core values that are threatened in the IT environment. Such values could be; unwanted information disclosure, scrutinized personal life, threats to our ability to maintain control over our bodies and mental state, and threats to our autonomy and decision-making. Further, the freedom from being pressured to conform, exploitation and freedom from being socially judged. Therefore, the "control over information" concept should be concluded as the most appropriate definition in terms of privacy and IT contexts.

With that said, there could be other specific contexts that capture other aspects of privacy presented, that would be better suited under another definition; such as "privacy as an economical interest" in a perspective of individuals interacting with commercial actors as consumers.[54] Again, privacy must be interpreted to its contextual underlying values.

Privacy is not only a matter of direct interaction between an individual and commercial actors, but indirect and passive spread of private information where "waived" consent has been discussed. Issues as control and third party involvement are critical aspects of privacy. For further analysis, data privacy as one context of protecting privacy is analyzed below, and is central for this thesis.

[53] Thomson, 1975, p. 295-296.
[54] See chapter 2.2.3.

3 The Context of Data Privacy

3.1 Introductionary Notes

Concluding notes from the previous chapter present that privacy entails several different perspectives of individuals' social lives, and captures different values depending on the context.[55] Further, it has been concluded that the "control over information" concept captures several underlying values that are inhibited in commercial IT environments, such as controlling spread of information to third parties, disclosure of secret personal details, and fear of social judgment. This chapter will further develop the context of data privacy when processing, monitoring, transmitting and storing of personally attributed data.

The implication of "data privacy" in commercial aspects encompasses two different aspects; the protection of personal data, and adequate practices in the processing of personal data.[56] The aim of this chapter is to examine the term "data privacy" and the implication of "personal data", and present underlying values and norms that have legitimized the interest to protect data privacy. Further, this chapter will illustrate possible threats to data privacy.

3.2 Underlying Interests to Protect in Data Privacy

Data privacy is argued to be a new phenomenon as the term flourished in correlation to the information technology boom starting in the 1950-60s.[57] Continuously, the field of data privacy has, and still is, undergoing excessive development in a regulative perspective and the term data privacy, or "data protection", has been defined relatively recent in the EU and the U.S. regulatory frameworks.[58]

There are various reasons why individuals provide or have their personal information processed by commercial actors. According to data privacy experts, technical innovation is growing and data privacy has become a disputable and crucial element in the development of technical solutions worldwide.[59] The digital society implies, in the aspect of this thesis, indirect

[55] Compare to chapter 2.2 and 2.3 with Solove, 2002, p. 1096, 1125-1125.
[56] Bygrave, Lee Andrew, *Data Privacy law: An International Perspective,* Oxford Scholarship Online, publ. 2014 [Bygrave, 2014], chapter 1, p. 2.
[57] Compare to Nissenbaum, 2009, pp. 20-21.
[58] See chapter 5.3 or 5.4.
[59] See: Klosek, Jacqueline, *Data privacy in the Information Age*, Greenwood Publishing Group, January 2000 [Klosek, 2000], p. 1-2.; and Vacca, John R., *Computer and Information Security Handbook (2*), published by Kaufmann, Morgan, November 2012 [Vacca, 2012], Chapter 42, p. 739.

interpersonal contact between individuals and corporate entities or organizations by technical means.[60] Individuals and corporations utilize technical solutions to control assets, to connect with each other, to access information, and store and manage information. IT solutions have resulted in extreme economical growth globally for businesses. Certain functionalities have specifically gained our daily lives; connectivity, accessibility, efficiency and storage.[61]

The understanding of data privacy merely focuses on protective interests of data subjects, as in individuals, and the flow of their personal data.[62] When data flows entail personal data, it becomes crucial to determine how personal data should be handled.

3.2.1 Personally Attributed Data

Data privacy is argued to function as an extended right to privacy in the digital environment but also encompass additional interests than the "traditional" discussion of privacy.[63] These additional interests are for instance the assurance of sufficient data quality processing.[64] Data quality and protection of personal data distinguishes "data privacy" from "privacy" with its dual underlying interests; specifically adapted in EU laws.[65]

The definition of data privacy is focusing on personal data. However, the term "personal data" is ambiguous and relates to the discussion of what constitutes "personal" or "private".[66] The term "data" is defined as:

> *"Information, especially facts or numbers, collected to be examined and considered and used to help decision-making, or information in an electronic form that can be stored and used by a computer*".[67]

The above explanation of data emphasizes information, and personal data should therefore be understood as "personal information".[68] The understanding of personal information relates to the "control over personal information" introduced by Brandeis and Warren.[69] Underlying values of

[60] Klosek, Jacqueline, *Data privacy in the Information Age*, Greenwood Publishing Group, January 2000 [Klosek, 2000], p. 1-2.; and Vacca, John R., *Computer and Information Security Handbook (2*), published by Kaufmann, Morgan, November 2012 [Vacca, 2012], Chapter 42, p. 740.
[61] Klosek, 2000, p. 2.
[62] Bygrave, 2014, chapter 1, p. 2.
[63] See chapter 2.
[64] Vacca, 2012, Chapter 42, p. 740.
[65] Thus, data privacy could also be argued to include less contexts of privacy, according to privacy law expert Lee Andrew Bygrave; see Bygrave, 2014, chapter 1, p. 3.
[66] Kuner, Christopher, *Transborder Data Flows and Data Privacy Law*, Oxford University Press, September 2013, p. 1.
[67] Cambridge Dictionary, February 20 2017.
[68] Vacca, 2012, Chapter 42, p. 740.
[69] See chapter 2.1.5 (Warren and Brandeis, 1890); compare to Westin, 1967, p. 7.

"control over personal information" and "the right to be left alone" encompass the will to be independent, autonomous, free of mind and body, freedom from unwanted or unsolicited disclosure, and social judgment. This perception of privacy aligns with modern theories of data privacy as "*anonymity, unobservability, and unlinkability"*.[70] "Anonymity" implies the wish to be unidentified by the personal data, "unobservability" the idea of being difficult to be distinguished from other data subjects or personal data, and "unlinkability" to not have certain kind of information linked together that facilitates identification of greater collections of data.[71] The term data privacy is therefore encompassing values indicating a wish of not being identified, and personal information facilitates the possibility to identify personal characters in data. Information making it possible to identify individuals digitally could be the identity of the data sender or receiver, the intermediary facilitating the data processing service, information about where the involved individuals are localized, or what the information in question reveals.[72]

3.2.2 Individuals' Incentives to Disclose Personal Data

As argued above, personal information is the critical factor that must be handled and protected. Thus, what are the incentives for individuals that result in personal information ending up in data? One of the reasons is to stay connected. Connectivity implies two aspects; the interest of individuals staying connected in social terms on platforms such as Facebook. The idea of privacy as the right to integrity, intimacy and personhood would substantiate the interest of being socially connected to other people in the digital sphere. Social media and other networking functions enable individuals to invest in friendships and relations independent on location and time.[73]

The other aspect of connectivity relates to material connection to different sources of information by using different devices to control technical functions, such as "Internet-of-things", and through location based services via Bluetooth, Wi-Fi, GPS and similar sensor functions. This perspective captures another underlying theory of privacy, as the concept of "privacy as an economical interest" in terms of controlling devices for financial records or controlling property, for instance.[74]

The coexistence of data privacy and connectivity will, however, counter difficulty due to the IT environment of interconnectedness and complexity; individuals wish to stay connected, but want to have their privacy protected

[70] Vacca, 2012, Chapter 42, p. 740.
[71] *Ibid.*
[72] *Ibid.*
[73] Fried, 1968, p. 482.
[74] Compare to Richard Posner, chapter 2.2.3.

simultaneously.[75] The balancing of countervailing interests is therefore problematic, and there are various threats to data privacy.

3.2.3 Threats to Data Privacy in Commercial Contexts

Personal information, or "personal data"/ "PII", ends up in information technology services for several reasons; individuals may provide the information themselves by entering their email addresses to access Wi-Fi, or the service providers obtain the information without the individuals knowing, either directly or by an intermediary such as data controllers. In the first scenario, individuals consent to their personal data being shared by providing the information themselves. This could be associated to what Thomson depicts as "waiving" privacy.[76] Problematically, personal information can be waived by consent to a certain purpose, but be further and undesirably transmitted to third parties and used for undesired purposes.

Thomson's idea of waiving one's right to privacy can be criticized. Individuals do not necessarily know what to "waive" and how to control waived privacy. Spreading of personal information in data is tremendously different from utilizing methods in "the real world". The connectivity between different information sources and communication systems is insurmountable and impossible to control from an individual's aspect. By applying the "information-control-concept" of privacy, it is problematic that individuals feel insecure when sharing personal information to certain environments and cannot control the information towards third parties.

Insufficient knowledge and power over technical infrastructure and personal data result in an immense intranet of personal information. However, this is not necessarily a violation of privacy pursuant to privacy laws, but problematic for individuals if no consent has been actively given.[77] In addition, it actualizes what other actors that should be held accountable and responsible for such lack of knowledge and lack of power among individuals. This results in an unbalanced vendor-customer relationship that negatively impact individuals in terms of trust, and commercial actors in terms of economical development. According to Posner, people would develop certain behavior to protect economic interests. Incentives to have sustainable data protection regulations could therefore be seen in an economic interest, to shield and control our private information provided to corporations in exchange for access and connectivity.[78] The more information provided and obtained, the more opportunities corporations have to develop suitable solutions designed after the consumers' demands, and individuals having control and knowledge. The balancing of data

[75] Vacca, 2012, Chapter 42, p. 739.
[76] Thomson, 1975, p. 295-296 (see chapter 2.1.4).
[77] See legal differences between the EU and the U.S. in chapter 5.
[78] Compare to Chapter 2.1.3 "*Privacy as an Economic Interest";* and Posner, *The Economics of Privacy*, p. 405.

privacy against transparency would not necessarily imply lack of power and the end of lucrative outputs; it could rather function as a gearwheel when creating new innovation. By influencing innovation with safe practices for consumers, individuals could develop more trust for commercial interests and innovators; a more sustainable relationship.[79]

Personal data could imply valuable information for frauds. In terms of financial services and other asset-management services, unsolicited obtained personal data could result in identity theft and unlawful transactions. For instance, the obtaining of passwords, credit- or debit card information, security installation passwords and bank account numbers.[80] Corporate entities, governmental institutions, schools and other organizations are subject to these risks to a higher extent than individuals.[81] A majority of data breaches have been considered as accidents rather than intentional breaches.[82] With that said, it is crucial that systems need appropriate data privacy management to avoid these kinds of threats.

3.3 Concluding Notes

The term "data privacy" entails the accurate protection of personal information transmitted by electronic means, in correlation to how data is being processed and used. Data privacy is associated with what Warren and Brandeis argued in 1890 as the "*right to be left alone"*.[83] Data privacy in commercial aspects relates to the interest of individuals to not be identified without consent or control.

Individuals provide, directly or indirectly, information that data providers, processors and controllers use for commercial purposes, such as marketing. Individuals may provide their personal information in private and social environments, or in terms of handling personal belongings and functions that requires connectivity to devices connected via sensors or network systems. Problematically, individuals provide consent and manage to control a certain amount of disclosure of personal information, but not fully in terms of transmitting of information to third parties. Individuals are therefore struggling in protecting or managing personal information provided to one commercial actor obtained by another, implying threats related to frauds, imbalance of power in daily consumer-to-vendor contracts, and unsolicited monitoring and storing of personal data with a risk to be socially judged. By creating more trust and transparency between commercial actors that collect personal data, and the individuals' right to data privacy, their relationship could be improved. Sustainability as a solution to this imbalance is presented below.

[79] Compare to: Vacca, 2012, Chapter 42, p. 739.
[80] *Ibid.,* p. 741.
[81] *Ibid.*, p. 742 Thus, such breaches are classified as data security, not completely similar to data privacy; see Bygrave, 2014, Chapter 1, p. 2.
[82] Vacca, 2012, Chapter 42, p. 742
[83] See chapter 2.1.5 (Warren and Brandeis, 1890).

4 Sustainability and Data Privacy Protection

4.1 Introductionary Notes

A modern IT-developed society is aware of that personal information has been somehow transmitted, monitored, processed and stored since the IT boom. Regulators, policy-makers, judicial mechanisms and also private organizations shall therefore consider well-established protection of personal interests embedded in technical data flows. Thus, as has been depicted in the previous chapter, it is difficult to balance the protection of personal data and other important interests affected such as economic benefits for innovators, rights and freedoms of other democratic interests, and efficiency.[84] In order to find an appropriate balance, this chapter analyzes the term sustainability.

Why should the term sustainability be the solution for balancing individuals' privacy towards commercial data processors ability to conduct successful businesses? As concluded in earlier chapters, personal data/ PII is the critical aspect to protect. Thus, data privacy must be balanced to the reasons why individuals chose to use data solutions; accessibility, connectivity and efficiency, for instance. Additionally, data quality as in the accuracy of data is important when discussing protection of data privacy. These countervailing interests must be evaluated from the commercial data provider's perspective. Data processors, providers and controllers are facilitators who have the ability to control accessibility, efficiency and connectivity as well as the data quality for its costumers. Their interests must therefore similarly be taken into account and balanced. This chapter proposes that theories of social sustainability could influence how to develop more balanced data processing practices.

4.2 Why Sustainability is Evident for Data Processing Practices

The United Nations General Assembly, with reference to the World Commission on Environment and Development, defines "sustainable development" as;

> *"[…] development that meets the needs of the present without compromising the ability of future generations to meet their own needs […]".*

[84] See chapter 3.1.2.

Further on, the UN conclude that there are three pillars of sustainability; economic development, social development, and environmental protection.[85] This thesis focuses on the social aspect. According to research undertaken in collaboration with the ECRI Ethics in Finance and Social Value Research Group, businesses in sustainable pathways should consider:

> "[…] *The basic function of any organization, i.e. that which legitimizes it socially, is to create social value for society as a whole […]".*[86]

Sustainability implies solutions extending beyond financial impacts and goals. Costs and values are associated with the impact on the society and environment and not only in financial terms.[87]

As argued by the UN, sustainability is often regarded as a three dimensions concept. Interests involved in "social protection" are ethics and human capital development, factors contributing to social impact, quality of life, fulfillment of human basic needs and human rights. The aim is to promote an ecosystem-thinking concept in the business cycle; both vertical and horizontal involving stakeholders such as supply chains and consumers. Important factors in the development of this ecosystem thinking are clear guidelines of transparency, accountability and strategic implementation structures.[88] Awareness of commercial sustainability creates trust among consumers and as the ECRI research group presented, businesses who can demonstrate long-term thinking strategies can be able to create social value for society as a whole.[89]

Data privacy has been concluded as a value and right closely related to individual fulfillment, dignity and several other components of how to define the human nature.[90] Thus, data privacy has also been associated to values including "appropriate data quality" that indicates an interest in technical innovation for economical gain.[91]

The interests of data privacy and the interest of achieving lucrative business results have been considered to be countervailing. However, the spectrum of the two interests is changing magnificently and new innovation as well as institutions indicates trends to combine the two interests to sustainable

---

[85] United Nations website, General Assembly of the United Nations, *Sustainable Development: Background*, available at: http://www.un.org/en/ga/president/65/issues/sustdev.shtml (accessed by February 22 2017, 11:41 EST).
[86] Retolaza, José Luis., San-José, Leire. and Ruíz-Roqueñi, Maite., *Social Accounting for Sustainability Monetizing the Social Value*, 1st ed. 2016., 2016 [hereinafter: Retolaza, San-José and Ruíz-Roqueñi, 2016], p. 5.
[87] Cabezas, Heriberto, and Diwekar, Urmila, *Sustainability; Multi-Disciplinary Perspectives*, Bentham Science Publishers, September 14, 2012 [Cabezas, Diwekar 2012], pp. 311-312; CSR will be further mentioned in chapter 7.
[88] Cabezas, Diwekar 2012, p. 313.
[89] Retolaza, San-José and Ruíz-Roqueñi, 2016, p. 5.
[90] See Chapter 2 and 3.
[91] See Chapter 3.1.1.

solutions.[92] This balancing of interests has especially been elaborated in the privacy frameworks of the EU and sector-based guidelines in the U.S.[93] Modern societies have reached a crossroads where sustainable development in data privacy and data protection is unavoidable. The worldwide economical spectrum is increasingly relying on IT and Internet solutions, and data protection is a crucial component for a functioning system with sustainable outcomes.[94] According to a report on development on data protection regulation by the UN, data privacy and protection of personal data is a significant increasing field that challenges policymakers worldwide.[95]

The definition of sustainable development has similar components to the discussions regarding privacy and how to protect its underlying values.[96] The ultimate concept of privacy, described by Gavison, or "coherentism", described by Judith DeCew, captures the idea of privacy as an overriding interest or moral value, an idealistic understanding of how to protect privacy long-term.[97] An ultimate concept, as well as coherentism, applies to the context of data privacy. With that said, it becomes clear that Gavison and DeCew have approached the field with a sustainable way of ecosystem thinking. According to DeCew, Solove and Priscilla Regan, privacy is becoming a "collective value" and do not only imply an individual right, but also a public and equal right that is becoming a minimum standard in technical and commercial environments.[98]

Consumer awareness in data privacy is an increasing factor and according to privacy expert Jacqueline Klosek, corporations should start, if not already started, to base corporate decisions on how to best protect and influence business models and technical solutions upon data privacy values. Importantly noted, however, is that services based on obtaining large amounts of personal information are beneficial not only for the companies or organizations, but for the individuals using these services. It is therefore crucial for individuals to be aware and gain knowledge about what personal data implies, when it is obtained, and how they can control it.[99] Consumer awareness is therefore an evident component of a sustainable concept of data privacy.

Data privacy as a sustainable interest needs to be balanced to other interests. Sustainability in the protection of data privacy further requires balance

[92] Vacca, 2012, Chapter 42, p. 742.
[93] This will be further explained in chapter 5.3 and 5.4.
[94] United Nations Conference on Trade and Development (UNCTAD), *Data Protection Regulations and International Data Flows: Implications for Trade and Development*, New York and Geneva, 2016 [UN Report on Data Protection, 2016], p. 11.
[95] UN Report on Data Protection, 2016, p. 2.
[96] See Chapter 2.
[97] Gavison, 1980, 459; and DeCew, 2002, (revision 2013), chapter 1.3.
[98] Compare to DeCew, 2002, (revision 2013), chapter 3.6; and Solove, 2008, p. 98 and 171; and Regan, Priscilla M., *Legislating Privacy*, publ. 1995, Chapel Hill, NC, University of North Carolina Press, p. 213.
[99] Klosek, 2000, p. 12.

between privacy and other countering interests; such as freedom of speech, the right to conduct you own business, the right to property, and other fundamental rights. Further, public interests such as national security must be acknowledged in terms of counter-crime purposes. As will be mentioned in chapter five, there are legal mechanisms balancing countervailing interests that must be taken into account for developing sustainable data privacy practices.

4.3 Concluding Notes

In order to find appropriate methods to balance individuals' right to data privacy towards commercial data actors' economical incitements, theories focusing on social sustainability is a solution. Privacy theorists emphasize the necessity for long-term protection of privacy as a collective interest in society. Several social theorists are arguing for sustainable data practices as unavoidable.

Sustainable solutions are referred to as developments benefiting the current needs and simultaneously ensure the needs of the future. Continuously, the interest to protect data privacy, economical incentives for commercial actors, and other fundamental human rights in society must all be taken into account in order to be sufficiently protected today as well as tomorrow.

Values such as transparency, coherence to consumers and other stakeholders, accountability, responsibility and long-term strategies contribute to more sustainable ecosystem thinking structures in organizations. According to the ECRI organization as well as the UN, awareness of these factors develops more trust among consumers, but also creates solutions that benefit society as a whole. By respecting each interest when processing data for commercial purposes, this chapter set forth that businesses could conduct better businesses not only receiving economical gain, but also better relationships to their customers and stakeholders.

5 Legal Protection in the Commercial Context

5.1 Introductionary Notes

Chapter two to four in this thesis have depicted a value-based theoretical discussion of the underlying values of privacy and data privacy. It has been concluded that the definition of privacy must be formulated as the understanding of privacy in its particular context. Data privacy is one specific context of privacy, entailing values that have strong connections to digital functions in IT and theories emphasizing "control-of-information-concepts".[100] Further on, data privacy mainly focuses on the will to protect personal data connected to data subjects and that data privacy must be balanced to interests benefiting commercial actors.[101] The balancing of data privacy against commercial interests has been concluded difficult and in chapter four, sustainability was introduced as an appropriate approach for ensuring a beneficial outcome for both individuals and commercial actors.

This chapter analyzes the legal aspect on the right to protection of personal data, and the aim is to evaluate whether the legal protection sufficiently safeguard the underlying values of data privacy. This chapter begins in a broad perspective by presenting the starting points of the attempts to regulate data privacy. Global organizations as the UN and OECD have guided the world to protect personal data, which will be presented first. Thereafter, the analysis focuses on legal aspects in the EU and the U.S. on interstate level and federal level. The laws will be presented in both written legislation as well as relevant case law. The relationship between the EU and U.S. is in focus to present legal differences of data privacy protection, and what underlying legal approach each economy has. Further, this chapter presents where the law is lacking protection in data privacy, both in the EU and the U.S., and how that impacts sustainable data protection practices and compliance.

5.2 Guidelines in International Frameworks

5.2.1 Lacking Applicability and the United Nations

The UN is recognized as the leading transnational organization for promoting and protecting fundamental human rights globally. Each member State of the UN is required to adopt legislation protecting individuals from

[100] Compare to Chapters 2.1.1 and 2.1.5.
[101] See Chapter 3.1.

interference and assurance of protecting such right efficiently.[102] According to the Universal Declaration on Human Rights of 1948,[103] article 12:

> *"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."*[104]

The Declaration of Civil and Political Rights as well as the UN Human Rights Charter have influenced the regulative approach to protect the right to privacy to a large extent in the EU as well as the U.S. Thus, none of the provisions defines "privacy" explicitly. The perception of privacy in these declarations is similarly formulated as the concept of "the right to be left alone", argued by Warren and Brandeis in the 1890s.[105] The Human Rights Committee Report of 1988 attempted to explain "family and home" as part of the right to privacy, and concluded that an extensive interpretation was necessary.[106] The broad interpretation aligns with the discussion Gavison set forth regarding an "ultimate concept of privacy" and the urge to protect its underlying values excessively.[107]

The UN has taken several steps towards responding to the information technology and digital development worldwide, and has adopted numerous resolutions in order to protect data privacy. In December 2013, *Resolution 68/167 on The Right to Privacy in the Digital Age* was adopted in order to strengthen the global level of protection of privacy.[108] Thus, the resolution is particularly emphasizing the responsibility of member States to ensure that no illegitimate surveillance is undertaken of individuals.[109]

Since the UN is posing requirements on national level, it implies that the definition of the right to privacy is determined by national legislative and judicial means, and the UN guidelines will merely serve as guidance.

---

[102] According to the UN Human Rights Committee. See; Office of the High Commissioner for Human Rights, CCPR General Comment No. 16: Article 17 (Right to Privacy), *The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, Adopted at the Thirty-second Session of the Human Rights Committee, on 8 April 1988 [Human Rights Committee Report, 1988], p. 1.

[103] [Hereinafter: UN Declaration on Human Rights].

[104] The right to privacy is also enshrined in article 14 and 17 in the International Covenant on Civil and Political Rights of 1966 [Hereinafter: Declaration of Civil and Political Rights].

[105] Compare to Warren and Brandeis, 1890.

[106] Human Rights Committee Report, 1988, p. 2.

[107] Compare to Gavison, 1980, 459; see also DeCew, 2002, (revision 2013), chapter 1.3.

[108] United Nations General Assembly, , *68/167 – The Right to Privacy in the Digital Age*, resolution adopted by the General Assembly on 18 December 2013 (on the report of the Third Committee, A/68/456/Add.2) [hereinafter: Resolution 68/167].

[109] Resolution 68/167; the resolution specifically state that democratic rights in the UN Declaration on Human Rights, the Declaration of Civil and Political Rights, and the International Covenant on Economic, Social and Cultural Rights must be fully enjoyed.

Therefore, practical regulations of commercial interactions between individuals and commercial actors remain undetermined.[110] A critical aspect is how efficient the States in fact can protect and enforce such protection on an individual basis.

5.2.2 Starting Points and Principles by the OECD

Since 1970, the international organization for economic co-operation and development[111] has influenced countries to develop more awareness of data privacy for better global business practices. Between 1980 and 1990, the world experienced an advanced digital boom that has expanded ever since. Continuously, OECD saw the necessity to respond to the fast digital development and published core principles to serve as best practices in handling data privacy issues on a domestic and transnational level.[112]

The guidelines entailed, and are still widely recognized in a worldwide regulative perspective, eight core principles for formulating data practice regulations applied in both public and private procedures; (1) a collection limited principle where any personal data must be obtained by fair and lawful means, (2) a data quality principle where the obtained data must be relevant and up to date, (3) a purpose specification principle where the data must be explained why it is obtained in connection to the processing, (4) a use limitation principle where data should not be disclosed without consent or if there is a lawful reason for disclosure, (5) a security safeguard principle implying that the data should be protected from unwanted modification or access, (6) an openness principle explaining what personal data implies, and how it is handled, (7) an individual participation principle for data subjects to obtain, request or otherwise access his or her own data by the data controller, and (8) an accountability principle for data controllers to be liable for that the principles above are being complied with.[113]

OECD undertook extensive research and concluded that different countries had different legal approaches to protect privacy and the adaption to the digital development. In 1980, 30% of the member countries had adopted the data practice principles. The application of the guidelines appeared differently depending on legislative approach; some countries had a general

[110] Compare to: A/HRC/27/37*, United Nations General Assembly, Human Rights Council: Twenty-seventh Session, Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General, *The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights*, GE. 14-08854 (E), *1408854*, 30 June 2014 [Hereinafter: Annual Report of the UN High Commissioner and the Secretary-General, 2014], pp. 3-4.

[111] [Hereinafter: OECD].

[112] OECD Council Recommendation, OECD Guidelines on the Protection of Privacy and Transboarder Flows of Personal Data, 1980 (amended 2013) [hereinafter: OECD Guidelines on Data Protection, 1980].

[113] OECD Guidelines on Data Protection, 1980, part two, *Basic Principles of National Application*.

approach, implementing data privacy provisions in general privacy provisions. Other countries adopted new data privacy laws.[114]

There were common concerns detected among the countries; the balance between individuals against "data controllers", as in organizations or companies providing data services, and the balancing of privacy against other interests such as freedom of speech and the prospering of innovation and economical growth.[115] However, OECD concluded that the protection of privacy had expanded, and that they could;

> "*[…] identify a more complex synthesis of interests which can perhaps more correctly be termed privacy and individual liberties […]".*[116]

The report from 1980 was updated in 2013 with numerous amendments such as a practical implementation guidance rooted in a risk management approach, improved interoperability in terms of the global perspective, new national privacy strategies, privacy management programs, and data security breach notifications.[117] OECD has influenced the EU and the U.S. in terms of developing data privacy regulations extensively and has clarified practical implementation processes, perhaps with better coherence than the UN framework. The data privacy development in the EU is presented below.

5.3 EU Privacy Laws in the Commercial Context

5.3.1 The Fundamental Human Right to Privacy

As a global economic market player, the EU has been leading in the development of the protection of data privacy. Today, personal data can solely be gathered under strict conditions under EU law. Simultaneously, the EU has facilitated the possibility for the context of data privacy to grow as an interest embedded in innovation worldwide, conceptualized as "data protection".[118] Thus, the EU framework has left doors open for varying interpretations of data privacy and differences in level of protection depending on each Member State.

In 1950, Europe enacted the European Convention on Human Rights.[119] Article eight recognizes the right to privacy for all citizens in Europe, stating that "[*e]veryone has the right to respect for his private life, his home,*

[114] OECD Guidelines, 1980, (web format) General Background.
[115] *Ibid.*
[116] *Ibid.*
[117] The OECD Privacy Framework of 2013, part 5-6 and chapter 2.
[118] Compare to the discussion of "the Context of Data Privacy" in Chapter 3.
[119] [Hereinafter: ECHR].

and his correspondence […]". The right to privacy could, however, be subject to restriction due to numerous exemptions.[120]

Even though Europe safeguard fundamental rights in ECHR, the EU adopted the Charter of Fundamental Rights of the European Union specifically for the Union and their interests in 2000.[121] The EU Charter became binding for all Member States in 2009 in connection to the enforcement of the Lisbon Treaty. The EU Charter explicitly recognizes interests focusing on dignity, solidarity, and citizens' rights in order to invoke more transparency in the administration benefiting the citizens of the EU.[122] The respect for private and family life is set forward in article seven.

The EU Charter explicitly recognizes the right to protection of personal data in article eight, stipulating that personal data must be fairly obtained and processed and by legitimate means. Further, a principle of consent, a right to access the personal data by the data subject, and the right to have personal data rectified. Article eight clarifies that compliance with this article shall be subject to control by an independent authority. Notably, the EU Charter applies to governmental institutions and organizations.[123]

There has been extensive room for interpretation of data protection in each Member State. The EU Charter clarifies that each State has a responsibility, but the EU do not put forward any practical applicable guidelines since each Member State is sovereign.[124] The abovementioned international Charters are therefore indicating lack of practical implementation guidelines for data privacy protection between commercial actors and individuals, similarly to the concept in the UN.[125] The critical and remaining question is therefore whether these Charters are sufficient for sustainable data privacy protection practices and compliance structures on corporate and individual level.

5.3.2 Secondary Data Protection Laws 1995 - 2016

The Directive on Data Protection (95/46/EC) was enacted in 1995 and was a response to the rapid digitalization. Further, a reaction to the extensive research undertaken by the OECD and the diverse application of data privacy laws in the EU Member States.[126] The directive is now repealed

[120] Such exemptions are enumerated in article eight point two, mentioning national safety and public interests, and in the event of collision of other rights and freedoms in the ECHR.
[121] [Hereinafter: EU Charter].
[122] European Commission, official website, Justice: Building a[sic!] European Area of Justice, EU Charter of Fundamental Rights, article one to seven.
[123] Compare to: E.U. Network of Independent Experts in Fundamental Rights (CFR-CDF), *Report on the Situation of Fundamental Human Rights in the European Union and its Member States in 2002*, pp. 77-78.
[124] Other independent organizations such as OECD has given more practical guidelines for private as well as public organizations, see Chapter 5.1.2.
[125] See chapter 5.2.1.
[126] [Hereinafter: the Directive on Data Protection].

with a data protection regulation that will be presented in the next chapter.[127]

The directive serves fundamental importance as one of the first evident decision-making progresses in the harmonization for data protection in the EU Member States. The aim for the directive was the ability to pursue common goals and concerns among the Member States, and to jointly preserve underlying interests to data privacy. The Directive on Data Protection introduced a dualistic approach for addressing the concerns by protecting personal data, but also the importance of developing the quality of the data processing in the Single Market. The harmonization was considered evident since unequal protection could constitute an obstacle for economic activities on the Single Market.[128]

The eight core principles that were introduced by OECD in 1980 are reflected throughout the Directive on Data Protection.[129] The provisions in the directive are technically neutral and addresses any "data controller" that process personal data by automatic means.[130] "Personal data" is defined in article two as information that facilitates the identification of a natural person, or "data subject", directly or indirectly, by:

> *"[…] [R]eference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*".[131]

To determine whether an individual is identifiable, the European Commission states that:

> "[…] [*A]ccount should be taken of 'all the means likely reasonable to be used either by the controller or by any other person to identify the said person".*[132]

In the case of Lindquist, the European Court of Justice[133] ruled a preliminary judgment by request from the Swedish Göta Court of Appeal[134]

---

[127] See chapter 5.2.2.
[128] See Directive on Data Protection (95/46/EC), recital seven and eight, and article one; and the European Commission, Staff Working Paper, Impact Assessment – Accompanying the Document, General Data Protection Regulation and the Directive on processing of personal data by competent authorities in criminal investigations, January 15, 2012 [hereinafter: European Commission, Staff Working Paper, 2012], pp. 9-11.
[129] Compare to chapter 5.1.2.
[130] Directive on Data Protection, article 2 (d-g) and 3.
[131] Directive on Data Protection, article 2(a).
[132] European Commission, *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, November 4, 2010, Brussels [European Commission, Communication, 2010], p. 5; compare to Recital 26 in the Directive on Data Protection.
[133] [Hereinafter: EUCJ].

that the mentioning of a person's name or a person's personal telephone number, information about working conditions or hobbies constitutes "personal data". Further, the uploading of such personal data on an online website constitutes "processing" by "automatic means". That Mrs. Lindquist's purpose was charitable and religious did not actualize any exemptions in article three point two of the Directive on Data Protection.[135]

The Directive on Data Protection was profoundly challenged only fifteen years later due to three main factors; (1) the technological development and the globalization of data, (2) the lack of harmonization between Member States, and (3) inefficient enforcement of the rules.[136]

In terms of (1) new technical solutions, the European Commission mentioned services as cloud computing and the implication of "big data". Further, the necessity to secure control and transparency for individuals regarding their personal data.[137] Research undertaken between 2010 and 2015 by the European Commission presented that 90 % of the citizens in the EU were anxious over the protection of personal data and preferred the level of protection to be improved equally in the EU among all Member States, regardless where their data is processed.[138] EU case law introduced a new concept of protecting personal data by creating a "right to be forgotten", where search engines such as Google became obliged to delete information that was no longer necessary for the service purposes.[139]

---

[134] Göta hovrätt.

[135] C- 101/01, the case of Lindquist, November 11, 2003, Judgment of the Court; The EUCJ also emphasized the importance of balancing data protection to other rights, such as freedom of expression, and that there is an appropriate restrain of other rights. For financial services and handling of personal data, see C-73/07, the case of Tietosuojavaltuutettu (Finnish Data Protection Ombudsman) v. Satakunnan Markkinaporssi Oy and Satamedia Oy, December 16, 2008, Judgment of the Court (Grand Chamber).

[136] European Commission, Communication, 2010, pp. 2-4 and 5; and European Commission, Staff Working Paper, 2012; and European Parliament Resolution of 25 November 2009 on the Communication from the Commission to the European Parliament and the Council – An Area of freedom, security and justice serving the citizen – Stockholm Programme, Multi-annual programme 2010- 2014 regarding the area of freedom, security and justice (Stockholm Programme), (P7_TA(2009)0090) [Stockholm Program], pp. 14-15.

[137] European Commission, Communication, 2010, p. 5.

[138] European Commission, Press Release, *Agreement on Commission's EU Data Protection Reform will Boost Digital Single Market*, Brussels, 15 December, 2015; European Commission, Press Release, *Commission proposes a comprehensive reform on data protection rules to increase users' control of their data and to cut costs of businesses*, 25 January, Brussels [hereinafter: European Commission, Press Release, January 2015]; compare to: European Commission Report, Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union, Conducted by TNS Opinion & Social at the request of Directorate-General Justice, Information Society & Media and Joint Research Centre, Survey Coordinated by Directorate-General Communication, Brussels, Fieldwork: November December 2010, Publication: June 2011 [hereinafter: Special Eurobarometer, 2011].

[139] See C-131/12, the case of Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzalez, Judgement of the Court (Grand Chamber), 13 May, 2014.

Harmonization and the equal data protection was another challenge (2). The European Commission stressed the difficulty of upholding equal protection of data privacy protection in the Member States and the lack of harmonization. In the case of Commission v. Luxembourg in 2001, the EUCJ ruled that internal disorder in a Member State's government do not justify failure to comply with the Directive on Data Protection. Thus, EUCJ merely influenced the awareness of the need for better uniform regulations. Therefore, the challenge to justify national regulations in accordance with the EU data protection laws remained.[140]

A third challenge (3) was the difficulty of ensuring equal protection in national law enforcement mechanisms and independent oversight in each Member State. In the case of Commission v. Germany, the EUCJ concluded that the German Data Protection Authority[141] was not sufficiently independent according to article 28(1) in the Directive on Data Protection considering that other governmental authorities could influence the decisions made by the DPA.[142]

The challenges emphasized by case law and extensive research and stakeholder consultations resulted in a new reform of the data protection regime in the EU.[143] It took almost six years until the proposition became new data protection law in the EU as the General Regulation on Data Protection (2016/679).[144]

5.3.3 The General Regulation on Data Protection

The Directive on Data Protection resulted in a well-illustrated example of the difficulty of combining protection of personal data, and the fast development of technical solutions. Therefore, a new and stricter data protection regulation entered into force May 24, 2016 and must be fully adopted by 2018 by all Member States in the EU; GDPR. The transition from a directive to a regulation would, according to the European Commission, save efficiency in data flows and approximately saving businesses €2.3 billion a year.[145]

There are numerous differences and modifications between the new regulation and the Directive on Data Protection. Firstly, there is a difference

[140] C- 450/00, the case of Commission v. Luxembourg, October 4, 2001, Judgement of the Court (First Chamber).
[141] [Hereinafter: DPA].
[142] C-518/07, the case of the European Commission v. The Federal Republic of Germany, Judgement of the Court (Grand Chamber), March 9, 2010; compare to C-614/10, the case of the European Commission v. The Republic of Austria, October 16 2012.
[143] See European Commission, Communication, 2010, p. 5; and European Commission, Staff Working Paper, 2012; and European Parliament Resolution of 25 November 2009 on the Communication from the Commission to the European Parliament and the Council – An Area of freedom, security and justice serving the citizen – Stockholm Programme, Multi-annual programme 2010- 2014 regarding the area of freedom, security and justice (Stockholm Programme), (P7_TA(2009)0090) [Stockholm Program], pp. 14-15.
[144] [Hereinafter: GDPR].
[145] European Commission, Press Release, January 2015.

between a "regulation" and a "directive" in EU law. The Directive implied more flexibility; each Member State was required to implement data protection laws compatible to the general aims of the directive, implying that national laws could be adjusted to align with the aims. Therefore, the Directive implied lacking uniform level of protection in the EU data protection. A regulation, however, implies immediate enforceability of the regulation in the Member States, and the regulation becomes national law. Further, there are specific national DPAs that are considered competent to inspect and enforce compliance issues appointed by the European Commission.[146]

A second difference is that the Directive on Data Protection did not pose direct obligations on all data processors, solely on "data controllers" according to article six point two. However, the new GDPR implies direct obligations for "data processors", and implies an increased accountability for any data service that process data entailing personal data of natural persons in the EU, such as third party data processors.[147] The GDPR is clearly indicating stronger data protection regulations for natural persons, and include further elaboration of the eight core data protection principles initiated by OECD.[148]

A third difference is that the European Commission has elaborated the definition of "personal data" in the GDPR article four point one. The GDPR include additional explanations such as; "*reference to an identifier such as a name […] location data, […] an online identifier"* and information that relates to a natural person's *"genetic identity"*.[149] Another modification is the control of individuals of their personal data, and foremost "the right to be forgotten" in article 17 in the GDPR initiated by the Google case.[150]

Any erasure of personal data requires at least one applying ground for when a data processor must erase any personal data. One of these grounds is if "*the personal data are no longer necessary in relation to the purposes […]"*, in article 17(a). Further, any measure to erase personal data, or in any other way comply with required actions for the benefit of consumers, is also subject to a cost implementation evaluation for the data processor. In article 20, data subjects have the right to "data portability", implying that individuals have the right to receive the data that has been processed about them. Similarly, this right is dependent on the expected capacity of the data processor to comply.

---

[146] European Commission, Justice, *Protection of Personal Data in the European Union*, Fact Sheet, Directorate-General for Justice, BE- 1049, November 2010, Brussels, p. 2.
[147] Phil Lee and Mark Weber, *The New EU General Data Protection Regulation Under 60 minutes!*, FieldFisher, January 31, 2016.
[148] Recital 14, GDPR. Compare to chapter 5.1.2.
[149] Article four point one, GDPR.
[150] See C-131/12, the case of Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzalez, Judgement of the Court (Grand Chamber), 13 May, 2014.

Even though the modifications above have introduced more control of personal data for individuals theoretically, they are still subject to vague exemptions and prerequisites before such measurements can be enforced. The GDPR has no clear explanatory notes of how long "necessary" implies for claiming the "right to be forgotten", for instance. The provisions are ambiguous for both individuals as well as companies due to the difficult challenge in balancing interests of individuals versus large companies lobbying for the reverse.[151]

The GDPR introduces "*pseudonymisation"* which implies processing practices where personal data has been detached from the data. In order to process data in this manner, personal data must be restructured in order to detach personal information, implying that the data no longer can identify individuals.[152] Pseudonymisation is a large step towards efficiency and safety when protecting personal data, promoting the idea of "data protection by design and default" as presented in article 25 in the GDPR. The provision requires that the data processor must be evaluated upon its capacity and actual ability to implement pseudonymisation measurements.

The GDPR will counter issues in terms of interconnectedness and complexity. Data is processed in several different systems simultaneously and the inability to control personal data and data quality is a difficult task. Innovation is developing faster than the EU laws, challenging its power towards data service providers. Further, the numerous exemptions provided for data processors facilitate loopholes and excuses for non-compliance, and therefore threaten the level of data privacy. Interconnectedness and vagueness will imply that accountability and liability for data processors will be ambiguous and interpretational. In addition, the GDPR encompasses large amounts of texts and is difficult to overview from a non-expert point of view. The GDPR is the most lobbied law in the EU's history by corporate interests as well as pro-privacy organizations in the EU and the U.S., affecting how data privacy will be formed in the EU.[153]

Stakeholder consultations present that individuals are increasingly revealing and disclosing personal information to public knowledge, but simultaneously express distrust and uncertainty towards new services. Uncertainty and distrust implies threats to innovation and economical growth in the EU.[154] Stakeholder consultations undertaken in the EU in 2016 demonstrates the majority of citizens, consumers and civil society organizations are in favor of increased protection of data privacy and especially in terms of electronic communications, while a majority of

[151] Phil Lee and Mark Weber, *The New EU General Data Protection Regulation Under 60 minutes!*, FieldFisher, January 31, 2016.
[152] See article four point five in the GDPR; compare to; Phil Lee and Mark Weber, *The New EU General Data Protection Regulation Under 60 minutes!*, FieldFisher, January 31, 2016.
[153] Phil Lee and Mark Weber, *The New EU General Data Protection Regulation Under 60 minutes!*, FieldFisher, January 31, 2016.
[154] Compare to chapters 5.3 and 5.4; see also European Commission, Staff Working Paper Report, 2012, p. 7.

industry representatives do not agree on the necessity for strengthened privacy rules in the EU.[155]

75 % of the citizens living in EU Member States consider that disclosure of personal information is a natural part of their daily life. 43% of the EU citizens think that they have revealed more information than necessary in order to get accessibility to online services.[156] Research indicates that citizens aged between 15 and 39 are most likely to change their browser privacy settings in a stricter manner towards data companies.[157]

5.3.4 Data Privacy Laws and Electronic Communications

The GDPR framework is complemented by regulations setting forth guidelines for the processing of electronic communications.[158] The Directive (2002/58/EC) on Privacy and Communications regulates the privacy of natural as well as legal persons when utilizing publicly available electronic communications services supporting data collection and identification services.[159]

The ePrivacy Directive stipulates that service providers of publicly available electronic communications should take measurements in order to safeguard the security of their services, preferably together with network providers.[160] The use of "cookies" on individual's terminal equipment would be an example of the coexistence and collaboration between communication services and network providers, also regulated by the GDPR.[161] The safeguarding of confidentiality of communications and related traffic data is specifically emphasized.[162]

The ePrivacy Directive set forth detailed guidelines for what a service provider shall do in the event of a personal data breach. Such breach implies that there is a breach of security of the service provider's system, leading to the "*[...] accidental or unlawful destruction, loss, unauthorized disclosure of, or access to, personal data [...]*".[163] Similarly to the GDPR, the ePrivacy

[155] European Commission, Report, *Flash Eurobarometer 443 e-Privacy*, Fieldwork July 2016, publ. December 2016, TNS Political and Social, Survey Requested by the European Commission, Directorate-General for Communications Networks, Content & Technology (DG Connect), Project No. 2016.7036 [Eurobarometer 443, 2017]; Compare to Privacy International, Report, *Privacy International's Contribution to the EU Commission Consultation on the Review on the e-Privacy Directive 2002/58/EC*, July 2016.
[156] Special Eurobarometer 359, 2011, pp. 1-5**.**
[157] Eurobarometer 443, 2016, pp. 5.
[158] 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) [hereinafter: ePrivacy Directive], article 1(1).
[159] ePrivacy Directive, recital 12, article three.
[160] *Ibid.*, recital 20 and article four.
[161] *Ibid.*, recital 25.
[162] *Ibid.*, article five point one. For definition of "traffic data", see recital 15.
[163] *Ibid.*, article two section "i".

Directive encourages practices of collecting personal data only if the users of the electronic services have given prior consent.[164] The ePrivacy Directive has, similarly to the GDPR, a dualistic protection of data privacy and the flourishing of innovation on the Single Market. There are therefore stipulations emphasizing that measurements posed on service providers must reflect the provider's capacity and ability to adopt certain safeguarding steps.[165]

67 % of the citizens in the EU are aware of that personal information on computers, smartphones and tablets can solely be collected under their permission, and 58 % knows that no service provider can store information without permission on abovementioned devices. Although, 58% *incorrectly* believes that current EU data privacy laws ensure that instant messaging and online voice calls are confidential and nobody can get access without prior permission.[166] The majority of EU citizens consider that privacy of their personal information, online communications, and online behavior is important (92%) or very important (78%).[167]

In January 2017, the EU proposed a new regulation on Privacy and electronic communications in order to better safeguard the data privacy of individuals.[168] The proposal is a result from the evaluations undertaken to better safeguard data privacy regarding the GDPR and also due to a specific Regulatory Fitness Performance Program, *REFIT*, introduced during 2009.[169] The proposal explains that the current data privacy protection is ambiguous and has not fully met its objectives. The GDPR requires complementing provisions in terms of protecting confidentiality even in situations where communications do *not* entail personal data and belongs to legal persons. This in order to fully protect privacy set forth in the EU Charter, article seven.[170]

5.3.5 Concluding Notes

The EU approaches the protection of personal data in a dualistic concept by focusing on the protection of data privacy, and the quality of data processing for the economical prospering the Single Market. The aim is to harmonize the level of protection in all Member States. With support from theories and conclusions in sustainable data protection, the dualistic approach in EU data

[164] See for instance articles 9-13; Compare to OECD's principles in chapter 5.2.2 and 5.3.
[165] See article 4(5), for instance.
[166] Eurobarometer 443, 2016, pp. 5-6, 22-26 (See Eurobarometer 443 document for more respondance).
[167] Eurobarometer 443, 2016, p. 29.
[168] European Commission, *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing the Directive 2000/58/EC (Regulation on Privacy and Electronic Communications)*, Brussels, January 10, 2017 [hereinafter: Proposal for Regulation on Privacy and Electronic Communications, 2017].
[169] See Proposal for Regulation on Privacy and Electronic Communications, 2017, p. 2 and 5.
[170] Proposal for Regulation on Privacy and Electronic Communications, 2017, p. 5.

privacy laws are resilient with the interests promoting ecosystem thinking, aligned with sustainable development in the social perspective.[171]

The repeal of directives and adopting of new regulations promoting higher protection of personal data implies higher protection and stricter requirements on the Member States. However, the new provisions have vague prerequisites and exemptions for when more accountability and liability is posed on data processors and controllers. The ambiguity facilitates loopholes to be utilized and denotes unclear responsibilities for data processors as well as sub-processors, and involvement of third parties. Further, it is notable that it took almost six years for the Member States and the European Commission to finalize the GDPR, due to pressure and concerns from large commercial data interests lobbying against strengthened data privacy protection. The major concern among corporate stakeholders is that regulations will challenge innovation and economical development.

Proportionality and balancing of other interests such as freedom of speech, and the right to conduct business are important factors to take into account when formulating data protection laws. However, the framework tends to let commercial interests set the limits of privacy instead of determining the necessary level of privacy protection for individuals in the Member States. Further, the EU framework could focus more on scoping specific technical solutions and the determining of responsibility, accountability and liability on a practical level among the data processors or service providers, in order to align with innovative development. To strengthen data protection provisions on corporate and individual level, measurements similar to pseudynomisation should be further developed.

Yet, EU data privacy laws should be considered as being on the forefront in protective level for individuals in the world. Problematically, the EU must ensure that their level of protection can be ensured in other non-EU countries and data processors' practices, such as the U.S.

5.4 U.S. Privacy Laws in the Commercial Context

5.4.1 The Constitutional Right to Privacy

The U.S. approaches the right to privacy and data privacy differently than the EU in terms of regulating privacy sector-wise. Furthermore, each State in the U.S. has its own data privacy laws, however these will not be presented. Instead, federal law and relevant cases will be analyzed. The historical influences on the US privacy laws derive from the English common law system and the philosophy embracing the importance of liberty. The canon legal system and political history of England are factors

[171] Also compare to the "ultimate idea of protecting privacy", or coherentism, as explained by Gavison and DeCew; Gavison, 1980, 459; and DeCew, 2002, (revision 2013), chapter 1.3.

unambiguously emphasizing the rights and liberties for the citizens of the U.S. in connection to the Declaration of Independence in the late 1700, promoting the civilians right to be independent from the governmental powers.[172]

The Constitution of the United States of America of 1789 set forward in its Fourth Amendment the right and freedom to the people in the U.S. from invasion in their persons, houses, papers and effects, "*against unreasonable searches and seizures, shall not be violated […]"*. The provision entails several terms that indicate protection from public forces, similarly to the provisions set forth in the UN Declaration of Human rights, the Convenant on Civil and Political Rights, ECHR, and the EU Charter.

In 1965, the U.S. Supreme Court ruled in the case of *Griswold v. Connecticut* that individuals have a constitutional right to privacy covering social institutions of marriage and sexual relations to married persons. Further, that privacy could be interpreted as embodied in several of the amendments of the U.S. Constitution; First, Third, Fourth, Fifth, and Ninth Amendments.[173] The opinion in majority of the *Griswold v. Connecticut* case was criticized. According to judge Robert Bork, there was no pre-existing right to privacy in the Fourth Amendment that explicitly recognized a right to privacy, and that the case illustrated an overstep in judicial power. One of the justices, Justice William O. Douglas, clarified in his defense that the right to privacy must be seen in its essence of the First, Third, Fourth, Fifth, and Ninth Amendments, and that they all recognize a "basic zone*"* of privacy. In addition, Justice Douglas argued that all Amendments entail the ability for citizens to make individual decisions about their home and family life.[174] The case of *Griswold v. Connecticut* was the starting point of the right to privacy as embedded in the U.S. Constitution, influencing following cases in the U.S.

Warren and Brandeis have influenced the interpretation of the scope of the Fourth Amendment. In 1967, the right to privacy was extended to capture a broader perspective of privacy. The case of *Katz v. United States* ruled that individuals have an immaterial right to privacy and overruled the previous case of *Olmstead v. United States*. The case of *Katz v. United States* implied that the Supreme Court ruled in favor of Brandeis' standpoint that privacy in the Fourth Amendment did not only scope physical privacy. Thus, the case of *Katz v. United States* concluded that once a person discloses personal information to the public, even if it is in his or her home or at the office, the information cannot be protected by the Forth Amendment.[175]

---

[172] Nissenbaum, 2009, p. 92.

[173] See the case of Estelle T. Griswold et al. (Appellants) v. State of Connecticut, Decided June 7, 1965.

[174] DeCew, 2002, (revision 2013), chapter 2.3; compare to Bork, R., 1990, *The Tempting of America: The Political Seduction of the Law*, New York, publ. Simon and Schuster, 1990.

[175] See *Olmstead v. United States*, 277 U.S. 438 (1928), U.S. Supreme Court, Argued February 20, 21, 1928, decided June 4, 1928 (Brandeis J., dissenting); and *Katz v. United States*, 389 U.S. 347 (1967), U.S. Supreme Court, No. 35, Argued October 17, 1967, Decided December 18, 1967; Compare to Solove, 2008, p. 17.

The right to information privacy and not having information disclosed was subject to decision in the case of *Whalen v. Roe*. The Supreme Court held that the constitutionally protected privacy zone does not only protect individuals right to make decisions independently, but also the interest of a person to not have personal information disclosed.[176] In the case of *California v. Greenwood* it was concluded by the Supreme Court that garbage could not be expected to be private since it is knowingly exposed to the public.[177]

Developed through case law, there are four privacy torts in the U.S. federal legislation; intrusion upon seclusion, public disclosure of private facts, false light and appropriation.[178] Notably, the protection of privacy has adapted theories emphasizing that privacy can be understood differently depending in the context, also influenced with the common law system in the U.S.

5.4.2 The Federal Right to Data Privacy

The U.S. approaches data privacy protection on an *ad hoc* perspective, implying that data privacy is regulated depending on practical application and is determined by organizations' private privacy policies, self-regulation and on a case-to-case basis in different business sectors. Protection of data privacy is therefore subject to both federal and State law that legally overlaps several data privacy issues. Federal legislation set forward abstract principles, or guidelines, for the right to privacy for citizens' and obligations for U.S. corporations. The State of California is considered leading in terms of enacted privacy laws and most up to date regarding privacy regulations, and has impacted federal privacy laws.[179]

In terms of federal law, the definition of protection of personal information in the digital environment has been depicted as "personally identifiable information", or PII. PII entails names, addresses, email addresses, governmental issued identification numbers, bank account number, credit or debit card information, biometric data such as fingerprints, or any other information related to a reasonable identification of an individual.[180] Two different fields of data privacy regulations are presented below, selectively chosen in order to analyze the commercial spectrum of the legal aspect of data privacy in the U.S.

---

[176] *Whalen v. Roe*, 429 U.S. 589 (1977), No. 75-839, Argued October 13, 1976, Decided February 22, 1977.
[177] *California v. Greenwood*, 486 U.S. 35 (1988), No. 86-684, Argued January 11, 1988, Decided May 16, 1988.
[178] Solove, Daniel J., *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*, Yale University Press, December 2007 [hereinafter: Solove, 2007], p. 119.
[179] Jolly, Ieuan, Partner at Loeb & Loeb LLP, Practical Law: a Thomson Reuters Legal Solution, *Data Protection in the United States: overview*, State Privacy Laws.
[180] Compare to S. 547, 114th Congress (Jan 2015 – 2016), Commercial Privacy Bill of Rights Act of 2015, Section 103 (5-6).

5.4.3 Sectorial Data Privacy Laws

5.4.3.1 Data Privacy and Consumer Protection Laws

The first sector of data privacy addresses different aspects on general consumer protection. According to the Federal Trade Commission Act 15 U.S.C. of 1914[181], provisions §§41-58 protects consumers from unfair or unreliable practices by U.S. companies. The FTC Act has been applied to online as well as offline privacy policies and the FTC is authorized to bring enforcement measurements against companies failing to comply with the company's own privacy policies, or if companies have disclosed personal data of consumers in an unauthorized manner. The FTC is also a federal watchdog over consumer protection and is the prime regulator for consumer privacy concerns in the U.S. The FTC has developed guidelines; limiting unwanted calls and emails to consumers, online protection of children, online security, and identity theft.[182]

The FTC Act is *not* explicitly setting forward concrete data protection regulations for specific forms of data. Thus, the FTC Act serves to ensure that companies with already established privacy policies will comply accordingly.[183] In the FTC Behavioral Advertising Principles, the FTC provides advice to companies undertaking behavioral advertising to disclose notification processes and "opt-out" solutions for consumers in order to follow best practices in the U.S. Thus, the abovementioned principles are not binding if a company has not enacted them.[184] The FTC Act addresses any company or individual undertaking business in the U.S. except from businesses facilitating financial services or electronic communication providers, for instance, which is regulated exclusively within their specific business sector.[185]

The 114th Congressional term has introduced an amended Bill of Rights regarding data privacy, and therefore extended rule-making capacity for the FTC to create further responsibility on businesses collecting and processing personal data. Further on, more control for individuals such as facilitating actively given consent and mechanisms for correcting stored information has been developed.[186] The new federal incitements by the U.S. Congress imply that businesses managing personal data must take necessary

[181] [Hereinafter: FTC Act].
[182] The FTC Act 15 U.S,C, §§41-58; compare to Federal Trade Commission, Online Guidance Report, Privacy, Identity & Online Security, Consumer Information.
[183] Jolly, Ieuan, Partner at Loeb & Loeb LLP, Practical Law: a Thomson Reuters Legal Solution, *Data Protection in the United States: overview*, Main Data Protection Rules and Principles.
[184] FTC Staff Report: *Self-Regulatory Principles For Online Behavioral Advertising*, Behavioral Advertising: Tracking, Targeting, & Technology, February 2009.
[185] Jolly, Ieuan, Partner at Loeb & Loeb LLP, Practical Law: a Thomson Reuters Legal Solution, *Data Protection in the United States: overview*, Notification.
[186] S. 547, 114th Congress (Jan 2015 – 2016), Commercial Privacy Bill of Rights Act of 2015, Section 111 – 122.

measurements in order to program systems in their business model to safeguard data privacy, defined as "privacy-by-design".[187]

5.4.3.2 Data Privacy in Electronic Communications

The second sector addresses electronic communications. The Electronic Communications Privacy Act of 1986[188], 18 U.S.C. §2510, regulates practices for electronic communications and computer damaging and applies to governmental authorities as well as private actors.[189] ECPA protects oral or wired communications when such communications are being made, in transit, or stored digitally. ECPA applies to data, emails or telephone conversations stored electronically.[190] ECPA is divided into three parts; *the Wiretap Act*, *the Stored Communications Act*, and *the pen register and trace and track devices Act*.

The Wiretap Act prohibits unlawful interception of communications and any obtaining, usage, or disclosing of such communications in provision ECPA 18 U.S. Code § 2515. Further, it restricts illegally obtained communications to be used as evidence.[191] Google Inc. has been subject to a class action lawsuit in violation of the Wiretap Act and was alleged of, in an unauthorized manner, scanning private emails of individuals for advertising purposes. The lawsuit was settled where Google certified that no processing of emails will continue, however, only prior to the point where a Gmail user can retrieve email, and that scanning of emails will then continue on Google's servers.[192] The U.S. Congress is currently considering an *Email Privacy Act* to be enacted, implying that the current situation for individuals and protection of their personal data is considered evident.[193]

The second part of ECPA, the *Stored Communications Act*, regulates the protection of private information stored in files by service providers of electronic communications, or in records held by a "subscriber" of services provided by a service provider. Such private information relates to the subscriber's name, billing address or records, and IP address.[194] According

[187] S. 547, 114th Congress (Jan 2015 – 2016), Commercial Privacy Bill of Rights Act of 2015, Section 113.
[188] [Hereinafter: ECPA].
[189] The Computer Fraud and Abuse Act of 1986, 18 U.S.C. §1030, compliment ECPA.
[190] The Federal Privacy Council, *Electronic Communications Privacy Act of 1986 (ECPA)*, Online Guidelines, March 15, 2017.
[191] Wiretapping by lawful means is, however, exempted from the provisions, with reference to the Foreign Intelligence Surveillance Act. Compare to Justice Information Sharing, U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, *Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S. § 2510-22*, Information Table for Federal Statues, March 16, 2017.
[192] *Daniel Matera and Susan Rashkis, as individuals, and on behalf of other persons similarly situated v. Google Inc.,* United States District Court, Northern District of California, Case No. 5:15-cv-04062 LHK, Joint Declaration of Class Counsel in Support of Plaintiff's Motion for Preliminary Approval of Class Action Settlement, March 9, 2017, Judge: The Hon. Lucy H. Koh.
[193] See H.R.387 – Email Privacy Act, 115th Congress (2017-2018).
[194] Justice Information Sharing, U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, *Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S. § 2510-22*, Information Table for Federal Statues, March 16, 2017.

to ECPA 18 U.S. Code §2701, any person or entity is prohibited to access a facility that provides electronic communication intentionally without authority to do so. According to provision ECPA 18 U.S. Code §2702, any service provider of electronic communications to the public shall not knowingly disclose the contents stored, maintained or carried out on that service to any person or entity.[195]

The third part of ECPA, the *pen register and trace and track devices Act*, constrains the usage of devices that capture incoming or outgoing telephone calls or other communications, so called "pen registers" or trace and tracking devices, according to ECPA 18 U.S. Code Chapter 206. The third part is mainly addressing situations where U.S. governmental officials need accurate permission to undertake criminal investigations.

On March 31 2016, the Federal Communications Commission[196] proposed new regulation on the data collection, use, and sharing practices of Internet-based Broadband Service Providers in order to amend the Communications Act of 1943. The new proposed framework indicated stronger requirements to be addressed to Internet broadband service providers, more transparency for consumers of their collected data, more control of what data is being used, "opt-in" and "opt-out" requirements, and security requirements on the service provider when personal data is being used or stored.[197] The stricter rules were incentivized by cases that have problematized such measurements.[198] In a case against Verizon, the FCC alleged that the company failed in providing opt-out mechanisms for customers and therefore, in an unauthorized manner, collected personal information about customers in order to target them with marketing.[199]

In March 2017, however, the Congress voted in favor of *deregulating* telecommunication services and their collecting and storing of consumer's data. This implies that broadband services that were required by law to ask for permission to track and sell personal data of costumers, are not obliged to ensure such permission. In a perspective of protecting individuals'

[195] Stipulated exemptions in ECPA 18 U.S. Code § 2703 are situations where the originator, subscriber, or intended recipient has given a legitimate consent, or due to law enforcement incitements by the U.S. government authorities.
[196] [Hereinafter: FCC].
[197] Federal Communications Commission, Notice of Proposed Rulemaking, Before the Federal Communications Commission, Washington D.C. 20554, in the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunication Services, WC Docket No. 16-106, Adopted March 2016, Released April 1, 2016 (Chairman Wheelers and others), p. 2507, para 14.
[198] See for instance; *Order in the Matter of AT&T Services, Inc*., before the Federal Communications Commission, April 8, 2015, regarding the failure in the duty of protecting consumer proprietary information;
[199] See Adopting Order, In the matter of Verizon, Compliance with the Commission's Rules and Regulations Governing Customer Proprietary Network Information, File No.: EB-TCD-13-00007027 Account No.: 201432170014 FRN: 0016304214, Adopted September 2 2014, Released September 3 2014.

personal data in the U.S., this action is a step back in the direction for strengthening data privacy policies in the U.S. on federal level.[200]

In a responding article by privacy expert Solove, he argues that this set back and deregulation of privacy laws on federal level will *not* result in more freedom for the data provider's industry. According to Solove, a "vacuum" in regulation will imply that other regulators will fill the gap.[201] Data processing, monitoring, transmitting and storing of personal data are activities subject to other federal laws, sectorial laws, but also EU law. EU regulators already consider U.S. privacy laws fragmented and have gaps, and this set back could therefore imply that EU privacy laws responds even more skeptical, a crucial influence on U.S. companies with business in, or affected by, the EU.[202]

Despite the above regulations, there are various other different industry-based regulations, such as the Gramm-Leach-Bliley Act regulating financial services providers. Further, data privacy in medical records and the Health Insurance Portability and Accountability Act, Children's Online Privacy Protection Act, and the Fair Credit Reporting Act, among others. Further, there are also guidelines set forward by different business groups such as the Network Advertising Initiative and the Privacy Future Forum. Such guidelines are not enforceable and are merely serving as best practices in their specific field.[203]

According to stakeholder surveys undertaken by the National Telecommunications and Information Association, 84 % of the American households express concern about their data privacy in the U.S. The concerns are related, but not limited to, the interaction on online-based services when purchasing goods and services, activities on social networks, and expressing opinions online. Customers are further concerned that personal information will end up with third parties, be subject to identity theft, that private information will be disclosed that could harm their personal lives, and data being used by employers, insurance providers, creditors and other institutions that could base decisions upon such information without the knowledge of the customer.[204]

---

[200] Kang, Cecilia, *Congress Moves to Overturn Obama-Era Online Privacy Rules*, The New York Times, March 28, 2017.

[201] Solove, Daniel J., Article, *Congress's Attempt to Repeal the FCC Internet Privacy Rules: The Void will be Filled*, Teach Privacy, April 2, 2017; compare to: Network Advertising Initiative (NAI) Yearly Summit 2017, Panel Discussion with Gina Woodworth, Emmett O'Keefe, Noga Rosenthal, Reed Freeman, Current at Pier 59, Chelsea Piers in New York City, May 17 2017.

[202] Solove, Daniel J., Article, *Congress's Attempt to Repeal the FCC Internet Privacy Rules: The Void will be Filled*, Teach Privacy, April 2, 2017.

[203] Jolly, Ieuan, Partner at Loeb & Loeb LLP, Practical Law: a Thomson Reuters Legal Solution, *Data Protection in the United States: overview*, Other Laws and Guidelines.

[204] Federal Trade Commission, Before the Federal Communications Commission Washington D.C. 20554, *Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission*, in the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunicatoions Services, WC Docket No. 16-106, May 27, 2016, pp. 1-2.

5.4.4 Concluding Notes

The U.S. approaches data privacy protection based on different business sectors. This implies that data privacy is regulated differently depending on what kind of data services or products individuals use, and the kind of commercial actor that processes the data. According to several privacy theorists and earlier conclusions in this thesis, it has been presented that privacy must be seen as a contextual right.[205] With that said, the U.S. approach for protecting data privacy aligns with privacy theories promoting privacy as a contextual right. The U.S. approach can also be seen as flexible depending on the business sector, providing narrow expertise in each sector to see what regulative needs there are.

However, the patchwork of regulations on data privacy appears to be complex and difficult to overview, also overlapping each other and lacking exhaustive protection. The FTC has ability to overlook the level of protection on a general consumer aspect, however the FTC will not be able to safeguard PII transmitted via all Electronic Communications, or regarding medical or financial institutions, for instance. Data privacy in the U.S. federal aspect is therefore lacking a comprehensive protection system. Individuals have no uniformed control over third party involvement and data processing of their PII when data is transmitted between different business branches.

The protective approach in the federal U.S. legal system could benefit from a more systemized collaboration between authorities, but foremost companies and individuals. Individuals must also be better informed. Further on, the existing commercial data privacy regulations are merely guidelines and not binding until implemented. Recent proposed legislation introduced broader jurisdiction for the FTC over telecom providers. However, the current political situation on federal level in the U.S. seems to deregulate data privacy protection to an increasing extent. Again, there is a lack of fully protecting regulations in the U.S. and the future legal status of data privacy in the U.S. is unclear.

5.5 Conclusions on Legal Aspects in the EU and the U.S.

The U.S. data privacy laws differ from the EU due to sector-based regulations. Thus, the U.S. approaches data privacy protection similarly to leading privacy experts with the perception of privacy as dependent on the specific context.[206] The sector-based approach contributes to more narrow regulations based on specific branches, and compared to the EU this is facilitating better understanding of what specific regulative needs there are. However, the EU have a more rigorous framework for data privacy

[205] Compare to chapter 2 and 3.
[206] Compare to chapters 2.2 and 3.

protection, and have a better ecosystem approach for balancing individuals right to data privacy versus business interests. Both the EU and the U.S. have introduced an approach called “privacy-by-design”, indicating that innovation and technical measurements are considered to be crucial factors for the future of data privacy protection in both economies.

In order to create more fully protecting regulations and more simplistic understanding of data privacy, one must take into account the global markets and transnational data flows. Technology is not national but an international matter. In terms of the definition of PII, the EU definition “personal data” is broader considering that each sector has its own definition of what constitutes PII in the U.S. The difference in definition creates data processing obstacles from a commercial point of view between actors in the EU and the U.S. The differencing level of data privacy protection in the EU and the U.S. will also be affected from the deregulation of broadband services. In order to build data transfer “bridges” between the U.S. and the EU, there has to be well-functioning standards, such as partnerships and agreements both on governmental and private level, to protect data privacy in a sustainable manner.

6 Transatlantic Data Privacy Protection

6.1 Introductionary Notes

EU laws and U.S. regulations on the protection of data privacy have been analyzed in previous chapters. As has been presented, the two economies approach data privacy protection differently. The EU tends to adapt broad regulations focusing on technical neutrality, and the balance between data quality and the protection of data privacy. The U.S. has a sector-based protection with more focus on key operators in each sector.[207] With that said, data flows are moving transnationally as a global legal matter.

Argued by EU and U.S. institutions as well as experts, the digitalization is crucial for economic growth and the transnational trade status.[208] In 2014, almost 50% of the world's GDP was due to the economic status of the EU and the U.S. jointly.[209] Collaboration in data privacy protection between the EU and the U.S. has been commenced formally since 2000 when the *Safe Harbor Agreement* was introduced. The Safe Harbor agreement implied that U.S. corporations and government authorities were obliged to comply with the data privacy laws of the EU when collecting, monitoring, transmitting or storing personal data of individuals in the EU. The Safe Harbor Agreement was clarified invalid in 2013, and the status of the transnational level of protection of data privacy was brought to attention when U.S. national security authorities were alleged of disrespecting the EU privacy laws.[210]

This chapter presents how the two largest economies in the world have dealt with the flows of personal data transnationally, what obstacles that have threatened the protection of data privacy in the EU as well as the U.S., and the importance of a well-functioning relationship between the two economies for upholding the level of data privacy protection and economical status.

---

[207] See chapters 5.3 and 5.4.

[208] European Commission, Growth: Internal Market, Industry, Entrepreneurship and SMEs, Online Report, *The Importance of the Digital Economy*, March 19, 2017; U.S Department of Commerce, Online Report, *U.S. Secretary of Commerce Penny Pritzker Discusses Importance of Digital Economy at 2016 Hannover Messe Digital Transformation of Industry Conference*, April 25, 2016; compare to Klosek, 2000, p. 1-2; and Vacca, 2012, Chapter 42, p. 739.

[209] Eurostat, Statistics Explained, *The EU in the World – Economy and Finance*, Data Extracted in March 2016 (March 19, 2017).

[210] Fidler, David P., *The Snowden Reader*, Bloomington, Contributor Ganguly, Sumit Indiana University Press, 2015 [Fidler, 2015], pp. 1-7.

6.2 Leakings and Transnational Lawsuits

Former employee at the Central Intelligence Authority[211] Edward Snowden was subject to worldwide attention in 2013 when he leaked an estimated amount of 1.7 million documents for public disclosure. The documents contained information of surveillance undertaken by the National Security Authority[212] of individuals. In terms of the transatlantic relationship between the EU and the U.S. the findings were grave, indicating that U.S. authorities had undertaken surveillance of individuals resident in the EU and therefore a violation of the EU data privacy laws and the Safe Harbor Agreement. Further, the surveillance had been possible due to usage of "back doors" in the systems of private corporations such as Google and Facebook with a program called *Prism*.[213]

Not only did the leaks clarify that the American government had violated individuals' right to data privacy in the EU, but also that U.S. IT companies had access to an insurmountable amount of personal data that individuals could not control. An Austrian law student and Facebook user, Maximillian Schrems, detected that his personal information on Facebook had been presumably available for the NSA to process and store.

Mr. Schrems alleged a legal claim with the Irish Data Commissioner at the Irish Authority, arguing that his data privacy had been violated against EU Privacy laws as his personal information had been disclosed through the services of Facebook and collected by the NSA. Furthermore, Mr. Schrems argued that the U.S. authority had proven insufficient protection according to the EU data protection framework, and in violation of the Safe Harbor Agreement.[214]

The Irish Data Commissioner and the Irish Authority disputed Mr. Schrems claim contending that there was no violation by the U.S. authority since the U.S. had ratified the Safe Harbor Agreement.[215] Mr. Schrems appealed to the High Court of Ireland that designated a preliminary ruling to the EUCJ.[216] The EUCJ concluded that the NSA had violated EU privacy

[211] [Hereinafter: CIA].
[212] [Hereinafter: NSA].
[213] Fidler, 2015, pp. 1-7; compare to: Szoldra, Paul, Business Insider Article, Tech Insider, *This is Everything Edward Snowden Revealed in One Year of Unprecedented Top-secret Leaks*, September 16, 2016.
[214] C-362/14 in the Case of *Maximillian Schrems v. Data Protection Commissioner, joined party Digital Rights Ireland Ltd*, Judgment of the Court (Grand Chamber), October 6, 2015.
[215] The Irish authorities argued that the U.S. had guaranteed compliance with the EU data privacy laws, according to the European Commission Decision 2000/520/EC.
[216] European Commission Decision 2000/520/EC Commission Decision 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 (notified under document number C (2000) 2441) (Text with EEA relevance), Official Journal L 215 , 25/08/2000 P. 0007 – 0047.

laws.[217] The EUCJ declared the Safe Harbor Agreement invalid and suspended any data transfer containing personal information of individuals resident in the EU to U.S. authorities or companies.[218] The suspension of data transfer from the EU to the U.S. implied an obstacle in the transnational economical status, and the two economies started to form a new data transfer agreement in order to maintain the relationship; the EU-U.S. Privacy Shield.[219]

6.3 The EU-U.S. Privacy Shield

The attention highlighted in the case of *Mr. Schrems v. the Irish Data Commissioner* incentivized several governmental measurements, nonetheless in the U.S. In 2015 the U.S. enacted the *Judicial Redress Act*, improving the protection of privacy against U.S. government authorities of non-U.S. citizens. The *Judicial Redress Act* improved the protection for EU citizens. Thus, the level of protection in data privacy in the U.S. was still considered incompatible and behind the level in the EU.[220]

The European Commission and the U.S. Department of Commerce[221] exchanged research and reported for several years until the Privacy Shield was ratified in 2016, replacing the Safe Harbor Agreement. The European Data Protection Supervising authority, *Working Party 29*[222], had extensive influence and was appointed by the European Commission to specifically investigate and approve the measurements undertaken from the U.S. authorities to ensure compliance.[223]

Today, the European Commission and the U.S. DoC argue that the Privacy Shield benefit individuals as well as companies in several ways. Individuals in the EU are guaranteed the same level of protection when their personal

[217] U.S. authorities were subject to compliance with the EU privacy laws in order to collect, transmit, store and use personal information of individuals in the EU.
[218] Court of Justice of the European Union, Press Release No 117/15, The Court of Justice Declares that the Commission's US Safe Harbour Decision is Invalid, Judgement Case C-362/14: Maximillian Schrems v Data Protection Commissioner, Press and Information, October 6, 2015.
[219] [Hereinafter: The Privacy Shield].
[220] European Parliament Report, *A Comparison Between US and EU Data Protection Legislation for Law Enforcement*, Policy Department C; Citizens' Rights and Constitutional Affairs, Directorate-General for International Policies, Study for the LIBE Committee. A Study by: Prof. Dr. Franziska Boehm, University of Münster, Institute for Information, Telecommunication and Media Law, Germany With the help of Markus Andrees, Jakob Beaucamp, Tim Hey, Robert Ortner, Giulia Priora and Felix Suwelack, 2015, pp. 51-54; Compare to: European Parliament Report, The US Legal System on Data Protection in the Field of Law Enforcement: Safguards, Rights and Remedies for EU citizens, Policy Department C, Directorate-General for International Policies, Study for the LIBE Committee. A Study by: Prof. Bignami, Francesca, George Washington University Law School, Washington, DC, USA, and Responsible Administrator Mr Davoli, Alessandro, 2015, p. 5.
[221] [Hereinafter: DoC].
[222] Soon to be called the *European Union Data Authority (EUDA)*.
[223] See for instance; Statement of the Article 29 Working Party, Brussels, October 2015.

data is transferred to U.S. companies, U.S. companies that voluntarily ratify the Privacy Shield must form and ensure corporate policy programs and annual reporting of compliance. U.S. companies must also inform and provide a free and independent dispute settlement for EU individuals, and therefore be subject to law enforcement measurements and remedies by the U.S. DoC.[224] The European Commission and the U.S. DoC have evident incitements to retain the trade and investment relationship between the two economies due to their positions on the global market.[225]

The interest of promoting business and economical growth is inevitable in the Privacy Shield. Thus, the protection of personal data transferred between the EU and the U.S. is subject to prerequisites; the Privacy Shield is optional for U.S. companies to ratify, implying that the framework is subject to bendiness. If a U.S. company chooses to ratify, it is legally bound by the provisions in the Privacy Shield and also subject to the special law enforcement procedures set forth, entailing the oversight system of DPAs.

If a U.S. company chose *not* to ratify, it is still subject to EU privacy laws if any transfer of personal data of EU individuals is undertaken. Any processing of personal data connected to EU individuals and non-compliance will be subject to EU procedures and not the special and efficient framework provided in the Privacy Shield. The current effective privacy laws in the EU refer to the GDPR and the ePrivacy Directive.[226] Special focus is on individuals' right to be forgotten and the control of personal information.[227]

The Privacy Shield is still under formation and large companies have undermined its power. Companies such as Facebook Inc., Google Inc., and Microsoft Inc. have decided to comply partly with the agreement and indicate certain dominance towards the agreement, even though these companies have declared their compliance officially.[228]

---

[224] United States Department of Commerce, Annex I, EU-U.S. Privacy Shield Framework Principles, The Under Secretary for International Trade, Washington D.C., 20230, Febrary 23, 2016, p. 4.

[225] United States Department of Commerce, Annex I, EU-U.S. Privacy Shield Framework Principles, The Under Secretary for International Trade, Washington D.C., 20230, Febrary 23, 2016, p. 4; compare to: European Commission, Decisions, 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.

[226] And momentarily the Regulation on ePrivacy.

[227] European Commission, Fact Sheet, *How does the Data Protection Reform Strengthen Citizens' Rights?* January 2016.

[228] Compare to; C-131/12, the case of *Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzalez*, Judgement of the Court (Grand Chamber), 13 May, 2014; compare to: Spion Report by Van Alsenoy, Brendan, Verdooth, Valerie, Heyman, Rob, Ausloos, Jef and Wauters, Ellen, *From Social Media Service to Advertising Network: A Critical Analysis of Facebook's Revised Policies and Terms*, Interdisciplinary Centre for Law and ICT/Centre for Intellectual Property Rights (ICRI/CIR) of KU Leuven and the department of Studies on Media, Information and Telecommunication (SMIT) of the Vrije Universiteit Brussel (VUB), both departments part of iMinds, Draft February 23, 2015 [hereinafter: Spion Report, *From Social Media Service to Advertising Network: A*

During the first period of 2017, the Privacy Shield has met governmental challenges. The current President of the United States has brought forward an executive order regarding the enhancement of public safety in interior of the U.S., and under section 14 the order concludes that U.S. agencies are from now on *only* subject to U.S. privacy policies, and does not cover any non-Americans regarding the collection and usage of personal identifiable information being subject to other laws.[229] This implies that the invoking of EU privacy laws to overrule such actions might be unsuccessful. Even though this executive order regards public authorities in the U.S., it is possible that the domestic interests of the U.S. will affect even the commercial incitements to maintain the Privacy Shield agreement, such as mentioned regarding the deregulation measurements of broadband service providers during March 2017.[230]

6.4 Concluding Notes

As has been presented in this chapter, the transatlantic partnership on data protection is subject to political vulnerability and influenced by trade incentives. The specially appointed enforcement mechanisms and the liabilities according to the Privacy Shield require full collaboration between the EU and U.S. authorities in order to be successful. Yet, commercial IT interests as well as the U.S. government have challenged the agreement fundamentally from the beginning. This chapter clarifies that large corporations have extensive opportunities to affect the transnational data transfer regime.

Data privacy is a transnational matter why protection must be practiced and complied with on transatlantic level, but foremost on corporate and individual level. The EU and the U.S. are able to look after their national interests, but cannot overrule the sovereignty of one another in terms of international data flows. A transatlantic dispute settlement system is efficient, but trigger issues of democratic power in the Member States of the EU as well as the U.S.

The current data privacy partnership is crucially formed based on economical incentives, influencing the outcome for the level of protection. The EU and U.S. should focus on transnational data quality and safeguarding the highest level of data privacy protection. A transatlantic agreement as the Privacy Shield explains a "general aim" to respect one another's data privacy laws. Thus, the agreement becomes undermined by

---

Critical Analysis of Facebook's Revised Policies and Terms, 2015]; compare to: Reuters Technology News, article by Fioretti, Julia, Facebook '*Tramples European Privacy Law': Belgian Watchdog*, Brussels, May 15, 2015 (April 5, 2017); The Telegraph, Article by Titcomb, James, Facebook Signs Up to Privacy Shield Data Treaty, October 15, 2016; compare to: The Privacy Advisor, Article by Meyer, James, Hamburg's DPA Aiming to Challenge Privacy Shield, August 4, 2016.

[229] The White House, Office of the Press Secretary, *Executive Order: Enhancing Public Safety in the Interior of the United States*, section 14, January 25, 2017.

[230] See chapter 5.4.3.

corporate interests and actors; actors that should lead by example for a more sustainable relationship. An interstate partnership might therefore not be sufficient for the development of sustainable data protection practices. In order to find sustainability in the transatlantic data protection regime, the EU and the U.S. must strengthen the incentives among commercial actors handling personal information transnationally, promoting high quality of data and secure flows of personal data between the two economies.

7 Commercial Privacy-by-Design

7.1 Introductionary Notes

As has been depicted in previous chapters in this thesis, legal protection on data privacy differ between the EU and the U.S. EU legislators have difficulties managing the balance between individual's and companies' interests where technical capacity and economical incentives steers how much privacy that should be considered sufficient. This "generality" opens up for possible loopholes. Thus, the EU has taken distinguishing steps towards stricter regulations, where solutions as pseudynomisation indicates actual examples on how commercial actors should implement better data privacy practices.[231]

In terms of the U.S., the sectorial business laws and the difference between federal and state laws result in differences regarding the level of protection on data privacy. The U.S. data privacy approach further implies a patchwork of rules where companies are forced to comply with overlapping regulations in terms of consumer protection and electronic communications, for instance. However, the legal status of U.S. data privacy protection has adopted a context-based approach that aligns with fundamental theories of privacy. Further, the sector-based approach also opens up for flexibility and specialization of each business-sector, hopefully leading to more understanding of data privacy in each sector.[232]

As has been presented, social values and philosophical standpoints have impacted both the EU and the U.S. Still, the EU level of protection is more rigorous than the data privacy protection in the U.S. Recent updates on data protection regulations in the EU and U.S. is evidence of this.[233] Even though the protected level differs, stakeholder consultations on individuals and consumer standpoints indicate that data privacy protection is an equal concern in both the EU and the U.S.[234] Concluded by privacy experts and professionals in data privacy, the importance of data privacy is an increasing standpoint in both economies.[235]

In this chapter, the infrastructure and technical flows of personal information will be analyzed, in terms of system-based solutions as well as concrete devices facilitating the processing of personal data. The purpose of this chapter is to illustrate examples of what actual technical solutions and systems that initiate the application of data privacy laws, and in what way such innovation challenges development of sustainable protection on data

[231] See chapter 5.3.
[232] Compare to chapter 5.4.
[233] See Brygrave, 2014, p. 205.
[234] Compare to chapter 5.3.3 and 5.4.3.
[235] See chapter 2 and 4.

privacy. The challenges could be summarized as; (1) the lack of clarity for companies, and the protecting of individuals interacting as "users" rather than customers and buyers, (2) established business models based on collecting personal data, (3) the lack of incentives among powerful companies to change such business models, and (4) an interconnected system with an uncontrolled and immense exchange of personal information between different services and products.

7.2 Data Privacy and Examples of Current Technology

Corporate interests are powerful and have impacted recent data privacy regulations and policy-making extensively in the EU and the U.S.[236] Three of the top ten largest IT companies in the world; Google, Facebook, and Microsoft, each spent $16.66 millions, $9.85 millions and $8.49 millions on lobbying *against* strengthened data privacy protection in 2015.[237]

IT companies have their business model built on data collecting, processing, monitoring, and storing personal data. Below is a corporate aspect of Facebook; the world's most used social network service, as an example of technical implications of transnational data flows of personal data. Further, it will be demonstrated how "Internet-of-Things" has impacted individuals' right to data privacy, as an example for how concrete devices are interconnected that monitor and store individual's personal data.

7.2.1 Social Networking - Transmitting and Storing of Personal Data

The American-based company *Facebook Incorporated*[238] is the largest social network platform in the world. The company has developed a core business model focusing on using, transmitting and storing personal data, benefiting social connections and networking possibilities for approximately 1.2 billion users around the world. Facebook has formally ensured that the company is complying with EU privacy laws and is always improving the protection of individuals' privacy.[239] However, the company has countered several allegations for violating users' data privacy both in the U.S. as well as the EU, and has also elicited international lawsuits challenging the transatlantic relationship.[240]

---

[236] Corporate Europe Observatory, Exposing the Power of Corporate Lobbying in the EU, Article, *Crowdsourced Lobby Exposé Shows Internet Giants have Footprints on our Data Privacy Laws,* February 18, 2013 (April 3, 2017).
[237] Statista, Statistic Report by Richter, Felix, *Lobbying Expenditure by U.S. Tech Companies*, January 25, 2016, (April 3, 2017).
[238] [Hereinafter: Facebook].
[239] See Facebook's Privacy Policy; compare to: Spion Report, *From Social Media Service to Advertising Network: A Critical Analysis of Facebook's Revised Policies and Terms,* 2015; compare to: Reuters Technology News, article by Fioretti, Julia, Facebook '*Tramples European Privacy Law': Belgian Watchdog*, Brussels, May 15, 2015 (April 5, 2017).
[240] See for instance; the case of Matthew Campbell et al., v. Facebook Inc., United States

Facebook is profiling their users by using different servers and systems that are interacting in order to best adapt its services to users demands, the so-called *Social-Graph*. The *Social-Graph* implies the connection between users activities, users friends activities, events, photos, status updates, and several other operators and activities interacting from the commercial perspective as advertisers.[241]

In recent years, Facebook's technological capacity has advanced, implying that the company can collect, process, transmit and store data from partnered companies as WhatsApp and Instagram. Individuals enable other services, such as mobile applications, to confirm access by providing personal information collected by Facebook. Continuously, this technical advancement entails the improved achievement of more detailed information about users, and the ability to create an immense network for advertisement where personal data is collected on users as well as non-users of Facebook.[242]

Facebook's technical capacity set the company in a monopolistic position on the market for online social networking. Facebook is connecting individuals, businesses, advertising companies, but also public authorities into one network. This interconnectedness implies that personal data is widely transmitted inside as well as outside Facebook's data system. Personal data provided by users in the belief that the information stay within his or her closest network, is in fact used for advertisement purposes, for improving Facebook's connections to partnered companies, and for several other commercial purposes. The company has been criticized for leveraging its dominant position by offering its users a "take-it-or-leave-it" concept, questioning the validity and enforcement of EU data privacy laws, U.S. consumer and communication laws, and the transatlantic relationship.[243]

According to the EU GDPR, consent must be given to the collecting, transmitting, monitoring, and storing of personal data. Such consent entails the *"[...] freely given, specific, informed and unambiguous indication of the data subject [...]"*, through a "*statement*" or "*affirmative action*" to the processing of personal data related to that data subject.[244] When signing up to Facebook's services, a text appears stating that the user agrees to the

---

District Court Northern District of California, Case No. 13-cv-5996-PJH, Order Granting in Part and Denying in part Motion for Class Certification; compare to Maximilian Schrems v. Facebook (Irish Data Commissioner), chapter 6; and Spion Report, *From Social Media Service to Advertising Network: A Critical Analysis of Facebook's Revised Policies and Terms,* 2015.

[241] MIT Technology Review, Zeichick, Alan, *How Facebook Works*, June 23, 2008 (April 5, 2017).

[242] Spion Report, *From Social Media Service to Advertising Network: A Critical Analysis of Facebook's Revised Policies and Terms,* 2015, p. 9. Compare to Scott, Mark, The New York Times, *Facebook Gets Slap on the Wrist from 2 European Privacy Regulators*, May 16 2017.

[243] *Ibid*, p. 10; compare to chapter 5.3, 5.4 and 6.

[244] See GDPR article 4(11); for further definition on "consent", see Article 29 Working Party, *Opinion 12/2011 on the Definition of Consent, Adopted on 13 July, 2011,* 01197/11/EN, WP187.

terms of Facebook and has read the data user policy as well as Facebook's "cookie use". Since Facebook include all its functions under the same consent indicator when signing up, it is questionable whether it could be concluded that the user have consented to *all* data processing procedures within the Facebook network.[245]

Users can adjust the audience when posting status updates, photos or attending events. Though, the data privacy policies indicate that the user agrees to let Facebook use and transmit content published as copyright protected photos or videos, which are owned by Facebook once a user publish such content. The privacy policies do not clarify whether other commercial actors, partnered companies or other third parties can get access to the content or not. Facebook's Privacy Policy states that Facebook "*[…] store data for as long as it is necessary to provide services to you and others […]"*, and that "*[…] information associated with you is kept until the account is deleted, unless we do no longer need the data […]"*.[246] Facebook has not provided any detailed explanation for how long "necessary" entails, indicating that Facebook's compliance with the "right to be forgotten" provision in the GDPR article 17 is questionable.[247]

Facebook has correspondingly been subject to lawsuits concerning its liabilities towards U.S. consumer protection and electronic telecommunication laws.[248] Cases have concerned alleged lack of sufficient consumer protection, the tracking of users after logging out of Facebook's services in an incompatible manner, and the collecting and storing of biometric data with face recognition technology, scanning users faces and suggesting tagging without explicit consent.[249] Further, third party transmitting practices have been brought up even in U.S. courts, indicating users' dissatisfaction of Facebook's sharing of PII to advertising companies.[250]

---

[245] Spion Report, *From Social Media Service to Advertising Network: A Critical Analysis of Facebook's Revised Policies and Terms,* 2015, p. 13.

[246] See Facebook's data privacy policies "*How can I Manage or Delete Information about me?"*

[247] Personal Enquiry/ Customer mail from Edler, Beatrice to the Privacy Team at Facebook, sent October 17, 2016.

[248] See for instance; *Matthew Campbell et al., v. Facebook Inc.*, United States District Court Northern District of California, Order Granting in Part and Denying in Part Motion for Class Certification (re: unsolicited scanning of users messages), and; *In Re Facebook Internet Tracking Litigation*, United States District Court Northern District of California San Jose Division (Justice Edward J. Davila), Order Granting Defendants Motion to Dismiss, (re: unsolicited use of cookies alleged in violation of the Wiretap Act, among other matters).

[249] Compare to cases of: *Jose Palomino et al. v. Facebook Inc*, United States Court Northern District of California, Order Granting Motion to Dismiss with Prejudice; *Nimesh Patel et al. v. Facebook Inc.*, United States District Court Northern District Illinois, Eastern Division, Class Action Complaint for Violations of the Illinois Biometric Information Privacy Act.

[250] See for instance the case of *Angel Fraley et al., v. Facebook Inc.,* United States District Court Northern District of California, San Jose Division, Facebook Inc.'s Reply in Support of Motion to Dismiss Second Amended Class Action Complaint, September 29, 2011.

The U.S. cases problematize Facebook's technical advancement, and how to uphold an equal level of protection between state laws and federal laws. Facebook's technical standards trigger ambiguity in the provisions and torts regarding data privacy that actualize grey zones in the law. For instance, consumer laws address "sellers" and "consumers" of services and products, not entirely compatible with what Facebook provides its "users".[251]

It is evident that Facebook has impacted the perspectives on data privacy in the EU as well as the U.S. Problematically, case law and the implication of technological advancement illustrate the difficulty to find sustainable data privacy solutions. Facebook has a dominant position on the global market with subsidiaries in the whole world, and has an ability to lead by example. Instead, case law and transatlantic agreements indicate that data privacy cannot be protected to its full potential, letting Facebook set its own standards. Whether the company itself should take better incentives and reasonable steps towards more sustainable data privacy protection practices is a remaining question.[252]

7.2.2 Internet-of-Things and Monitoring of Individuals' Behavior

What was presented as interconnected in the previous chapter regarding Facebook was only the surface of technological advancement. One fundamental component of the immense network of information is due to devices enabling the accessibility, efficiency and connectivity, so-called Internet-of-Things.[253]

IoT is the implication of concrete objects, people, or devices that can be connected with information systems in online or digital environment. Such objects are, for instance; smartphones, tablets, computers, vehicles, refrigerators, cameras, wearable health tracking devices, and machines that are able to communicate initiated for business use.[254] It is estimated that approximately 50,000 billion objects on earth currently can be programmed to the concept of IoT. The technical explanation of IoT is complex, however the architecture is based on a system of radio frequency sensors facilitating the tracking, identifying and locating of assets as in Bluetooth for instance. Further, new technology introduces mobile tracking features via Wi-Fi.

---

[251] See the case of *Jose Palomino et al. v. Facebook Inc*, United States Court Northern District of California, Order Granting Motion to Dismiss with Prejudice.

[252] Spion Report, *From Social Media Service to Advertising Network: A Critical Analysis of Facebook's Revised Policies and Terms,* 2015.

[253] [Hereinafter: IoT].

[254] U.S. Department of Commerce, National Telecommunications & Information Administration, *In the Matter of the Benefits, Challanges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, Comments of the Staff of the Federal Trade Commission's Bureau of Consumer Protection and Office of Policy Planning, June 2, 2016 [hereinafter: U.S. DoC, *In the Matter of the Benefits, Challanges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, 2016], p. 4.

Advertising technology companies have recently enabled the connection of online sensors to track offline behavior.[255]

The benefits for individuals as consumers of IoT implicate fast interaction in daily life, personalized and electronic health control, controlling of energy usage, navigation services when utilizing vehicles, and facilitates extensive research to be collected entailing the data from these IoT's in order to improve consumers' living standards and respond to behavior and demands in the commercial sector.[256] Further, IoT improves management of assets and optimizes supply chains as effective outcomes for individuals and companies. IoT reduces human interaction in the commercial sector, but also entail more environment friendly solutions.[257]

IoT implies risks to the protection of data privacy. IoT raises privacy concerns regarding the collection of sensitive personal data such as financial records, precise location data of individuals, and health records such as physical and mental conditions. Not only is the collecting of sensitive data critical. In terms of location data, IoT services such as beacons or Wi-Fi have started to collect more precise coordinates of an individual's device by tracking "device ID". The tracking of device ID is lawful in the U.S. however subject to different sectorial laws, but prohibited pursuant to article four point one in the GDPR.[258]

Further risks of IoT imply the lack of control over personal information in the interconnected system that smartphones, vehicles, health tracking devices and machines operates in. There is a risk for personal data to end up with unauthorized service providers with commercial incentives where consent has not been given.[259] For instance, an individual who uses location services in a car could be subject to have his or her driving behavior monitored unknowingly by an insurance company, impacting decision-making procedures for how to establish insurance rates. At the same time the location can be obtained by data processing companies who distribute

---

[255] Weber, Rolf H., and Weber, Romana, *Internet of Things; Legal Perspectives,* SpringerLink ebooks, Berlin, Zürich, Schulthness, March 21, 2011, p. 2 (there are countless different methods for setting up such tracking, identifying and locating assets, see pp. 2-9).

[256] U.S. Department of Commerce, National Telecommunications & Information Administration, *In the Matter of the Benefits, Challanges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, Comments of the Staff of the Federal Trade Commission's Bureau of Consumer Protection and Office of Policy Planning, June 2, 2016 [hereinafter U.S. DoC, *In the Matter of the Benefits, Challanges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, 2016], p. 4.

[257] Commission of the European Communities, Commission Staff Working Document *Accompanying the Document to the Communication from the Commission to the European Parliament, the Council, the European Economi and Social Committee and the Committee of the Regions*, *Future Networks and the Internet, Early Challenges regarding the "Internet of Things"*, Brussels [hereinafter: European Commission Staff Working Document, *Future Networks and the Internet, Early Challenges regarding the "Internet of Things"*], p. 5.

[258] U.S. DoC, *In the Matter of the Benefits, Challanges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, 2016, pp. 6-7.

[259] *Ibid.*

the collected data to advertisement companies, creating the ability to see where and when a potential customer is close to the nearest store without the consent or conscious of the individual.[260]

Even though these companies and their services could benefit individuals in a commercial perspective, and consent must be opted-in in apps when connecting to Wi-Fi, it is rather an issue of non-control over the personal data and the unawareness of the consequences when staying connected. An individual must have the chance to consent and control what commercial perceptions he or she receives. Further on, the risk of having whole systems unauthorized disclosed entailing financial records, fitbits,[261] and security systems at home could be at stake if there is no rigorous system protecting data privacy. [262]

Regulating IoT solutions is currently a global challenge. The transnational characteristics of IoT and data flows imply difficulty for domestic regulative approaches to successfully address the risks and threats to data privacy in the EU and the U.S. Successful approaches to regulate IoT are self-regulation and international frameworks, according to IoT experts Rolf and Ramona Weber.[263]

EU and U.S. institutions and legislators have undertaken extensive research regarding the most appropriate approach to regulate IoT. Thus, EU and U.S. institutions differ in terms of which regulatory approach is most appropriate. The European Commission, with support from research and opinions from public institutions as well as consumer protection organizations, argues for public regulative approaches and institutional control over data privacy concerns and enforcement mechanisms.[264] Though, the American Chamber of Commerce[265] took the standpoint in 2008 that the stakeholders' opinions were "*premature*".[266] AmCham argued that it was too early to conclude any consequences of IoT to potentially effect individuals and profiling of consumers, and that a neutral technological approach would be too rushed to

[260] U.S. DoC, *In the Matter of the Benefits, Challanges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, 2016, pp. 6-7.
[261] Health records in information technology systems.
[262] Aleks Krotoski, *The Power of Privacy – Documentary Film,* The Guardian, publ. January 28, 2016.
[263] See European Commission Staff Working Document, *Future Networks and the Internet, Early Challenges regarding the "Internet of Things"*, p. 5; compare to: Weber, Rolf H., and Weber, Romana, *Internet of Things; Legal Perspectives,* SpringerLink ebooks, Berlin, Zürich, Schulthness, March 21, 2011, p. 23.
[264] See for instance; European Commission Staff Working Document, *Future Networks and the Internet, Early Challenges regarding the "Internet of Things";* and the standpoints of stakeholders such as the European Association for the Coordination of Consumer Representation in Standardization, the European Consumer's Organization BUEC in Weber, Rolf H., and Weber, Romana, *Internet of Things; Legal Perspectives,* SpringerLink ebooks, Berlin, Zürich, Schulthness, March 21, 2011, p. 34.
[265] [Hereinafter: AmCham EU].
[266] See European Commission Staff Working Document, *Future Networks and the Internet, Early Challenges regarding the "Internet of Things"*, p. 35.

consider.[267] With that said, it can be argued that the privacy consequences are evident factors and unavoidable at this point.

EU and U.S. commercial data actors present varying aspects on how to regulate IoT; by public institutional means, or by letting the private sector initiate self-regulative compliance methods.[268] Self-regulation is considered "soft law" and apprehends the normative social behavior based on a tacit agreement between interacting operators. Self-regulation requires the intent to operate in a certain manner, and incompliance initiates social and reputational sanctions, rather than law enforcement measures. Self-regulation is the typical element in corporate codes of conduct worldwide. Problematically, self-regulation requires existing intent to comply fully and does not provide efficient law enforcement measurements if not specifically agreed, normally in contracts.[269] In order to ensure a rigorous protective level, public authorities and the impact of legislative powers seems unavoidable. Thus, a crucial strength of self-regulation is the realistic need and reflection of the specific business sector affected, which can adjust innovation and data privacy with flexibility[270]; an approach that has similarities with the U.S. legal status of data privacy protection.[271]

Another point for discussion has been the implementing of international institutions to safeguard the protection of data privacy globally.[272] This approach is taken in the transatlantic agreement for the Privacy Shield; a concept that has met resistance and been challenged by dominant corporate interests. Further, it confronts the democratic power of all countries involved, a factor that has been controversial in stakeholder consultations.[273]

7.3 Organizational Solutions for Sustainable Innovation

Key factors that have been argued essential for data privacy protection established in earlier conclusions in this thesis have high lightened control over one's personal data, more transparency in the processing practices, and more safeguarding obligations on commercial data and communication service providers.[274] The first key element is consent and how to prove unambiguous consent in data and communication services. In EU privacy

[267] See European Commission Staff Working Document, *Future Networks and the Internet, Early Challenges regarding the "Internet of Things"*, p. 35.
[268] *Ibid*. pp. 34-36.
[269] However, the European Commission set forward regulations on Binding Corporate Rules (BCR) for companies; see for instance http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm, accessed by April 13, 2017.
[270] Weber, Rolf H., and Weber, Romana, *Internet of Things; Legal Perspectives,* SpringerLink ebooks, Berlin, Zürich, Schulthness, March 21, 2011, pp. 24-25.
[271] See chapter 5.4.
[272] *Ibid.* p. 27-32.
[273] Compare to chapter 5.
[274] See chapter 5 (for comprised explanations, see "concluding notes" in chapter 5.3.5 and 5.4.4).

laws, it has been fundamentally stressed that active consent is an evident component in successfully addressing data privacy matters.[275] In U.S. privacy laws, consent and control have similarly developed extensively but through a sectorial approach, but recently countered a set back in the communications sector on federal level.[276]

Institutional measurements such as regulations, law enforcement, and the Privacy Shield can create national or interstate guidance for sustainable systems for protecting data privacy. However, as can be seen in the history of the American Constitution[277], the EU declarations and charters[278], and in the case of *Mr. Schrems v. the Irish Data Commissioner*[279], the attitude towards government practices and international frameworks has not always created successful outcomes or trust among corporate interests and individuals.[280]

Stuart Lacey, privacy expert, argues that we are facing more solutions based on a shared-economy concept[281], for instance solutions as Uber and AirBnB. These structures imply the interacting on an individual basis, requiring sustainable frameworks and systems on corporate and individual level. Simultaneously, individuals need technological knowledge and easier understanding on a daily basis. [282]

In order to find data privacy solutions benefiting the society today and in the future, all stakeholders' interests affected by data privacy protection must be brought to attention. Importantly, corporate solutions developed to provide data services or electronic communications including processing, monitoring, transmitting and storing personal data must be evaluated, impacting both the EU and the U.S. businesses and consumers. FTC Chairwoman Edith Ramirez explains that we are currently just "*scratching the surface of technological advancement*".[283] She further argues that if we want to ensure progress in solutions benefiting innovation and privacy, we must build policies that are influenced by innovation and research break-through. By looking at practical, realistic examples of what technology we

[275] Compare to chapter 5.3.3.
[276] Compare to chapter 5.4.3.
[277] See chapter 5.4.1.
[278] See chapter 5.3.1.
[279] See chapter 6.2.
[280] Compare to chapters 5.4.1 and 6.
[281] The definition of a "shared economy" is, for example, when an individual rents or borrows assets owned by someone else. This means that individuals are interacting with each other commercially on a peer-to-peer basis, where companies not necessarily are involved directly. For more information; see European Commission, Codagnone, Christiano, and Martins, Bertin, JRC Technical Reports, Institutes for Prospective Technological Studies Digital Economy Working Paper 2016/01, *Scoping the Sharing Economy: Origins, Definitions, Impact and Regulatory Issues,* 2016.
[282] Stuart Lacey, *The Future of Your Personal Data – Privacy v. Monetization*, TED-talks, Bermuda, publ. December 20, 2015 (March 23, 2017, approx. 11.00 minutes).
[283] Federal Trade Commission, PrivacyCon, Part 1 – *The Current State of Online Privacy*, 2016 Workshops, Video Conference (Edith Ramirez, minutes 15 – 25), January 14, 2016 (March 31, 2017).

see today and likely in the future, we can attempt to identify the technical flaws and how they threat data privacy. [284]

Companies that process, transmit, monitor and/ or store personal data should be able to understand when, what and where to manage personal data, and this by undertaking privacy risk management strategies. According to privacy lawyers, consideration must be taken to (1) adoption of detailed data processing records, (2) implementation of security measures, (3) privacy impacts assessments, (4) "privacy-by-design" and "privacy-by-default", (5) and appointment of Data Privacy Counsels in organizations.[285] Privacy law experts further advice companies to prepare Q&A for consumers, stakeholders and company partnerships, and become aware of what possible flaws the organization has if it would be subject to legal claims or enforcement measurements.[286]

Companies must ask themselves how they can obtain active consent from consumers and end-users. Other factors also associated with the individual's control of personal data are *"*the right to be forgotten*"*[287] and the data service providers' "obligation to report*"*.[288] According to marketing experts, the right incentives to develop better solutions for consumers as well as protecting their data privacy starts with the internal organization. Companies must adapt ecosystem-thinking models and create a brand that consumers trust. Further, the key successor to challenge companies such as Facebook is to provide data that is as precise and accurate as possible.[289] Thus, implementing better privacy protection for users or consumers.

7.4 Technological Solutions for Sustainable Innovation

New technology is introduced daily, shaping individuals lives fundamentally with more narrow and accurate data that explains how we behave on a daily basis. It has been presented how companies in dominant positions have exploited their position. Thus, it should also be stressed that new innovators on the market build their business models fundamentally around privacy strategies, respecting U.S. and EU laws, transatlantic agreements, and corporate policy-making and best practices. Below are

[284] Federal Trade Commission, PrivacyCon, Part 1 – *The Current State of Online Privacy*, 2016 Workshops, Video Conference (Edith Ramirez, minutes 15 – 25), January 14, 2016 (March 31, 2017).
[285] Phil Lee and Mark Weber, *The New EU General Data Protection Regulation Under 60 minutes!*, FieldFisher LLP (UK), January 31, 2016 (29 minutes); compare to *Network Advertising Initiative (NAI)* Yearly Summit 2017, Panel discussion by Mike Hintze, Estelle Werth, Oliver Gray, Matthias Mattheisen, Sheila Millar, Current at Pier 59, Chelsea Piers in New York City, May 17 2017.
[286] *Network Advertising Initiative (NAI)* Yearly Summit 2017, Panel discussion by Mike Hintze, Estelle Werth, Oliver Gray, Matthias Mattheisen, Sheila Millar, Current at Pier 59, Chelsea Piers in New York City, May 17 2017.
[287] See article 17 GDPR.
[288] See article 19 GDPR.
[289] Event Panel Discussion, Nielsen Inc., "*The Future of Identity*", May 10 2017.

standpoints from IT experts and what possible solutions there are for creating sustainable data privacy solutions, technically.

7.4.1 Plurality of Services and Products

According to Bruce Schneier, data security expert, and Edward Snowden, former CIA employee, it is crucial to evaluate the technical infrastructure and investigate where data systems are lacking protection of data privacy. Further, how data services meet ethical and moral grounds, and the greater perspective of data protection as an ideal.[290] Even though these experts are merely focusing on data security and system breaches, it highlights the problem of interconnectedness complexity of current data systems. As individuals utilize the same devices and systems for several different purposes; such as payment methods, storing of medical records, and location services, it is evident that individuals can stay in control over their personal information for the right and intended purposes.

Schneier and Snowden further argue that encryption could imply safer technology solutions and therefore increased protection level of data privacy. By creating different systems with different personal information provided, collected, monitored, transmitted or stored, individuals could keep their personal information under control and limited to a certain purpose.[291] This also aligns with Professor Monica Lam at Stanford University, arguing that privacy could be better safeguarded in an "open-source-system" regarding IoT. This open-source-system would imply that if the IT market would increase the market players, as in competitors, there would be no specific giant owners of different systems and solutions, such as Facebook. According to Prof. Lam, plurality of services and companies would increase the possibility to better protect data privacy in an eco-system structure, but also prospering of innovation and competition.[292]

7.4.2 Innovation Built on Privacy

Speaking on an academic lecture on behalf of the European Commission, EU Commissioner Margerethe Vestager mentioned that "privacy-by-design" and "compliance-by-design" are appropriate and forthcoming solutions on EU institutional regulative level.[293] As can be studied in the new GDPR, there are provisions encouraging companies to implement pseudonymisation.[294] Further, the U.S. authority FTC has taken further

[290] Bruce Schneier and Edward Snowden, *Harvard Data Privacy Symposium 1//23/15*, Webinar, Harvard Institute for Applied Computational Science, publ. January 23, 2015.
[291] *Ibid.*
[292] Professor Monica Lam, Webinar, *Maintaining Privacy in the Internet of Things*, Stanford University Alumni, publ. March 29, 2016.
[293] European Commissioner Margrethe Vestager, UPF Lecture, The Association of Foreign Affairs Lund at Akademiska Föreningen Lund, March 13, 2017.
[294] See European Commission Staff Working Document, *Future Networks and the Internet, Early Challenges regarding the "Internet of Things"*, p. 8.

measurements to ensure that companies develop systems and data services ensuring "privacy-by-design".[295]

The EU has undertaken studies regarding *Privacy-Enhancing Technologies*[296], implying technical solutions for data systems that have been developed in order to particularly consider and respect data privacy of individuals. Data minimization and encryption tools have particularly been emphasized in order to best safeguard data privacy concerns. Deployment is determined based on a cost-effective-model, and the demand from customers for such technologies. The consumer perspective is crucially impacting the development for new technologies adjusted to protect our data privacy, and according to research, the consumer awareness is indicating that individuals and pro-privacy organizations se an increasing need for such solutions.[297]

7.4.3 Consumer Awareness

Awareness among individuals is an increasing factor incentivizing commercial data companies to engage in technologies safeguarding data privacy. Stakeholder consultations in the EU and the U.S. have presented that individuals demand necessary data privacy measurements from corporate interests to ensure the right to privacy.[298]

Stakeholder consultations have further indicated that companies deploying solutions adjusted to high level of data privacy protection see a tendency among customers to refuse paying for their own data privacy. Furthermore, that the refusal to pay for privacy solutions implies an obstacle for companies to further deploy better data privacy protected solutions.[299] Surveys demonstrate that the cost of reputational degrading and negative stock market impacts on IT companies' failing to handle data losses and privacy concerns, have relatively low impact on individuals. To develop more sustainable data privacy protection, companies must be able to create services and products that consumers can afford. The implementation of solutions safeguarding data privacy must be rewarded in the EU and U.S. legal system in order to accomplish so. Further, consumers must be better informed in order to impact corporate failure to manage data privacy according to data privacy laws. Current data privacy laws in the EU and the U.S. are practically impossible to understand for individuals without being an expert on the area, due to its extensive amount of principles and text codes and lack of clarity. By simplifying the current basic values and

[295] S. 547, 114th Congress (Jan 2015 – 2016), Commercial Privacy Bill of Rights Act of 2015, Section 13.
[296] [Hereinafter: PETs].
[297] London Economics, *Study on the Economic Benefits of Privacy-Enhancing Technologies (PETs),* A Final Report to the European Commission, DG Justice, Freedom and Security, publ. July 2010, p. 11.
[298] See chapters 5.4 and 5.5.
[299] London Economics, *Study on the Economic Benefits of Privacy-Enhancing Technologies (PETs),* A Final Report to the European Commission, DG Justice, Freedom and Security, publ. July 2010, p. 11.

contexts behind regulations in amount and clarity, and imposing more responsibility on individuals to make sure that their personal data is being handled, individuals could be better aware of what necessary functions data services and products should offer in order to protect their data privacy. [300]

7.5 Concluding Notes

The regulative dilemma for new innovation and resilience to data privacy protection is evident. Existing privacy regulations are only capturing the surface of the development in technology on a global scale. In order to reach the data processing practices and make them more sustainable, compliance and incentives to protect data privacy of individuals must derive from data service providers, processors and controllers, and other similar commercial actors handling data.

Facebook as the world's leading social networking service has demonstrated its ignorance to take necessary steps to comply and lead by example for a sustainable data privacy protection. The company has world-leading advanced technology. Yet, the company has been subject to several allegations and class actions in the EU and the U.S., indicating that the current data privacy frameworks in the EU and the U.S. are not efficient towards Facebook. The question remains how Facebook could be forced to change its practices.

IoT is increasingly facilitating interconnection and efficiency for companies as well as individuals worldwide. IoT is a relatively new phenomenon and the regulative aspect is still under development. As has been presented, IoT benefit our daily lives, but will also imply risks to individuals' data privacy. The risks are; the immense amount and infrastructure of personal data, the threat to the individual control over personal data, and the unsolicited disclosure of personal data to third parties without consent.

As has been concluded from previous chapters, sustainable data privacy protection must be initiated and enforced on corporate and individual level. If solutions such as Facebook and IoT would be entirely regulated by soft law and private incentives, it would result in more adjusted solutions benefiting both innovation and data privacy protection. Thus, self-regulation requires corporate intent to comply and hold the level sustainable, and Facebook has been an example of where corporate dominance has exploited its position and power.

In terms of the possibility to strengthen international institutionalism, it has been concluded that international frameworks merely serve as guidance, and

[300] London Economics, *Study on the Economic Benefits of Privacy-Enhancing Technologies (PETs),* A Final Report to the European Commission, DG Justice, Freedom and Security, publ. July 2010, p. 10.

the Privacy Shield is an example of how much power corporate interests have on transnational policy-making.[301]

To develop technical solutions and business models addressing data privacy concerns factors, companies must get the right incentives to do so; sustainability is not just compliance with EU law or sectorial laws in the U.S., but the will to be coherent with consumers' standpoints and see deeper into the underlying values of data privacy transnationally. Additionally, commercial actors must start demanding each other's compliance to sustainable data services. Data processing often involve several companies and third parties, and each step in the process should be able to confirm transparent compliance and honoring safe data practices towards consumers and end-users. By providing such information, the liability for each data processor can also be better balanced.

In order to engage more commercial actors in the IT environment, the regulators in the EU and U.S. should focus on innovative collaboration. Companies that conduct businesses benefiting data privacy should be rewarded on the transnational market. With the right incentives, companies would be able to contribute to individuals retaining their control over their personal data, also benefiting the social values behind data privacy in society as a whole.

[301] See chapter 6.

8 Concluding Remarks

The purpose of this thesis is to answer the research question; *how data privacy protection can be more sustainable in commercial data processing practices*. The question captures what social, legal and technical factors that must be taken into account for developing more sustainability in commercial data processing of personally attributed data. Further, how commercial sustainability impact businesses in technical terms engaging in processing, monitoring, transmitting and storing of personal data/ PII. The question is addressed to the relationship between the EU and U.S. as two of the most IT developed economies in the world.

As for what social, legal, and technical factors that must be taken into account, this thesis has presented three blocks of perspectives in order to comprehend the critical factors for developing sustainable commercial data protection practices. These three blocks are (1) the philosophical viewpoint of privacy and data privacy, and the approach of sustainability, (2) the legal protection of data privacy within and between the EU and U.S., and (3) the technical implication of data privacy in current developing commercial data solutions.

The three-part taxonomy presents a theory of how these three blocks can lead to more sustainable data protection practices, but also emphasizes the core challenges to protect data privacy today. Data privacy is threatened since underlying social values of privacy have changed. This has lead to dominant positions for large corporations impacting the ethics and morals of data privacy, gaining a privileged position in lobbying aspects. The legal frameworks provided in the EU and U.S. are not protecting data privacy fully; it implies a patchwork of regulations that companies would avoid rather than be incentivized to comply with, uncertainty on transnational level, and complex to overview. Further, the innovation of today is far ahead of the regulative measurements, resulting in legal as well as ethical grey zones for where the protective level should be.

The social factors of sustainable data practices are the following. Data privacy is the concept of privacy in the digital environment. Personally attributed data has become the new value in digital commercial contexts for lucrative businesses, and individuals build their lives around data solutions. Core elements of the term data privacy encompass personal data/ PII, and the quality level of data transfers. There are several theories that have influenced the term data privacy historically; control-over-information, limited access to one's personal life, privacy as clustered to other rights, an economic perspective on privacy, and privacy as the moral capital to personhood, intimacy and integrity. In order to protect privacy most successfully in the data environment, the "control over information" concept, complemented with "privacy as an economic interest", should be best suited.

In order to implement a sustainable perspective of protecting data privacy, data privacy must be comprehended as an ultimate value and fundamental human right that should be perceived as a ground stone when forming laws and undertaking law enforcement measurements. Even though other interests should be fairly balanced to the protection of data privacy, the society must strengthen the understanding of privacy in order to develop better sustainable commercial practices and compliance of data privacy regulations. Individuals must take control and ownership of their personal information. This by consenting to how data practices will be undertaken.

The legal factors for sustainable data practices are the following. It has been argued that international frameworks merely serve as guidelines and are nearly impossible to implement sufficiently in an efficient and practical manner on corporate level. In EU laws, data privacy is on the forefront in level of protection in the world. However, the European Commission has difficulty balancing the power of corporate interests and the individual standpoints. Prerequisites for compliance are challenging the protected level. However, the EU is currently undertaking regulative measurements in the right direction for stronger data privacy protection, such as strengthening "the right to be forgotten", extended obligations on third party data processors, and pseudynomisation.

The U.S. regulations on data privacy are divided into federal and State laws, but also sectorial laws depending on branch and business practice. The sector-based structure implies a patchwork of regulations that initiate loopholes and overlapping regulations. Similarly to the EU laws, large companies have challenged the validity of U.S. data privacy laws fundamentally and recent political events have further challenged a sustainable future of data privacy practices in the U.S. Thus, the U.S. approach has flexibility to better regulate specific business sectors with the expertise to see specific needs. However, current political influences challenges advancing privacy regulative measurements, and the U.S. authorities, policy-makers and corporations would benefit from more inter-sector collaboration.

The EU and the U.S. have developed a transnational agreement, the EU-U.S. Privacy Shield. The partnership is initiated to better harmonize the transatlantic data flows in order to safeguard the level of protection of individuals. The agreement set forward efficient dispute settlement procedures and institutionalized powers to safeguard extra-territory data flows. Thus, the agreement has been countered by governmental as well as corporate powers from the beginning. The Privacy Shield illustrates the difficulty to implement transnational powers and the skepticism for overstepping national legislative power.

The EU and the U.S. lack efficient, clear, sufficient and practical incentives and implementation for more sustainable practices and compliance on corporate and individual level. However, national laws and law enforcement powers are necessary to set visions and guidance. Thus, in order to fully

develop sustainable data protection practices and compliance strategies, the measures must be taken on innovative and individual level among companies and individuals.

The technical implication of sustainable data practices is the following. In order to narrowly investigate how current IT solutions challenge sustainability in data privacy protection; corporate aspects have been analyzed. It has been presented that each business must evaluate and undertake a data privacy strategy for how to manage personal data, and to find incentives for sustainable compliance and start internally in the organization. To exemplify individuals demand for social networking and connectivity, Facebook Inc. has been evaluated. To exemplify physical connectivity and interconnectedness, IoT has been analyzed.

Facebook demonstrates lacking practical incentives to comply with both EU and U.S. data privacy laws, and has challenged the current transatlantic framework of collaboration. In terms of IoT, there are risks for individuals and their control over personal data and the infrastructure of data. The study of Facebook as well as IoT indicates that third party involvement is the critical factor undermining individuals' control and consent. As a possible approach to regulate better compliance by Facebook, and future development of IoT practices, self-regulation has been analyzed.

Facebook is an example of how a powerful market player has the ability and the capacity to set new data privacy standards and lead by example, but shows ignorance to take such role. Self-regulation requires full intent to develop sustainable data privacy practices and compliance accordingly. Facebook has proved how self-regulation is not a sufficient solution. With that said, it is possible to handle Facebook differently by posing more measurements from EU and U.S. authorities to force the company to comply. The demand for more control over personal data from consumers could also force Facebook to improve compliance, and the EU and U.S. should therefore let pro-privacy organizations and individual standpoints receive more influence on the future development on law and policy-making transnationally. Consumer awareness could therefore also be a "final measurement" to force Facebook to comply in a sustainable manner in the future.

The phenomenon IoT is an increasing technical solution enabling society to get even more connected, and has been discussed in the light of self-regulation as well as international approaches. IT experts have argued that encryption, more competitors and consumer awareness could benefit improved data privacy protection, and could therefore incentivize new innovation to fundamentally build their business models based on data privacy protection. To be successful as an innovator, the EU and U.S. must further develop innovative collaboration promoting and rewarding businesses taking steps towards sustainable solutions consumers can afford, focusing more on the quality and level of protection, rather than economical and short-term outcomes.

The chapter of IoT in this thesis depict how new technology is countered on the transnational commercial market. Compared to Facebook, it is evident that new services and innovators are more aware of privacy laws, and are able to engage in more sustainable innovation and be new technical leaders on the transnational market, benefiting data privacy as a social value benefiting society as a whole. Data privacy regulations will always be behind technical innovation, and regulatory measurements require evidence of what actual consequences potential issues can raise before successfully address such issues. By applying theories of sustainability, and creating incentives for commercial actors to respect and honor data privacy laws and policies, the gap between regulatory scope and technical innovation can decrease in a sustainable manner, benefiting individuals and commercial actors today as well as in the future.

***

Bibliography

International Conventions

The European Convention on Human Rights of 1950.

The International Covenant on Civil and Political Rights of 1966.

The International Covenant on Economic, Social and Cultural Rights of 1966.

The Universal Declaration on Human Rights of 1948.

United Nations General Assembly, *68/167 The Right to Privacy in the Digital Age*, resolution adopted by the General Assembly on 18 December 2013 (on the report of the Third Committee, A/68/456/Add.2).

United Nations website, General Assembly of the United Nations, *Sustainable Development: Background*, available at: http://www.un.org/en/ga/president/65/issues/sustdev.shtml, accessed by February 22 2017.

EU Law and Institutional References

Article 29 Working Party, *Opinion 12/2011 on the Definition of Consent, Adopted on 13 July, 2011,* 01197/11/EN, WP187.

Commission of the European Communities, Commission Staff Working Document, *Accompanying the Document to the Communication from the Commission to the European Parliament, the Council, the European Economi and Social Committee and the Committee of the Regions*, *Future Networks and the Internet, Early Challenges regarding the "Internet of Things"*, Brussels.

Court of Justice of the European Union, Press Release No 117/15, The Court of Justice Declares that the Commission's US Safe Harbour Decision is Invalid, Judgement Case C-362/14: Maximillian Schrems v Data Protection Commissioner, Press and Information, October 6 2015.

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).

Directive 95/46/EC of the European Parliament and 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.

European Commission, Codagnone, Christiano, and Martins, Bertin, JRC Technical Reports, Institutes for Prospective Technological Studies Digital Economy Working Paper 2016/01, *Scoping the Sharing Economy: Origins, Definitions, Impact and Regulatory Issues,* 2016.

European Commission, *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*, November 4 2010, Brussels.

European Commission Decision 2000/520/EC Commission Decision 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 (notified under document number C (2000) 2441) (Text with EEA relevance), Official Journal L 215 , 25/08/2000 P. 0007 – 0047.

European Commission, Justice, *Protection of Personal Data in the European Union*, Fact Sheet, Directorate-General for Justice, BE- 1049, November 2010, Brussels.

European Commission, Official Website, Justice: Building a[sic!] European Area of Justice, *EU Charter of Fundamental Rights*, available at: http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm (accessed by February 28 2017.

European Commission, Online Fact Sheet, *Overview on Binding Corporate Rules*, http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm, accessed by April 13 2017.

European Commission, Online Report, Growth: Internal Market, Industry, Entrepreneurship and SMEs, *The Importance of the Digital Economy*, available at https://ec.europa.eu/growth/sectors/digital-economy/importance_en, accessed by March 19 2017.

European Commission, Press Release, *Agreement on Commission's EU Data Protection Reform will Boost Digital Single Market*, Brussels, 15 December, 2015, available at http://europa.eu/rapid/press-release_IP-15-6321_en.htm, accessed by March 19, 2017.

European Commission, Press Release, *Commission proposes a comprehensive reform on data protection rules to increase users' control of their data and to cut costs of businesses*, 25 January, Brussels.

European Commission, *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing the Directive 2000/58/EC (Regulation on Privacy and Electronic*

Communications), COM(2017) 10 final, 2017/0003 (COD), Brussels, January 10 2017.

European Commission, Report, *Flash Eurobarometer 443 e-Privacy*, Fieldwork July 2016, publ. December 2016, TNS Political and Social, Survey Requested by the European Commission, Directorate-General for Communications Networks, Content & Technology (DG Connect), Project No. 2016.7036.

European Commission, Report, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union,* Conducted by TNS Opinion & Social at the request of Directorate-General Justice, Information Society & Media and Joint Research Centre, Survey Coordinated by Directorate-General Communication, Brussels, Fieldwork: November December 2010, Publication: June 2011.

European Commission, Staff Working Paper, Impact Assessment – Accompanying the Document, *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)*, and, *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,* Brussels, January 25, 2012.

European Data Protection Supervisor, *Statement of the Article 29 Working Party*, Brussels, October 2015, available at: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf, accessed by March 29 2017.

European Parliament Report, *A Comparison Between US and EU Data Protection Legislation for Law Enforcement*, Policy Department C; Citizens' Rights and Constitutional Affairs, Directorate-General for International Policies, Study for the LIBE Committee. A Study by: Prof. Dr. Franziska Boehm, University of Münster, Institute for Information, Telecommunication and Media Law, Germany With the help of Markus Andrees, Jakob Beaucamp, Tim Hey, Robert Ortner, Giulia Priora and Felix Suwelack, 2015.

European Parliament Report, *The US Legal System on Data Protection in the Field of Law Enforcement: Safguards, Rights and Remedies for EU citizens*, Policy Department C,Directorate-General for International Policies, Study for the LIBE Committee. A Study by: Prof. Bignami, Francesca, George Washington University Law School, Washington, DC, USA, and Responsible Administrator Mr Davoli, Alessandro, 2015.

European Parliament Resolution of 25 Novsember 2009 on the Communication from the Commission to the European Parliament and the Council – *An Area of freedom, security and justice serving the citizen – Stockholm Programme, Multi-annual programme 2010- 2014 regarding the area of freedom, security and justice (Stockholm Programme)*, (P7_TA(2009)0090).

European Union Commissioner Margrethe Vestager, UPF Lecture in Akademiska Föreningens Borg, Lund University, February 18, 2017.

Regulation (EU) 216/679 of the European Parliament and of the Counsil of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

The Charter of Fundamental Rights of the European Union of 2000.

U.S. Law and References from Governmental Institutions

Before the Department of Commerce, National Telecommunications & Information Administration, *In the Matter of the Benefits, Challanges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, Docket No. 160331306-6306-01, Comments of the Staff of the Federal Trade Commission's Bureau of Consumer Protection and Office of Policy Planning, June 2 2016.

Federal Communications Commission, Washington D.C. 20554, Adopting Order, *in the matter of Verizon, Compliance with the Commission's Rules and Regulations Governing Customer Proprietary Network Information*, File No.: EB-TCD-13-00007027 Account No.: 201432170014 FRN: 0016304214, Adopted September 2 2014, Released September 3 2014.

Federal Communications Commission, Notice of Proposed Rulemaking, Before the Federal Communications Commission, Washington D.C. 20554, *in the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunication Services,* WC Docket No. 16-106, Adopted March 2016, Released April 1 2016 (Chairman Wheelers and others).

Federal Trade Commission, Before the Federal Communications Commission Washington D.C. 20554, *Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission*, in the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunicatoions Services, WC Docket No. 16-106, May 27 2016.

Federal Communications Commission, *Order in the Matter of AT&T Services, Inc*., before the Federal Commucnications Commission, File No.:

EB-TCD-14-00016243 Acct. No.: 201532170010 FRN: 0005193701, Adopted and released April 8 2015.

H.R.387 – Email Privacy Act, 115th Congress (2017-2018), available at https://www.congress.gov/bill/115th-congress/house-bill/387 (accessed by March 17 2017).

Justice Information Sharing, U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, *Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S. § 2510-22*, Information Table for Federal Statues, available at: https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285 (accessed by March 16 2017).

S. 547, 114th Congress (Jan 2015 – 2016), Commercial Privacy Bill of Rights Act of 2015, *A bill to establish a regulatory framework for the comprehensive protection of personal data for individuals under the aegis of the Federal Trade Commission, to amend the Children's Online Privacy Protection Act of 1998 to improve provisions relating to collection, use, and disclosure of personal information of children, and for other purposes*, Section 111 – 122.

The Communications Act of 1943.

The Computer Fraud and Abuse Act of 1986.

The Constitution of the United States of America of 1789.

The Electronic Communications Privacy Act of 1986.

The Federal Privacy Council, *Electronic Communications Privacy Act of 1986 (ECPA)*, Online Guidelines, available at https://www.fpc.gov/electronic-communications-privacy-act-of-1986-ecpa/, (accessed by March 15, 2017).

The Federal Trade Commission Act 15 U.S.C. of 1914.

The Federal Trade Commission, Online Guidance Report, *Privacy, Identity & Online Security, Consumer Information*, available at: https://www.consumer.ftc.gov/topics/privacy-identityonline-security (accessed by March 13 2017).

The Federal Trade Commission, Online Report, *Financial Institutions and Customer Information; Complying with the Safeguards Rule,* available at: https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying (accessed by March 13 2017).

The Federal Trade Commission, Online Guidance Report, *Gramm-Leach-Bliley Act,* available at: https://www.ftc.gov/tips-advice/business-

center/privacy-and-security/gramm-leach-bliley-act (accessed by March 13 2017).

Federal Trade Commission, PrivacyCon, Part 1 – *The Current State of Online Privacy*, 2016 Workshops, Video Conference, January 14, 2016, available at https://www.ftc.gov/news-events/audio-video/video/privacycon-part-1, accessed by March 31 2017.

The Federal Trade Commission, Protecting America's Consumers, Press Release, Companies that Own and Manage Payday Lending and Check Cashing Stores to Settle FTC Charges That They Tossed Sensitive Consumer Data into Trash Dumpsters, November 7 2012.

The Gramm-Leach-Bliley Act of 1999.

The White House, Office of the Press Secretary, *Executive Order: Enhancing Public Safety in the Interior of the United States*, section 14, January 25, 2017, available at https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united, accessed by March 20, 2017.

United States Courts, Press Release, *2nd Circuit Mounts Efforts to Build Civic Awareness*, publ. February 2, 2017, available at http://www.uscourts.gov/news/2017/02/02/2nd-circuit-mounts-effort-build-civics-awareness, accessed by March 19 2017.

United States Department of Commerce, Annex I, *EU-U.S. Privacy Shield Framework Principles*, The Under Secretary for International Trade, Washington D.C., 20230, Febrary 23 2016.

United States Department of Commerce, Online Report, *U.S. Secretary of Commerce Penny Pritzker Discusses Importance of Digital Economy at 2016 Hannover Messe Digital Transformation of Industry Conference*, April 25, 2016, available at https://www.commerce.gov/news/secretary-speeches/2016/04/us-secretary-commerce-penny-pritzker-discusses-importance-digital, accessed by March 19 2017.

Reports

A/HRC/27/37*, United Nations General Assembly, Human Rights Council: Twenty-seventh Session, Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General, *The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights*, GE. 14-08854 (E), *1408854*, 30 June 2014.

E.U. Network of Independent Experts in Fundamental Rights (CFR-CDF), *Report on the Situation of Fundamental Human Rights in the European Union and its Member States in 2002.*

Eurostat, Statistics Explained, *The EU in the World – Economy and Finance*, Data Extracted in March 2016, available at http://ec.europa.eu/eurostat/statistics-explained/index.php/The_EU_in_the_world_-_economy_and_finance, accessed by March 19 2017.

FTC Staff Report: *Self-Regulatory Principles For Online Behavioral Advertising*, Behavioral Advertising: Tracking, Targeting, & Technology, February 2009.

London Economics, *Study on the Economic Benefits of Privacy-Enhancing Technologies (PETs),* A Final Report to the European Commission, DG Justice, Freedom and Security, publ., July 2010.

Privacy International, Report, *Privacy International's Contribution to the EU Commission Consultation on the Review on the e-Privacy Directive 2002/58/EC*, July 2016.

OECD Council Recommendations, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980 (amended 2013).

OECD Guidelines on Data Protection, 1980, part two, *Basic Principles of National Application*, available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, accessed by February 27 2017.

Rosemary P. Jay, Hunton & Williams Report, *Data Protection and Privacy 2015; In 31 Jurisdictions worldwide*, publ., Gideon Reberton, Law Business Research 2015.

Spion Report by Van Alsenoy, Brendan, Verdooth, Valerie, Heyman, Rob, Ausloos, Jef and Wauters, Ellen, *From Social Media Service to Advertising Network: A Critical Analysis of Facebook's Revised Policies and Terms*, Interdisciplinary Centre for Law and ICT/Centre for Intellectual Property Rights (ICRI/CIR) of KU Leuven and the department of Studies on Media, Information and Telecommunication (SMIT) of the Vrije Universiteit Brussel (VUB), both departments part of iMinds, Draft February 23 2015.

The OECD Privacy Framework of 2013 (Revised version of the OECD Guidelines on Data Protection, 1980), available at: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (accessed by: February 27, 2017).

Office of the High Commissioner for Human Rights, CCPR General Comment No. 16: Article 17 (Right to Privacy), *The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, Adopted at the Thrirty-second Session of the Human Rights Committee, on 8 April 1988.

United Nations Conference on Trade and Development (UNCTAD), *Data Protection Regulations and International Data Flows: Implications for Trade and Development*, New York and Geneva, 2016.

Literature

Bogdan, Michael, *Komparativ rätt: Comparative Law*, publ., Juridiska föreningen, Lund 1978.

Bork, Robert H., *The Tempting of America: The Political Seduction of the Law*, publ., Simon and Schuster, 1990.

Bygrave, Lee Andrew, *Data Privacy law: An International Perspective,* publ., Oxford Scholarship Online, 2014.

Cabezas, Heriberto, and Diwekar, Urmila, *Sustainability; Multi-Disciplinary Perspectives*, publ., Bentham Science Publishers, September 14 2012.

Fidler, David P., *The Snowden Reader*, Bloomington, Contributor Ganguly, Sumit Indiana University Press, 2015.

Klosek, Jacqueline, *Data privacy in the Information Age*, publ., Greenwood Publishing Group, January 2000.

Kuner, Christopher, *Transborder Data Flows and Data Privacy Law*, publ., Oxford University Press, September 2013.

Nissenbaum, Helen Ray, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, publ., Stanford Law Books, November 2009.

Regan, Priscilla M., *Legislating Privacy*, publ., Chapel Hill, NC: University of North Carolina Press, 1995.

Retolaza, José Luis., San-José, Leire. and Ruíz-Roqueñi, Maite., *Social Accounting for Sustainability Monetizing the Social Value*, publ., SpringerBriefs in Business, 1st ed., 2016.

Solove, Daniel J., *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*, publ., Yale University Press, December 2007.

Solove, Daniel J., *Understanding Privacy*, publ., Harvard University Press, Cambridge Massachusetts, 2008.

Thomason, Sara Grey and Kaufman, Terrence, *Language Contact, Creolization, and Genetic Linguistics*, publ., University of California Press, 1988.

Vacca, John R., *Computer and Information Security Handbook (2*), publ., Kaufmann, Morgan, November 2012.

Weber, Rolf H., and Weber, Romana, *Internet of Things; Legal Perspectives,* SpringerLink ebooks, Berlin, Zürich, Schulthness, March 21, 2011.

Westin, Allan F., *Privacy and Freedom*, publ., Antheneum for the Assoc. of the Bar of the City of New York, 1967.

Academic Articles and Journals

DeCew, Judith, *Privacy*, Stanford Encyclopedia of Philosophy, First published Tuesday May 14, 2002; substantive revision Friday August 9, 2013, available at: https://plato.stanford.edu/entries/privacy/#Bib, accessed by January 26 2017.

Fried, Charles, *Privacy*, The Yale Law Journal, Vol. 77, No. 3, (Jan., 1968), publ., The Yale Law Journal Company Inc., pp. 475-493.

Gavison, Ruth, *Privacy and the Limits of Law*, The Yale Law Journal, Vol. 89, No 3, January 1980, publ., by The Yale Law Journal Company Inc., pp. 421 – 471.

MIT Technology Review, Zeichick, Alan, *How Facebook Works*, June 23, 2008, available at: https://www.technologyreview.com/s/410312/how-facebook-works/, accessed by April 5 2017.

Posner, Richard A., *The Economics of Privacy*, publ., The American Economic Review, Vol. 71, No. 2, Papers and Proceedings of the Ninety-Third Annual Meeting of the American Economic Association (May, 1981), pp. 405-409.

Reiman, Jeffrey, *Privacy, Intimacy and Personhood*, Philosophy and Public Affairs, Vol. 6, No. 1 (Autumn 1976), publ., Wiley, pp. 26-44.

Solove, Daniel J., *Conceptualizing Privacy*, California Law Review, Vol. 90, No. 4 (Jul., 2002), pp. 1087-1155.

Thomson, Judith Jarvis, *The Right to Privacy*, Philosophy and Public Affairs, Vol. 4, No 4 (Summer, 1975), publ., by Wiley, pp. 295 – 314.

Warren, Samuel and Brandeis, Louis, *The Right to Privacy,* Harvard Law Review, Vol. 4, No. 5, December 15, 1890.

Online Articles

Corporate Europe Observatory, Exposing the Power of Corporate Lobbying in the EU, Article, *Crowdsourced Lobby Exposé Shows Internet Giants have Footprints on our Data Privacy Laws,* February 18, 2013, available at: https://corporateeurope.org/lobbycracy/2013/02/crowdsourced-lobby-expos-shows-internet-giants-have-footprints-our-data-privacy, accessed by April 3 2017.

Jolly, Ieuan, Partner at Loeb & Loeb LLP, Practical Law: a Thomson Reuters Legal Solution, *Data Protection in the United States: overview*, Other Laws and Guidelines, available at: http://uk.practicallaw.com/6-502-0467#a596299, accessed by March 15 2017.

Kang, Cecilia, *Congress Moves to Overturn Obama-Era Online Privacy Rules*, The New York Times, March 28, 2017, available at https://www.nytimes.com/2017/03/28/technology/congress-votes-to-overturn-obama-era-online-privacy-rules.html?emc=edit_nn_20170329&nl=morning-briefing&nlid=76917530&te=1, accessed by March 29 2017.

Reuters Technology News, article by Fioretti, Julia, Facebook '*Tramples European Privacy Law': Belgian Watchdog*, Brussels, May 15 2015, accessed by April 5 2017.

Scott, Mark, The New York Times, *Facebook Gets Slap on the Wrist from 2 European Privacy Regulators*, May 16 2017.

Solove, Daniel J., Article, *Congress's Attempt to Repeal the FCC Internet Privacy Rules: The Void will be Filled*, Teach Privacy, April 2 2017.

Szoldra, Paul, Business Insider Article, Tech Insider, *This is Everything Edward Snowden Revealed in One Year of Unprecedented Top-secret Leaks*, September 16 2016.

The Privacy Advisor, Article by Meyer, James, Hamburg's DPA Aiming to Challenge Privacy Shield, August 4 2016.

The Telegraph, Article by Titcomb, James, Facebook Signs Up to Privacy Shield Data Treaty, October 15 2016.

Interviews, Webinars, and Conferences

Aleks Krotoski (edited Hough, Robin et al.), *The Power of Privacy – Documentary Film,* The Guardian, publ. January 28, 2016, available at: https://www.youtube.com/watch?v=KGX-c5BJNFk, accessed by April 7 2017.

Bruce Schneier and Edward Snowden, Webinar, *Harvard Data Privacy Symposium 1//23/15*, Webinar, Harvard Institute for Applied Computational Science, publ. January 23, 2015, available at: https://www.youtube.com/watch?v=7Ui3tLbzIgQ, accessed by April 11 2017.

European Commissioner Margrethe Vestager, UPF Lecture, The Association of Foreign Affairs Lund at Akademiska Föreningen Lund, March 13 2017.

Event Panel Discussion, Nielsen Inc., ”*The Future of Identity*”, May 10 2017.

Network Advertising Initiative (NAI) Yearly Summit 2017, Current at Pier 59, Chelsea Piers in New York City, May 17 2017.

Professor Monica Lam, Webinar, *Maintaining Privacy in the Internet of Things*, Stanford University Alumni, publ. March 29, 2016, available at: https://www.youtube.com/watch?v=EgLh25ZyMRA, accessed by April 11 2017.

Personal Enquiry/ Customer mail from Edler, Beatrice to the Privacy Team at Facebook, sent October 17 2016.

Phil Lee and Mark Weber, *The New EU General Data Protection Regulation Under 60 minutes!*, FieldFisher, January 31, 2016, available at: https://www.youtube.com/watch?v=NxgZ57BTkFQ, accessed by: February 11 2017.

Stuart Lacey, *The Future of Your Personal Data – Privacy v. Monetization*, TED-talks, Bermuda, publ. December 20 2015, available at https://www.youtube.com/watch?v=JIo-V0beaBw, accessed by March 23, 2017.

Statistics and Websites

Facebook Inc. Privacy Policy, available at: https://www.facebook.com/policy.php, accessed by April 5, 2017.

Privacy International, Explainers, *What is Privacy?*, available at: https://www.privacyinternational.org/node/54, accessed by April 6, 2017.

Statista, Statistic Report by Richter, Felix, *Lobbying Expenditure by U.S Tech Companies*, January 25, 2016, available at: https://www.statista.com/chart/4277/lobbying-expenditure-in-2015/, accessed by April 3 2017.

Dictionaries

Cambridge Dictionary, available at: http://dictionary.cambridge.org/dictionary/english/data, accessed by February 20 2017.

Table of Cases

EU Case Law

C-73/07, the case of *Tietosuojavaltuutettu* (Finnish Data Protection Ombudsman) *v. Satakunnan Markkinaporssi Oy and Satamedia Oy*, December 16, 2008, Judgment of the Court (Grand Chamber), reference for a preliminary ruling under Article 234 EC from the Korkein hallinto-oikeus (Finland), made by decision of 8 February 2007, received at the Court on 12 February 2007.

C-101/01, the case of *Lindquist,* November 11, 2003, Judgment of the Court, reference to the Court under article 234 EC by the Göta hovrätt (Sweden) for a preliminary ruling in the criminal proceedings before the court against Bodil Lindquist on, inter alia, the interpretation of the Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data (OJ 1995 L 281 p. 31).

C-131/12, the case of *Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzalez*, Judgement of the Court (Grand Chamber), 13 May, 2014, Request for a preliminary ruling under Article 234 TFEU from the Audiencia Nacional (Spain), made by decision of 27 February 2012, received at the Court on 9 March 2012.

C-362/14 in the Case of Maximillian Schrems v. Data Protection Commissioner, joined party Digital Rights Ireland Ltd, Judgment of the Court (Grand Chamber), October 6 2015.

C- 450/00, the case of *Commission of the European Communities* (applicant, represented by X. Lewis, acting as Agent) *v. Grand Duchy of Luxembourg* (represented by N. Mackel, acting as Agent), October 4 2001, Judgement of the Court (First Chamber).

C-518/07, the case of the *European Commission* (represented by C. Docksey, C. Ladenburger and H. Krämer, acting as Agents, with an address for service in Luxembourg), *supported by the European Data Protection* Supervisor (represented by H. Hijmans and A. Scirocco, acting as Agents, with an address for service in Luxembourg) *v. the Federal Republic of* Germany (represented by M. Lumma and J. Möller, acting as Agents, with an address for service in Luxembourg) Judgement of the Court (Grand Chamber), Decision March 9, 2010 (Action under Article 226 EC for failure to fulfil obligations, brought on 22 November 2007).

C-614/10, the case of the *European Commission* (represented by B. Martenczuk and B.-R. Killmann, acting as Agents, with an address for service in Luxembourg) *supported by the European Data Protection*

Supervisor (EDPS) (represented by H. Kranenborg, I. Chatelier and H. Hijmans, acting as agents) *v. The Republic of* Austria (represented by G. Hesse, acting as Agent, with an address for service in Luxembourg) *supported by the Federal Republic of Germany* (represented by T. Henze and J. Möller acting as agents) October 16 2012.

U.S. Case Law

Angel Fraley et al (Plaintiff)*., v. Facebook Inc.* (Defendant)*,* United States District Court Northern District of California, San Jose Division, Case No. 11-CV-01726-LHK (PSG), Facebook Inc.'s Reply in Support of Motion to Dismiss Second Amended Class Action Complaint, F.R.C.P. 12(b)(1), 12(b)(6), September 29 2011.

California v. Greenwood, 486 U.S. 35 (1988), No. 86-684, Argued January 11, 1988, Decided May 16, 1988, Certiorari to the Court of Appeal of California, Forth Appellate District.

Daniel Matera and Susan Rashkis, as individuals, and on behalf of other persons similarly situated v. Google Inc., United States District Court, Northern District of California, Case No. 5:15-cv-04062 LHK, Joint Declaration of Class Counsel in Support of Plaintiff's Motion for Preliminary Approval of Class Action Settlement, March 9, 2017, Judge: The Hon. Lucy H. Koh.

Estelle T. Griswold et al. (Appellants) v. State of Connecticut, 85 S.Ct. 1678, Supreme Court of the United States, No. 496, Argued March 29, 1965, Decided June 7 1965.

In Re Facebook Internet Tracking Litigation, United States District Court Northern District of California San Jose Division (Justice Edward J. Davila) Case No. 5:12-md-02314-EJD, Order Granting Defendants Motion to Dismiss, Re: Dkt. No. 44

Jose Palomino et al. (Plaintiffs) *v. Facebook Inc.* (Defendant), United States Court Northern District of California, Case No. 16-cv-04230-HSG, Order Granting Motion to Dismiss with Prejudice, Re: Dkt. No. 22.

Katz v. United States, 389 U.S. 347 (1967), U.S. Supreme Court, No. 35, Argued October 17 1967, Decided December 18 1967.

Matthew Campbell et al., (plaintiff) *v. Facebook Inc.* (defendent), United States District Court Northern District of California, Case No. 13-cv-5996-PJH, Order Granting in Part and Denying in part Motion for Class Certification.

Nimesh Patel et al. (Plaintiff) *v. Facebook Inc.* (Defendant), United States District Court Northern District Illinois, Eastern Division, Class Action,

Demand for Jury Trial, Class Action Complaint for Violations of the Illinois Biometric Information Privacy Act.

Olmstead v. United States, 277 U.S. 438 (1928), U.S. Supreme Court, Argued February 20, 21, 1928, decided June 4, 1928 (Brandeis, J., dissenting).

PLS Financial Services, Inc. et al., an Illinois corporation, PLS Group Inc., a Delaware corporation, and The Payday Loan Store of Illinois Inc., an Illinois corporation (Defendants) *v. United States of America* (Plaintiff), case No. 1:12-ev-8334, United States District Court Northern District of Illinois Eastern Division, Stipulated Final Judgment and Order of Civil Penalties, Permanent Injunction, and other Equitable Reliefs, October 26 2012.

Whalen v. Roe, 429 U.S. 589 (1977), No. 75-839, Argued October 13, 1976, Decided February 22, 1977, Appeal from the United States District Court for the Southern District of New York.