Privacy in Information Technology

by

Amin Rabinia, MA

A Thesis

In

Philosophy

Submitted to the Graduate Faculty
of Texas Tech University in
Partial Fulfillment of
the Requirements for
the Degree of

MASTER OF ARTS

Approved

Daniel O. Nathan, PhD
Chair of Committee

Howard Curzer, PhD

Mark Sheridan
Dean of the Graduate School

December, 2018

ACKNOWLEDGMENTS

A teacher will never know how far his or her influence will go to form a student's intellectual life. My appreciation for the presence of my teacher, mentor, and thesis advisor, Daniel Nathan, in my academic life cannot be expressed in words.

I am deeply grateful, fulfilled, and moved by the opportunities that I was provided with during my master's program. Particularly, I would like to thank Mark Webb, the Boss!, Howard Curzer, for co-reviewing this thesis, and also Joel Velasco and Joseph Gottlieb, for their intellectual and professional mentoring and support.

I also thank my PhD advisor in Computer Science program, Sepideh Ghanavati, for her understanding, accepting, and encouraging attitude towards my philosophical adventures.

TABLE OF CONTENTS

ACKNOWLEDGMENTS ..... **ii**

ABSTRACT ..... **v**

CHAPTER I **1**

INTRODUCTION **1**

Privacy as a Moral/Legal Concern 1

Privacy and its Challenges in IT 1

What We Learn from Theories of Privacy 2

CHAPTER II **3**

PRIVACY IN HISTORY **3**

Public vs. Private 3

Need for Privacy Law 5

Privacy Law in the US and Europe 5

CHAPTER III **8**

THEORIES OF PRIVACY **8**

Reductionist View 8

Coherentism 9

Theories of Privacy 10

Privacy as Control over Information 10
Human Dignity and Autonomy 13
Intimacy and Relationships 14
Reasonable Expectations and Contextual Integrity 16

CHAPTER IV **21**

PRIVACY AND INFORMATION TECHNOLOGY **21**

Personal Information and Data Privacy in IT 22

Internet and Social Media 22
E-Commerce and E-Government 23
Smartphones and Internet of Things 24
Big Data and Cloud Computing 24

Legal Provisions for Data Privacy Protection 25

CHAPTER V 29

LEGAL AND ETHICAL OBLIGATIONS TO PROTECT PRIVACY 29

CHAPTER VI 34

CASE STUDY: FACEBOOK'S PRIVACY SCANDAL.....34

CHAPTER VII.....39

CONCLUSION 39

BIBLIOGRAPHY.....41

ABSTRACT

In this thesis, we review the history, philosophical background, and legal status of privacy, in general, as well as in information technology. In our search for a viable, comprehensive, and applicable understanding of the notion of privacy, we survey, criticize, and analyze the existing theories of privacy in the philosophical writings and also legal provisions. Accordingly, we propose a theory of privacy, based on the theories of contextual integrity and individual's expectations, that can properly deal with the challenges of privacy raised by the concerns from information technologies. As a case study, we also apply our privacy theory on the privacy violation cases of Facebook.

CHAPTER I

INTRODUCTION

Why is privacy important to us? What is the impact of information technologies on our privacy? Is there any way to ensure the protection of our privacy in the digital age? In order to answer these questions, first, we need to know what privacy is. Second, we need to learn about the new technologies that might threaten our privacy. And finally, we need to search for and assess the possible measurements of privacy protection.

Privacy as a Moral/Legal Concern

For learning about the concept of privacy, there are two major directions of study: legal and ethical. In legal philosophy literature, privacy has been claimed to be a legal right that could either be based on other fundamental rights (e.g. property right or right to freedom) or be one of the basic human rights. From the ethical point of view, privacy is sometimes claimed to be a moral right that belongs to anyone as a person. Privacy as a moral right could be based on personhood, autonomy, or human dignity. In Chapter III, we look at different legal and moral theories that try to analyze and understand the notion of privacy.

Privacy and its Challenges in IT

New information technologies, despite all the opportunities that they have provided for people, have also drastically changed the dimensions of privacy concerns. Cambridge University researchers, for example, have shown that Facebook 'likes' can predict human personality types better than close family members.[i] After Cambridge Analytica scandal, manipulation of online clients by the data gathered from themselves should no longer sound surprising.[ii] The emerging dimensions of privacy concerns cannot be known without considering the new technological advances in our

study of privacy. Chapter IV, reviews the new concepts in IT (such as Big Data and Internet of Things) that have a huge influence on our data privacy.

What We Learn from Theories of Privacy

In this essay, besides philosophical theories of privacy we also look at the data privacy regulations (such as GDPR, OECD, and FIPP). We want to see how different theories of privacy are reflected in the regulations and how it is possible to improve our theoretical understanding and legal provisions of data privacy protection. Having such a comprehensive picture of privacy, or having a privacy paradigm, for IT will help: 1) legislators to provide the regulations with interpretative guidelines, 2) service providers to be proactive with respect to privacy protection measurements, and 3) individuals to make informed decisions about their data privacy.

For the purpose of determining such a paradigm, this essay is organized as follows. In the next Chapter, we start with the history of privacy in philosophical and legal writings. In Chapter III, we discuss theoretical stances for analysis of privacy right. Chapter IV, discusses a number of prominent contemporary legal and moral privacy theories that might cast light on our understanding of privacy. In Chapter V, we briefly review the technological sources of privacy concern in IT along with the relevant legal provisions. Then, in Chapter VI, we analyze the privacy theories, that we already discussed, in order to come up with a theory that is proficient to deal with the privacy concerns of IT. At the end (Ch. VII), we also look at the case of privacy scandal of Facebook to see how our proposed approach will help to understand and resolve the problem of data privacy protection.

---

[i] https://www.telegraph.co.uk/news/science/science-news/11340166/Facebook-knows-you-better-than-your-members-of-your-own-family.html

[ii] http://time.com/5197255/facebook-cambridge-analytica-donald-trump-ads-data/

CHAPTER II

PRIVACY IN HISTORY

In this Chapter, we look at the earliest discussions on privacy in the philosophical and legal writings. We also review the first regulations of privacy.

Public vs. Private

In the earliest relevant debates about privacy, the notion of privacy is never independent from the notion of publicity, and in general, the private is always understood with respect to the public. Maybe the first discussion of public vs. private goes back to Aristotle's *Politics*, where the domain of politics (i.e. public) is distinguished from the domestic realm (i.e. private). (DeCew, 2015, 73) For Aristotle, the public and private spheres are distinct realms of life; the domestic or private sphere is located within the home and family, and clearly separated from the public realm of government. (*ibid*, 84)

Regardless of whether a clear cut distinction between public and private is possible or even desirable, the social-political perspective for demarcating these two realms is followed in writings of other philosophers such as Locke, Mill, and Dewey. While the spheres of public and private for Aristotle are constant, for Locke there is a way to alter the belongings of the two. In *Second Treatise on Government*, Locke explains the distinction between public and private in terms of his labor theory and property right. In his view, what that distinguishes the two is the way that one possesses a property. A property can be separated from the public and become one's private possession if it is resulted from the "labour of his body and the work of his hands". (Locke, 1689, 27) In this view, everything at first belongs to the public, except individuals themselves. Since one's labor belongs only to him, whatever that he mixes with his labor becomes his property and thus excluded from the common resources. Therefore, the private, in Locke's view, is the realm created by individuals and their labor.

Mill speaks about public and private in terms of liberty and harm. For him individual liberty, which demands privacy, is necessary for prosperity of the public. In Mill's view, one's private actions should not be of interest for the public, in so far as they harm no person but himself. Public attention and legal intervention is permitted only when an action is harmful for others. Otherwise, even if the action is injurious, but only to the agents themselves, it should not be legally prohibited. (Mill, 1869, 186) Therefore, what that delineates the public from the private, in Mill's view, is the scope of possible harms of an action.

Similarly, John Dewey in *The Public and its Problems* (1927), points out that "the line between private and public is to be drawn on the basis of the extent and scope of the consequences of acts which are so important as to need control". (Dewey, 1927, 15) In other words, the public is where interests of many intersect and thus need control, while this is not the case for the private. For example, where we distinguish private path and public highway, or private assets and public funds, we seek to put control on public affairs in order to protect the interests of people.

Despite the differences in approaches and purposes, these philosophers all attempted to make a distinction between public and private. Although making this distinction is an everlasting challenge for every privacy theory, it is by no means the only relevant direction to understand the concept of privacy. In fact, the ongoing social, political, and economical interest shift within the set of problems associated with privacy (e.g. security and privacy, democracy and privacy, e-commerce and privacy, privacy in healthcare, privacy in IT, etc.), demands a broader scope of inquiry than what that can be explained by the dichotomy of public/private, society/individual, or state/citizen. The privacy concerns, nowadays, are not limited to, for example, the ones that existed in Victorian England or the ones depicted in George Orwell's *1984*. The emerging concerns of privacy are not only about the enforcements of moral or political views from society or state to individuals; they are also about the cases, say in social media or health care, where individuals stand against individuals. Therefore,

description of the private as against the public is not the best, or at least the only, way to understand privacy.

Need for Privacy Law

In the Western legal tradition, the significance of having legal protection for privacy was first addressed in Warren and Brandeis, 1890. Their privacy discussion, which was motivated by the conflicts of modern enterprises with individuals' private interests, sought to highlight the importance of privacy as a modern value. The authors claimed that, due to the changes in our modern era, people have "become more sensitive to publicity, so that solitude and privacy have become more essential to the individual". (Warren and Brandeis, 1890, 196) From this perspective, the need for privacy or solitude, as a sort of freedom from being exposed to the public, had become so fundamental that it deserved to be seen as a legal right.

A noteworthy distinguish to be made here is between privacy as a moral right and privacy as a legal right. In the first case, a violation of privacy might merely be assumed as a morally bad behavior with no judicial penalty. In contrast, a violation of privacy as a legal right would be subject to legal prosecution and penalty. Warren and Brandeis asked for the second sort of right. They argued that the invasions of privacy cause severe mental pain and distress for the victims. The right to privacy, then, just "like the right not to be assaulted or beaten, the right not to be imprisoned, the right not to be maliciously prosecuted, [or] the right not to be defamed" (*ibid*, 205), is "a part of the more general right to the immunity of the person, -- the right to one's personality." (*ibid*) With this argument, Warren and Brandeis could justify the need for legal protection of privacy, which was missing at the time.

Privacy Law in the US and Europe

What that the Warren and Brandeis paper has suggested is a demand for legal protection of privacy right in a stronger and clearer sense than what some assume to be

entailed by the Fourth Amendment.[1] Based on this Amendment and also some other constitutional guarantees, Justice Douglas, in Griswold v. Connecticut (1965), argued in favor of the so-called constitutional right to privacy. He believed that, even though the right to privacy is not explicitly mentioned in the Constitution or the Bill of Rights, it is a valid consequence of them. The punembral zones of constitutional guarantees create a "zone of privacy", which accordingly provides the necessary ground for the exercise of other fundamental rights such as freedom of association or the right to education. Therefore, Douglas claimed that the right of privacy did already exist in the law.

Nevertheless, considering the variety of themes that concerns privacy (e.g. health care, financial information, family and groups, etc.) the need for new legislation was undeniable. Here, we only mention the very first attempts in Europe and the US to enact the general privacy law.

The European Convention on Human Rights (ECHR), 1950,[iii] explicitly reflects this concern by including a specific article on privacy (Article 8). This article states that everyone "has the right to respect for his private and family life, his home and his correspondence" and also limits any interference of authorities with this right to exceptional conditions. United Nations also in the International Covenant on Civil and Political Rights (ICCPR), 1966,[iv] announces a similar stand to acknowledge the right to privacy: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence". (Article 17)

In the US, even though the right to privacy is generally endorsed as a fundamental right, there is no comprehensive or explicit privacy law. William Prosser's work (1960) is one of the first attempts to document the existing privacy law in four categories of possible invasions of privacy rights:

[1] The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.

- Intrusion upon individuals' seclusion or solitude, or into their private affairs.
- Public disclosure of embarrassing private facts about individuals.
- Publicity which places individuals in a false light in the public eye.
- Appropriation of one's name or likeness for the advantage of another. (Prosser, 1960, 389)

In recent years, however, privacy laws in the United States have been explicitly enacted to protect the privacy rights of specific groups or domains (e.g., COPPA for minors or HIPPA in health care).

[iii] https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c
[iv] https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

CHAPTER III

THEORIES OF PRIVACY

Whether privacy is an independent, fundamental, and irreducible right, is a substantial question. In the previous chapter, we claimed that even though privacy can be discussed as against publicity, this is not the only way to define it. In fact, an independent understanding of privacy is both possible and wanted. In this chapter, we show how it is possible by looking at some of the theories that discuss the concept of privacy without contrasting it with publicity. An independency from publicity is also wanted, as we mentioned earlier, because not all the privacy cases are conflicts between the private and the public. In this chapter, we also examine the fundamentality of privacy right to see how different theories can justify privacy as a fundamental right, i.e. as an indispensable human right.

Irreducibility of privacy as a right, whether legal or moral, however, is a separate issue. There are other rights beside privacy, say property right, that might protect the same values or interests as privacy does. In this case, privacy would be reducible to other rights. Here, we discuss the competing views on the reducibility of privacy right, i.e. the so-called reductionist view and its counterpart coherentism.

Reductionist View

Reductionists believe that the interests meant to be protected by a privacy right are already covered by other rights and thus any right to privacy is reducible to other rights. One prominent proponent of this view is J. J. Thomson (1975). In order to put her claim, Thomson points out that there are ambiguities in the understanding and application of privacy as a moral right that make it difficult to assume it as a distinct right. By proposing a variety of examples of privacy violations, she argues that these cases can simply be protected by other rights such as property right or the right not to be hurt. Then, she suggests a simplifying hypothesis: “that the right to privacy is itself a cluster of rights, and that it is not a distinct cluster of rights but itself intersects with the cluster of rights which the right over the person consists in and also with the

cluster of rights which owning property consists in." (Thomson, 1975, 306) For example, trespassing into one's property, even though is a violation of privacy right, is already forbidden in accordance with property right. Therefore, in Thomson's view, if "every right in the right to privacy cluster is also in some other right cluster, there is no need to find the that-which-is-in-common to all rights in the right to privacy cluster". Then "the right to privacy is "derivative" in this sense: it is possible to explain in the case of each right in the cluster how come we have it without ever once mentioning the right to privacy." (*ibid*, 313)

While Thomson speaks of the derivativeness of privacy as a moral right, Robert Bork (1990) examines privacy as a legal right. He believes that privacy right is not even derivable from constitutional provisions that are considered for protecting other rights, say liberty. He argues against the constitutional right of privacy, insisting that in Griswold v. Connecticut the court invented "a general but wholly undefined "right of privacy"", (Bork, 1990, 98) which is not based on "some pre-existing right or law of nature" (*ibid*, 97) and has no solid foundation in the Constitution or Bill of Rights.

Coherentism

Many proponents of a legal right to privacy believe, not only the right to privacy is actually implemented in the Bill of Rights, but it also supports the other fundamental rights as well. As we saw in Chapter II, Justice Douglas argued that the right of privacy, even though is not explicitly mentioned in the Constitution, is still the key assumption for a meaningful understanding of the other rights such as freedom of association.

A similar viewpoint, with respect to privacy as a moral right, is suggested in what that Schoeman (1984) calls coherentism. He describes, while the reductionist claims that privacy cases are "diverse and disparate and are only nominally or superficially connected", the opposing view, coherentism, argues that there is "something fundamental, distinctive, and coherent about the privacy cases".

(Schoeman, 1984, 200) This view is motivated by the idea that there is "something special about human moral and social character [...] that transcends the particular cases" of privacy. Note that coherentists assert, not only there is something common to all privacy cases, it is also something distinctive which makes it irreducible from other rights. However, it is hard to see much agreement between coherentists on what makes the essence of privacy. (*ibid*) In the following section, we look at some of the prominent coherentists theories about what constitutes a right to privacy.

Theories of Privacy

What is privacy? Why is privacy valuable? What is the right to privacy? What is the unique feature of privacy that purports to unify divergent privacy cases and distinguishes them from being a case for other rights? How can a right to privacy not be reducible to other fundamental rights? These are the questions that various theories on privacy try to answer. The first question demands a definition for what privacy is and the first theory that we look at here, i.e. privacy as control over information, answers this. However, the rest of the theories that we review in this section are focused more on privacy as a unique moral right.

Privacy as Control over Information

One of the widely used definitions of privacy that dominates the legal and philosophical literature is in terms of control over information. Alan Westin (1967), Charles Fried (1968), and Richard Parker (1974) are among those who proposed or adopted a control-based definition of privacy. Fried states that privacy "is the *control* we have over information about ourselves." (Fried, 1968, 482) Westin believes "privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." (Westin, 1967, 7) A clear and concise definition proposed by Parker is that: "*privacy is control over when and by whom the various parts of us can be sensed by others*." (Parker, 1974, 281) He clarifies that "sense" includes all sort of perceptual access to "parts" or belongings of us. This general definition does also entail control over

personal information as a part of the person and prohibits any sort of unwanted access to it.

The definition of privacy as control over information is incorporated in several theories of a right to privacy. Scanlon (1975) is one of the coherentist theorists who adopts this definition in order to oppose the reductionist view of Thomson. He believes that there is a unique and common foundation (or better, function) in the cluster of rights associated with privacy and that is protecting the "interests in having a zone of privacy". The boundaries of this zone are conventionally defined either by social rules or law, and within which one has better control over when and where certain forms of observations are permitted or prohibited. Therefore, defining a zone of privacy has the practical benefit of giving individuals more comfort in carrying out their activities without the necessity of being continually alert for possible observations. (Scanlon, 1975, 317) The benefits of having a zone of privacy is not attainable when we reduce the privacy right to other rights like ownership. Scanlon clarifies that even though ownership is relevant in defining the boundaries of the zone of privacy, "its relevance is determined by norms whose basis lies in our interest in privacy, not in the notion of ownership." (*ibid*, 318)

But if privacy is valued only because it protects our interest in mental comfort of not being observed, then we cannot condemn unnoticed privacy violations, e.g., when a victim feels comfortable because she does not know about an ongoing violation of her privacy. In this case, a violation of privacy is not provable to be morally wrong if the subject does not feel disturbed by the violation.

Based on Scanlon's view, our interest in privacy, i.e., the immunity from unwanted observations, presupposes the control-based definition of privacy. In other words, the interest in privacy is the interest in having control over information about ourselves. This definition of privacy as having control, however, does not provide us with a robust foundation for a right to privacy.

William Parent (1983) recognizes the weakness of control-based theory of privacy by pointing to the cases where one voluntarily relinquishes her control over part of her privacy. For example, someone shares her private documents with someone else, say her doctor. In this case she is exercising the control over her information but she is not preserving or protecting her privacy, conversely "she is voluntarily relinquishing much of her privacy. People can and do choose to give up privacy for many reasons. An adequate conception of privacy must allow for this fact. Control definitions do not." (Parent, 1983, 273)

Control over information by itself is not the ultimate indicator of protected privacy; it depends on how this control is being exercised. In the following sections, we argue that control over information is effective for protection of privacy only when placed and considered in a context. More important, a right to privacy must be distinguished from what definition of privacy is adopted. In our example, even if the person is relinquishing her control over the information by sharing it and thus waiving part of her privacy, her *right* to privacy should not be waived. In other words, lack of control over personal information does not terminate one's right to privacy.

The control-based definition of privacy, at best, specifies one of the conditions of what it means to have privacy, but does not tell us why we should value our privacy, and thus, it is unsatisfactory for those who search for some intrinsic significance of privacy. Having control over information is merely a consequence of a right to privacy, but not a justification for such a right. Even if we assume control over information as a necessary condition of protected privacy (i.e. having control over information is necessary for having our privacy safeguarded), it by no means provides a sufficient warrant for our right to privacy (at the end of this chapter, we further discuss this shortcoming). Therefore, there must be other theories of privacy that tell us what might constitute a *right* to privacy.

Human Dignity and Autonomy

Some more insightful views attempt to pinpoint the significance of privacy somewhere in one's personality rather than capability (say, of having control). An early example is found in Warren and Brandeis, where it was claimed that the right to privacy is a part of "the right to one's personality." (Warren and Brandeis, 1890, 207) Any individual, as a person, possesses certain basic rights such as the right not to be assaulted or beaten. The right to privacy, likewise it is claimed, is a basic right that belongs to any person. However, the connection between privacy and personality here is not further developed. It is not obvious that privacy right is as basic as, and on a par with, other fundamental human rights.

An indirect but fundamental contribution to the grounding of a privacy right is given by Joel Feinberg (1970) in "The Nature and Value of Rights". He emphasizes that claiming a right is connected with "what it is to be a human being." Each person as a holder of rights does "have that minimal self-respect that is necessary to be worthy of the love and esteem of others. Indeed, respect for persons may simply be respect for their rights". (Feinberg, 1970, 151) In Feinberg's view, then, "human dignity" is rooted in this possession of rights and the appreciation as so. The right to privacy can be seen in this light as an indicator of one's dignity, and accordingly, one might argue that invasion of privacy is a denial of one's possession of rights and thus of their human dignity.

Stanley Benn in "Privacy, Freedom, and Respect for Person" (2017), tries to articulate on the connection between the right to privacy and human dignity. In a similar position to Scanlon and in accordance with the control-based theory of privacy, Benn endorses that privacy provides us with some sort of immunity from unwanted observations, and goes on to relate this to our conception of a person. Like Feinberg's attempt to connect the basic notion of rights with that of respect for personhood, Benn aims to ground the general principle of privacy on a "general principle of respect for persons." (Benn, 2017, 8) By person he means "a subject with consciousness of himself as an agent," which implies "to see him as actually or potentially a chooser".

(*ibid*, 9) Then he clarifies the aspects of "respect": if a person is a potential chooser, respecting him entails respecting his choices too. To disrespect a man is not only to injure him, ignoring his choices is also disrespecting him. Consequently, a seemingly harmless action like unlicensed scrutiny, or making someone an object of observation without his consent, is also offensive; because it ignores his possible choice of not being observed or spied on. Note that the disrespectfulness of spying is not conditional on the possible harm that victims might receive, nor on the knowledge of the victims about their privacy violation. It is disrespectful because it ignores the agent's capability of making choices. It is a denial of him as a choosing subject or an autonomous person. If we assume autonomy as essential for personhood, as Benn does, rejection of one's autonomy is a denial of his personhood. Now, a violation of privacy right might be argued to be a denial of personhood of the subject, because he was not asked for his choice (or consent) and thus his autonomy, which is essential to his personhood, is denied.

Benn stresses that what others know about a person or being observed by others might disrupt, distort, or radically affect what the person does. Therefore, privacy gives individuals more freedom in order to pursue their enterprises regardless of others' judgments about their performance. However, he states that the positive consequences of having privacy should not be the main reason why we respect it. Benn, therefore, has a non-consequentialist argument in favor of the significance of privacy, in which privacy is in principle valuable. Not because privacy promotes one's success, but because anyone who is potentially autonomous is entitled to be respected as a person; privacy is what he deserves as a person. (Benn, 2017, 26)

Intimacy and Relationships

The connection between privacy and intimacy, and the role that privacy plays in any sort of relationship is another theme for the coherentist theories of privacy right. If privacy is the unique and common factor in any relationship and cannot be substituted by other rights, then the reductionist view will fail. Charles Fried (1968), in response to the reductionist stance, highlights the intrinsic significance of privacy. He

argues that privacy is essential for intimacy and relationships. Privacy provides "a necessary context for love, friendship and trust" (Fried, 1968, 478) and these values are "only possible if persons enjoy and accord to each other a certain measure of privacy." (*ibid*, 482)

Fried emphasizes that despite the differences of love, friendship and trust, "each build on a common conception of personality and its entitlement." (Fried, 1968, 478) Privacy grants us "control over knowledge about oneself", and therefore, enables us to regulate our relationships (by giving different persons different degrees of access to our private) and thus makes intimacy possible. (*ibid*, 483) "To be friends or lovers persons must be intimate to some degree with each other. But intimacy is the sharing of information about one's actions, beliefs, or emotions which one does not share with all, and which one has the right not to share with anyone. By conferring this right, privacy creates the moral capital which we spend in friendship and love." (*ibid*, 484) The right to privacy, by granting us control over information about ourselves, as a manifestation of "personal liberty", protects our very integrity as persons. There are thoughts and feelings whose expression would be appropriate and meaningful only to a friend or lover. Privacy gives us freedom of expression or a "freedom to define ourselves" and "control not only over what we do but over who we are". (*ibid*, 485) Fried clarifies that even if privacy is necessary for other human interests (i.e. love, friendship, and trust), it should not be assumed only as a means for these interests. Indeed, privacy is deeply connected to what it means to be a person. Accordingly, a violation of privacy not only sets back other interests that rest upon privacy, it also negates the very personality of the subjects.

The right to privacy is, on Fried's analysis, one of the "basic rights in persons, rights to which all are entitled equally, by virtue of their status as persons." (Fried, 1968, 478) On the same non-consequentialist line with Benn, this means, the promoting benefits of privacy right for individuals is not the (only) reason to justify the privacy right, rather it is the stance of being a person that necessitates the right to privacy. Although Fried and Benn use different terminology (Benn emphasizes on

"choice" and Fried on "control"), they both recognize privacy as a guarantee for personal freedom or autonomy and therefore essential to personhood.

Reasonable Expectations and Contextual Integrity

All the privacy accounts that we reviewed so far adopt the control-based definition of privacy. Whether privacy is justified based on human dignity, autonomy, or intimacy, it presupposes the idea of having control over access to our information as a definition of what privacy means. Indeed, it seems very intuitive that full control over information safeguards our privacy and lack of control is equal to lack of privacy. As I mentioned earlier, however, this view of privacy protection and the role of control over information is not viable. In this section, I show that the idea of control over information is quite irrelevant in safeguarding privacy. As an alternative, we discuss the moral theory of reasonable expectations and contextual integrity.

There are cases that the control-based theory of privacy alone fails to be satisfactory, e.g. when the subjects do not know about the scope of control or when they exercise their control in order to give up their privacy. A right to privacy demands protection of privacy even if control is absent or control is relinquished. Indeed, as soon as we share our information with others we lose our control over the information. But this is exactly where a theory of privacy should be accountable.

To clarify this issue, assume you are having full control over to whom you are texting. For example, you text a colleague complaining about your job. You also won't mind if he shares that with other colleagues, but absolutely not with your boss. Now assume one of your colleagues informs your boss about your opinion. This is an obvious invasion of your privacy (you shared your view with someone but he was not allowed to share it with others). However, it is hard to account for such cases based on the idea of control over information. After all, you had control over your texting and relinquished that by sharing your thoughts. This control does not extend over the shared information between you and your colleagues. Note that even though by

sharing information with others you are relinquishing your control over information, it should not be a relinquishment of your right to privacy.

Cases of privacy most of the time in our daily-life-interactions with others go beyond the scope of control over information. In this case, privacy is still defensible in a broader domain of "reasonable expectations" or "contextual integrity". When you text your colleagues, even though it is going beyond the scope of your control, it still remains within (assuming a high degree of trust between colleagues) the domain of contextual norms and your reasonable expectations, e.g. your text should not go to your boss. In other words, an invasion of your privacy is definable as a violation of your reasonable expectations or contextual norms, but not lack of control.

On the other hand, when our privacy is protected it is again hard to account for that based on the control view. When you share your information with someone, you relinquish your control and thus your privacy. This lack of control, however, does not necessarily mean violation of privacy. Your privacy is not violated as long as your information is kept in accordance with your reasonable expectations and contextual norms. In other words, protection of privacy is definable as consistency of information flow with reasonable expectations and contextual norms, even if control is absent.

Now we can take a closer look at the theory of reasonable exceptions and contextual integrity. Daniel Nathan (1990), attempting to justify privacy as a moral right, recognizes the ground for privacy right in universal human interests: "interests in having a realistic understanding of the world and our situation within it, in having our reasonable expectations fulfilled, in having some grounds for being able to predict the consequences of our actions, in knowing the context of our communications so that we may express what we choose, etc." (Nathan, 1990, 380) Our understanding of the world gives us expectations that make us able to mindfully act and communicate in this world. An invasion of privacy violates these expectations and disturbs the setting necessary for a moral life.

This account was mainly proposed as a response to apparent failure of "no harm principle" when there is an unnoticed violation of privacy. In many cases of privacy, the victim might not know about their violation of privacy for a long time or even forever. Then, since the victim does not feel any harm, it might be claimed based on no harm principle that this violation of privacy is not necessarily a wrongdoing. Back again to our example, assume your boss was secretly monitoring all your conversations since you started your job and he was also very careful of his decisions not affecting your career so that you would never realize that a continuing breach of privacy is happening. However, this invasion of privacy is still a wrongdoing even though there exists no experienced physical or emotional harm. This is a case that Warren and Brandeis could not (or did not want to) include in their theory of privacy. Since their theory justifies the right to privacy based on mental harm, they cannot condemn the cases that the harm is not sensed by the victims. Nevertheless, the violation of privacy in this case is harming, and thus morally wrong, because it violates your reasonable expectation of not being spied on. (I leave the question about the connection of privacy as legal and moral right open here. While Nathan is arguing for privacy as a moral right, Warren and Brandeis look at privacy as a legal right and thus have a different standard or definition for "harm".)

When a covert violation of privacy negates your reasonable expectations, it actually falsifies your perception of your autonomy, dignity, and relationships. You could have different choices if you knew the real situations you were acting in. So the violation of privacy undermines your control and autonomy, and thus your dignity as an actual chooser. Note that "we can fail to respect others as persons" also by ignoring "what we know to be their actual choices, not just their capacity to choose." (Nathan, 1990, 371) In fact, granting someone control over their information might only identify them as "potentially a chooser". For being an actual chooser, however, we need correspondence of reality with our expectations and being able to make informed choices. When the setting of our actions is not in accordance with our expectations, the assumption of having control is only an illusion. Therefore, privacy understood as

consistency of goings-on with our reasonable expectations comes before having control. Within such undisturbed setting we can have genuine control over our information.

So far we understood that to be faithful to individuals' privacy we need to act in accordance with their reasonable expectations, and a violation of such expectations might be a violation of their privacy. But when it comes to privacy people have different sorts of expectations which sometimes might be quite unreasonable. Then, what is the criterion of *reasonableness* of expectations? This can be based on the context of privacy case. Helen Nissenbaum (2004), suggests the "contextual integrity" as an alternative benchmark for privacy, when the old accounts of privacy fail to deal with the challenges posed by information technologies. In her view, "contextual integrity ties adequate protection for privacy to norms of specific contexts, demanding that information gathering and dissemination be appropriate to that context and obey the governing norms of distribution within it." (Nissenbaum, 2004, 119) Nissenbaum explains that "contexts are partly constituted by norms, which determine and govern key aspects such as roles, expectations, behaviors, and limits." In most contexts there are two norms that govern information about the people involved in the contexts, called "informational norms: norms of appropriateness [govern what information about persons is appropriate, or fitting, to reveal in a particular context], and norms of flow or distribution [govern movement, or transfer of information from one party to another or others]. Contextual integrity is maintained when both types of norms are upheld, and it is violated when either of the norms is violated." (*ibid*, 138) Then, concerning our question about the reasonableness of expectations, we can rely on the context and its informational norms. Expectations that are formed within a specific context and are in accordance with its informational norms can be assumed as reasonable expectations.

To conclude this section, a proper protection of privacy is possible when the privacy goings-on within a context are in accordance with subject's reasonable expectations about informational behaviors of other parties, expectations that are

formed within the context and are based on its informational norms. Since we behave based on contextual norms and our actions are regulated by our expectations of goings-on, any violation of such expectations could be a violation of our privacy right.

Thus far we saw how theories of privacy evolved throughout history and specially in recent decades where technological development demanded more sophisticated understanding of privacy. The growth of informational technologies, however, had a dazzling speed in recent years, which accordingly caused unprecedented challenges for individuals' privacy. With the background proposed here about the theoretical basis of privacy, we can now look at the privacy challenges posed by new developments in information technology to see how regulations handle the data privacy cases and whether our analysis of privacy sheds light upon the problems.

CHAPTER IV

PRIVACY AND INFORMATION TECHNOLOGY

Privacy has always been a focal concern in recent decades, but the new technological developments has drastically changed the problems concerning individuals' privacy. Modern information technologies are widespread and influential. They are everywhere and used almost by everyone for a very wide range of purposes from health care to entertainment. Despite the advantages and opportunities provided by this development, there are also downsides leading to serious privacy concerns.

Modern services on the internet such as social media, search engines, online shopping, and all the other online services associated with the concept of Big Data, are the major source of privacy concerns in IT. Besides that, the new technological platforms such as smart phones and IoT (Internet of Things) devices, cause an unprecedented extension of the domain of computer-based services into physical world. As a result, nowadays we can be easily watched, heard, and tracked at anyplace and anytime.

Moreover, the covert and expanding dimensions of informational privacy are hardly known by ordinary users. An empirical study recognized that "consumers often lack enough information to make privacy-sensitive decisions and, even with sufficient information, are likely to trade off long-term privacy for short-term benefits." (Acquisti, 2005) In this chapter, regulations play an important role to mitigate the possible risk of data privacy violations. Privacy regulations, however, will not be fully effective to protect individuals' privacy if privacy and privacy law are not properly understood by the participating parties (i.e. users, service providers, legislators, and authorities).

In this chapter, first we explain the concept of data privacy and look at the examples of online services and their related data privacy concerns. Then, we look at the regulations for personal data protection and discuss their moral/legal rationale.

Personal Information and Data Privacy in IT

The concept of personal information or personal data is somehow self-explanatory, though its instances can be challenging to recognize. For example, it is easy to admit unique identifiers (e.g. birth date, social security number, etc.) as part of personal information, or patients' profiles as containing personal data. However, it is hard to count people's preferences on an online shopping website as personal data, or at least as sensitive data as identifiers. Thus, some types of personal data are more sensitive than the others, i.e. their breach will cause harsher harms. A theory of privacy should be able to account for this variation of sensitivity.

Note that not all the sensitive data, on the internet, are "personal" and thus central to privacy concerns (e.g. passwords, which also protect individuals' privacy, are more about security than privacy). On the other hand, there are non-sensitive data (e.g. personal preferences and feedbacks), which might be used to derive sensitive data and thus result in acute privacy concerns. Having a thorough picture of what counts as the subject of privacy talk in IT, then, is essential.

Besides the subject of data privacy, i.e. personal data, it is worth considering two different sides of data protection, i.e. privacy and security. Despite the difficulty of demarcation of these two, security in general is more about the technical safeguards for protecting the data from unauthorized access or cyber attacks. Privacy, on the other hand, has a broader scope and includes protecting the data from all sort of illegitimate access or operation. Even though data privacy entails security, the latter is not the main focus of our discussion here.

Now we look at several contexts of privacy concerns in IT, along with the sorts of data that need to be taken care of by data protection policies.

Internet and Social Media

The internet is a worldwide network that connects a huge number of computers together for a variety of purposes. The internet is also a gigantic source of data, gathered from its users. The main privacy concern on the internet is anonymous web-

surfing, i.e., being incognito when the recognition of user's identity is not necessary, say on a search engine. However, many websites use tracking techniques, like cookies (small files stored on user's computer), to track and remember the users in order to improve their service. The data collected, stored, and used by cookies are not always clear and thus are an important source of privacy concern on the internet.

Social media likewise is proposed to connect people all around the world via phone applications and websites like Facebook, Google+, or Twitter. Many of these social networking websites ask users for all sorts of information in order to provide them with better services. For example, Facebook has the option to find people who live in your neighborhood or attend the same school as you do, provided you enter your location or academic affiliations. The degree of richness of the data on social media is much higher than what say cookies contain. The data on social network sites range from rather general or seemingly trivial data (like your favorite books or songs) to sensitive information (e.g. location or date of birth). The data gathered on these websites can also be processed, shared, or used for many purposes. For this reason, nowadays social media is a major source of privacy concerns. In Chapter VI, we look at one example of a privacy scandal that happened for Facebook.

E-Commerce and E-Government

New information technologies have transformed the way traditional services used to be offered. Websites like Amazon or eBay are examples of e-commerce corporations that have changed and dominated the shopping method and habit of many consumers around the globe. The range of services provided by e-commerce companies is vast (from ordinary shopping to entertainments) and the number of their clients is huge (Amazon had 310 million active customers in 2016)[v]. Online marketing websites in addition to personal information also collect and process financial and marketing data. They are also big users of personal data coming from other online resources and thus raise many privacy concerns with respect to data sharing.

The same platform also has changed the way governments offer services to citizens. The data and services associated with e-government (e.g. biometric passport or online voting) are highly sensitive and therefore are the main focus of privacy/security concerns. E-government has also inspired the ways that citizens can participate in legislation and policy-making, and promoted equal opportunities for practice of democracy. The advantages of this opportunity likewise is contingent on protection of privacy.

Smartphones and Internet of Things

Devices connected to the internet are the other emerging source of privacy concern. Smartphones are equipped with GPS, cameras, sensors, microphone, and a huge capacity to store private information of users. They have also access to biometric features of users (via fingerprint and face-recognition technology). Due to these capabilities, smartphones are much more sophisticated in tracking and monitoring users than what people imagine.

Internet of Things (IoT) refers to smart devices that have some of the capabilities mentioned above plus being connected to other devices and household appliances. They can gather data and monitor users' behavior. Amazon Alexa, for example, is a virtual assistant which is able to access to the internet, control smart home, get information, and make to-do lists, by using user's voice. So it is constantly listening to its users. Devices like Alexa are extending the domain of information technologies into real life more than ever.

Big Data and Cloud Computing

The size of data gathered from smart devices, social media, websites, or any other online sources, is colossal. This amount of data, known as Big Data, is usually being used by data mining and pattern extraction techniques to derive useful information about users. For example, the choices of consumers on an online market can imply some shopping trends. This could be revealed by further process of the Big Data and could help the website to improve its advertisements and marketing

strategies. Note that Big Data does not belong to one person but it contains meaningful data within a context about a group of people. Therefore, even though Big Data does not reveal an individual's data, it still has privacy implications because the derivative data might be used to target a group of users.

Simply put, cloud computing is the delivery of computing services, e.g. servers, storage, networking, analytics, and more, over the Internet or the "cloud".[vi] There are companies, called cloud providers, that offer cloud services to other businesses. It is the cloud provider that decides about the maintenance of the data and not the businesses that collect the data from users. Thus, the operations on the data may or may not follow the Terms of Service agreement between users and businesses.

Legal Provisions for Data Privacy Protection

To protect individuals' data privacy, there are privacy regulations enacted by several jurisdictions all around the world. These regulations aim to reduce the risk of privacy violations and possible harms that online users might be subject to on the internet or through the digital services. There are also economic motivations for the privacy regulations, but those issues are out of the scope of our study. Here, we will only review fragments of prominent data privacy laws. In the next chapter, we will go on to analyze the objectives and rationales of these regulations.

As an attempt to depict a roadmap for data privacy laws, a set of principles, indicating fair use of personal data, has been proposed by the Organization for Economic Co-operation and Development (OECD)[vii], in 1980. The Guidelines on the Protection of Privacy suggested by OECD, is accepted under the Data Protection Directive 95/46/EC[viii], by European countries as well as Canada, the United States, and Japan, to unify the existing regulations of data privacy and control the trans-border flows of personal data across continents. OECD has eight principles for this purpose:

- Collection limitation principle, which limits the collection of personal data to be obtained only by lawful and fair means and with the knowledge or consent of the data subject.
- Data quality principle, which demands relevance of the collected data to the purposes for which they are to be used.
- Purpose specification principle, which necessitates specifying the purposes of data collection at the time of collecting the data.
- Use limitation principle, which limits the disclosure, share and use of the data to the specified purposes.
- Security safeguards principle, which demands protection of personal data by reasonable security safeguards against risk of loss or unauthorized access, destruction, use, modification or disclosure.
- Openness principle, which asks for a general policy of openness about developments, practices and policies with respect to personal data.
- Individual participation principle, which specifies several rights for data subjects, including having access and control over the data.
- Accountability principle, which signifies that a data controller should be accountable for complying with the measures stated by these principles.

OECD's recommendations and the Data Protection Directive, however, are not regulations and thus are not binding for the participating nations. The General Data Protection Regulation (GDPR)[ix] has been enacted and adopted by European Union (EU) countries, in 2018, to substitute the Directive. GDPR regulates the processing of personal data by any individual or institution in the EU and also expects compliance from foreign companies that process personal data of EU citizens. Note that the word "process" here represents a broad range of operations on personal data, which includes collection, recording, storage, retrieval, use, and share. Any viable privacy law needs

to consider these different forms of data processing. GDPR also specifies the governing principles of lawful data processing (Article 5), which demand personal data to be:

- processed lawfully, fairly and in a transparent manner.
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- accurate and, where necessary, kept up to date.
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing.

Similar to OECD's principles, GDPR asks for security, fairness, and openness but also has some more sophisticated demands like anonymity and temporality.

In the United States, the Fair Information Practice Principles (FIPPs)[x], an equivalent guideline with GDPR, have been suggested by Federal Trade Commission (FTC). The Fair Information Practice, widely accepted by other guidelines and regulations, has five principles:

- Notice/Awareness: consumers should be given notice before any personal information is collected (or processed). Without notice, a consumer cannot make an informed decision.
- Choice/Consent: consumers should be given options as to whether and how any personal information collected from them may be used.

- Access/Participation: individual should be able both to access their data and to contest that data's accuracy and completeness.
- Integrity/Security: collectors must take reasonable steps to keep the data accurate and secure.
- Enforcement/Redress: there should be an enforcement and redress mechanism for effectiveness of these principles.

These principles of fair information practice, however, are not backed by governmental enforcement and are only effective by self-regulation of data collectors. Other US privacy regulations (such as the Health Insurance Portability and Accountability Act (HIPAA), the Fair Credit Reporting Act (FCRA), or the Electronic Communications Privacy Act (ECPA)) even though are backed by law, are not either comprehensive or specific with respect to informational privacy.

In the following chapter, we analyze these guidelines/regulations based on their legal and ethical philosophy.

---

[v] https://www.statista.com/statistics/476196/number-of-active-amazon-customer-accounts-quarter/
[vi] https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/
[vii] http://www.oecd.org/sti/ieconomy/ oecdguidelines ontheprotection ofprivacy andtransborderflowsofpersonaldata.htm
[viii] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046
[ix] https://www.eugdpr.org/
[x] https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf

CHAPTER V

LEGAL AND ETHICAL OBLIGATIONS TO PROTECT PRIVACY

Among other reasons, due to the diversity, complexity, and rapid changes of the context of privacy concerns in information technology, the process of law making and implementation of regulations in IT businesses is very challenging. Businesses do not receive much help from regulations for implementing privacy laws except some general and abstract rubrics of obligations and prohibitions. Therefore, regulations need to be accompanied with an interpretative understanding of what privacy and privacy law is about in order to be properly implemented by businesses.

Moreover, regulations usually come after the fact, i.e., when the unknown aspects of privacy concerns become real problems. Therefore, businesses need to be proactive with respect to privacy protection and proceed their activities before new enactments (e.g., recent version of GDPR which has affected many businesses around the world). This is also suggested in the very first principle of widely accepted "privacy by design" (PbD) approach (a system design framework entailing a set of privacy principles), where it encourages system developers to be proactive instead of reactive. In other words, it asks system developers to prevent privacy violations instead of just remedy them. (Cavoukian, 2010, 249) This need for proactiveness can be met by having a privacy heuristic that helps developers to imagine what the possible privacy requirements would be like.

Therefore, to mitigate the problems of implementation of regulations and proactiveness, we need to provide the privacy regulations with a privacy philosophy. The legal obligation to protect data privacy would not be fully effective without a moral obligation to do so. There should be a privacy paradigm that leads all the participating parties (consumers, service providers, legislators) towards looking at privacy as a value. This needs an integration of privacy regulations with ethical awareness and commitment of service providers. This stand, to some extent, is also suggested by the PbD approach, where it highlights "respect for user privacy" as the

ultimate principle in system design. (Cavoukian, 2010, 250) This principle of PbD asks developers in the course of system design to focus more on the privacy needs of individuals than other technical requirements or systemic objectives.

A privacy paradigm that entails a comprehensive understanding of privacy and of the playground in which participating parties interact is what we will propose at the end of this section. Such a paradigm, however, is missing in the state of affairs of privacy in IT.

When it comes to legislation, it is hard to see a coherent and persuasive privacy theory to guide the legislators towards a proper privacy policy. Regulations, in a broad view, have two sorts of motivations which are meant to justify privacy policies: 1) protection of legal/moral rights of consumers and 2) economical advantages of regulated markets. Aside from the second motivation, which is out of the scope of our discussion, the first motivation is only loosely addressed within the privacy guidelines and regulations.

GDPR, for instance, following the Charter of Fundamental Rights of the European Union[xi] (Chapter II, Freedoms), recognizes the protection of individuals in the course of data processing as a fundamental right. (Paragraph 1) The GDPR document, however, does not propose its legal philosophy and the possible meanings of privacy which might underpin its suggestive principles. Similarly, OECD demonstrates two essential basic values (i.e., the protection of privacy and individual liberties and the advancement of free flows of personal data (II.A.22)) as the main focus of its provisions. And finally, the FIPP only has a short background on its suggestive principles, which are to assure that the "information practices" are fair and provided with adequate privacy protection. (III.A.)

Even though the aforementioned regulations do not discuss their legal philosophy, they show common characteristics in their principles. GDPR, OECD, and FIPP, all three value freedom or liberty of consumers and also reserve the right of control over personal data for consumers. And thus, it might be argued that these

regulations, looking back at the privacy theories that we reviewed in Chapter III, have implemented the idea of privacy as autonomy and privacy as control over information. This claim, however, is still far from the assumption that these regulations are reflecting a unifying theory of privacy that covers the multifarious aspects of privacy in IT. The privacy principles of GDPR, OECD, and FIP merely represent a set of ad-hoc provisions that have little to show about what proactiveness with respect to privacy protection would be like.

Now, on the side of organizations or service providers, since the regulations are not accompanied with an explicit philosophy, each company would have to come up with its own privacy theory or "code of conduct", which is not guaranteed to be a proper guideline. Even some regulations, like FIPP, ask for more and urge the organizations for self-regulation. As studies have shown (Gellman, 2011), self-regulation has never been a successful experience. Lack of a privacy theory, which justifies and gives meaning to the regulations, might be one possible reason of this failure.

And finally, on the side of consumers, there is no proper theory of privacy that consumers all around the world even generally share. However, there are privacy tendencies that might be insightful for illuminating the problem. Consumers usually have different understandings, and thus strategies, with respect to privacy. Some people value their privacy over the possible benefits of information sharing and do not participate activities with privacy risk. Others just ignore the value of privacy and easily relinquish their right. However, most people are what Westin (2003) calls privacy pragmatists; they examine the benefits and risks of data collections and then decide whether to trust the organizations or seek legal oversight. (Westin, 2003, 22) In other words, when it comes to use online services most users, who care about their privacy, make privacy decisions based on the context of their activity. For example, a simple search engine might seem benign and thus users usually trust the website for their basic needs, but an online service that requests rather sensitive information from customers might make its users to be more cautious.

Therefore, in a theory of privacy, context is a decisive factor. The other factor would put stress on the users. What that is at stake is users' privacy after all. Thus, it is important to consider what consumers' assumptions are. This being said, we believe a theory of privacy based on the idea of reasonable expectations and contextual integrity, discussed at the end of Chapter III, would be a proper candidate for explaining what privacy is about and how an appropriate protection of privacy is possible.

Integration of this privacy theory with regulations will necessitate both legal and moral obligations for organizations to protect individuals' privacy based on the context and in accordance with the expectations of their costumers. Since costumers' expectations form within the context, any action inconsistent with reasonable expectations of costumers might be counted as a violation of contextual norms and thus as a possible risk of privacy violation.

This understanding of privacy, even though seems to ask for further obligations for organizations, has in fact practical advantages too. It facilitates, for example, being proactive with respect to privacy protection. Contextual privacy urges the system designers to think like a typical costumer, who is surrounded by contextual norms, in order to figure out the best way of being consistent with the expectations that are formed within the context. The contextual integrity and reasonable expectations theory might, then, also be used for better understanding and further interpretation of the regulations. For instance, principles ii and iii of GDPR, and ii-iv of OECD, require faithful gathering and processing of personal data based on the agreed purposes. One's personal data, for example, might be gathered for scientific studies, but it is not permitted to be used for commercial purposes. Such usage of personal data is against the reasonable expectations that formed at the time of data gathering. Such usage, however, might be legitimate if we inform the data subject of the new purposes of data processing, i.e., if we update his expectations.

This privacy theory is also in accordance with people's daily-life intuitions. The way that we behave within a given environment is based on the norms in that

setting, the norms that shape our expectations and regulate our behaviors. Therefore, the contextual (or norm-based) theory of privacy has no further burden for individuals to be adopted.

At the end, incorporation of contextual privacy with the regulations has been suggested in President Obama's Privacy Bill of Rights (White House Privacy Report, 2012). This bill entails the unprecedented principle of "Respect for Context":

"Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data."[xii]

Respect for context, in one interpretation (Nissenbaum, 2015), "means to respect contextual integrity, and, in turn, to respect informational norms that promote general ethical and political values, as well as context-specific ends, purposes, and values." (Nissenbaum, 2015, 298) This understanding of data privacy is deeply rooted in the moral theory of consistency with reasonable expectations. Respect for context, then, means respect for the context-dependent choices of the agents who might have different choices being in an unexpected situation. With this interpretation, the challenging cases of data privacy would be easier to analyze and resolve.

In the next chapter, we study and discuss the contentious case of Facebook's privacy violation to see how the privacy paradigm that we discussed here will deal with privacy cases in practice.

[xi] http://www.europarl.europa.eu/charter/pdf/text_en.pdf
[xii] https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf

CHAPTER VI

CASE STUDY: FACEBOOK'S PRIVACY SCANDAL

In March 2018, The Guardian and The New York Times, revealed that the data extracted from 50 million (and even more) Facebook profiles were sold to Cambridge Analytica, which used the data to develop "psychographic" profiles of users, and target users with pro-Trump advertising.[xiii] This data breach was maybe the biggest privacy scandal by Facebook in terms of size and impact on people since Facebook's inception in 2004. In this section, we take a closer look at the goings-on in this privacy case to see how our theory of privacy responses to the questions.

In 2014 Aleksandr Kogan, a psychology professor at Cambridge University, built a personality survey app and lunched on Facebook to harvest data for Cambridge Analytica. The app scraped some private information from users' profiles and those of their friends. The data included details on users' identities, friend networks and "likes." The idea was to map personality traits based on what people had liked on Facebook, and then use that information to target audiences with digital ads. About 270,000 users (those who participated in the survey) had consented to having their data harvested, though they were all told that it was being used for academic use.[xiv] Since friends' data of the participants were also accessible to the study, ultimately over 50 million raw profiles became available to the firm; and even later in April, Facebook reported that the "information of up to 87 million people — mostly in the US — may have been improperly shared with Cambridge Analytica."[xv]

Although during this incident the data were taken from the system without authorization and also Facebook's officials admitted that, they still refused to call it a "data breach". Deputy general counsel Paul Grewal announced that "the claim that this is a data breach is completely false" because the researcher got consent from everyone involved. Similarly, Andrew Bosworth, Facebook's former vice president of ads, writes: "This was unequivocally not a data breach. People chose to share their data with third party apps and if those third party apps did not follow the data agreements

with us/users it is a violation; no systems were infiltrated, no passwords or information were stolen or hacked." Instead, Facebook's executives call it a "breach of trust", which has no legal implications while "Data breach" does.[xvi]

After delivering an apology by Mark Zuckerberg, Facebook's founder and chief executive officer, Facebook also took practical actions to make sure that such privacy breach does not happen again.[xvii] Facebook announced that it would voluntarily implement the EU's new General Data Protection Regulation (GDPR) laws in all areas where Facebook operates. "We're going to make all the same controls and settings available everywhere, not just in Europe".[xviii] Facebook also took steps for making its Terms and Data Policy clearer, without asking users for new rights to collect, use or share their personal data on Facebook.[xix]

One echoing theme in Facebook Data Policy, which is also demanded by the laws, is about users' right to have control over personal data. Privacy Basics of Facebook highlights that "You have control over who sees what you share on Facebook." And this, indeed, is where the lawmakers in the US and Europe focused on when questioning Zuckerberg for the privacy scandal. In his testimony to Congress, in April 10, 2018, Zuckerberg in his answers to various questions of senators, repeats the word "control" over 60 times;[xx] and almost the same times in House committee hearing, for his second day of questioning.[xxi]

Having control over information is already addressed in several regulations, as we saw in previous section. However, giving users control over their personal data has only become a leeway for businesses to satisfy the minimum requirements of the regulations. As an answer to Senator Hatch's question, "what sorts of legislative changes would help to solve the problems the Cambridge Analytica story has revealed?" Zuckerberg states, "giving people complete control. This is the most important principle for Facebook: Every piece of content that you share on Facebook, you own and you have complete control over [it]". [xxii]

Nevertheless, this did not and will not prevent such privacy breaches. Control over information is always limited by its nature. In fact, as we explained in Chapter III, having control over information only means one can decide whether to give others access to his data or not, but once he decided to share the data with others control over the data is relinquished. Control over information, indeed, is merely a right for individuals as part of their right to privacy and it will never guarantee privacy protection of users. The most important part of privacy concern begins when the data is shared and thus is out of control of user.

A proper protection of personal data would not be attainable if we disrespect the contextual integrity and reasonable expectations of users. Even having control over information is contingent on the consistency of expectations (my belief that I have control over the data) with the context (my control within a given setting is in fact effective). The principle of consistency with reasonable expectations or contextual integrity guarantees that the control over information would be effective and in accordance with contextual norms or users' expectations.

In the case of Cambridge Analytica, where the app used participants' profile to access their friends' data, users' control over information was rather irrelevant. Although at first users exercised their right to control over personal information (i.e. they chose to use the app and thus shared their data with it), this right could not guarantee their privacy protection. Once the users, by sharing the data with the app relinquished their control, there was no guarantee, with respect to control-based theory of privacy, for fair use of their data. Then, the researchers can access their data, including those of their friends.

For the other aspect of this breach, where the data is being used for political purposes, the control-based theory of privacy again fails to condemn the abuse of the data. Since the users have consented the data collection, the data is no longer under their control and thus, based on control theory, they have no longer any right to decide about it. Although the data should be used based on the purpose specifications in the terms of service of the app, the right to control has no impact here.

However, contextual integrity and consistency of use with reasonable expectations does not permit either of these actions. Even though the users shared the data with the researchers and the data includes information's of friends, they are not permitted to access those information of friends because this is not something reasonably expected by users. The contextual norms that are formed within the social networks do not approve such an overreaching for friends' data, and the reasonable expectations based on these norms never agree with it. After all, why should one's participation in the survey affect others who had no interest in it? The contextual norms also do not permit unusual use of the data for political purposes. Based on the context, most Facebook users expect the data to be collected for scientific and academic purposes (unless it is directly connected to advertisements). Using the data for other purposes, especially targeting the users for political manipulation, was not expected at all. Therefore, the act of using the data for this type of goals is a violation of contextual norms and thus it violates the right of users' reasonable expectations to be met.

This being said, terms of services is one of the important elements that *should* form user's expectations and therefore needs to be discussed here. First of all, it is extremely rare for terms of services to be read by users. Even Facebook did not read the terms of "THISISYOURDIGITALLIFE", the app used by Cambridge Analytica.[xxiii] Second, even if users read the terms, chances are they would not understand it properly. And finally, terms of services do not exhaust all the possibilities for data collection, share, and use. For example, the terms of the app states its purposes as such: "We use this Application [...] as part of our research on understanding how people's Facebook data can predict different aspects of their lives. Your contribution and data will help us better understand relationships between human psychology and online behavior."[xxiv] This note, however, does not give users a picture of what this "understanding" (i.e. the product of the data processing) would be used for.

But if terms of services is not an effective tool for shaping users' expectations (while it should be), how are, then, reasonable expectations formed? Once again, contextual norms. In fact, the way people exercise their control over information to make privacy decisions or even whether to read the terms of services or how to interpret them are all based on the norms of the environment where the privacy-sensitive goings-on happen. For example, since Facebook is, or used to be, a trusted platform and also does not sell or use personal data for unusual purposes, it seems reasonable to also trust the applications that run on Facebook. This is the same expectation that most people have when they use other trusted platforms like App Store or Google Play in order to have access to safe applications. Facebook's failure in ruling out a malicious app, therefore, should be condemned, not because Facebook did not give enough control to users, but because it failed to comply with the contextual norms and to meet users' reasonable expectations.

[xiii] https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/
[xiv] https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html
[xv] https://newsroom.fb.com/news/2018/04/restricting-data-access/
[xvi] http://time.com/money/5210825/facebook-data-breach-experts/
[xvii] https://www.facebook.com/zuck/posts/10104712037900071
[xviii] https://www.xda-developers.com/facebook-voluntarly-enforce-eu-privacy-law/
[xix] https://newsroom.fb.com/news/2018/04/terms-and-data-policy/
[xx] https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?noredirect=on&utm_term=.9259837202dc
[xxi] https://www.washingtonpost.com/news/the-switch/wp/2018/04/11/transcript-of-zuckerbergs-appearance-before-house-committee/?utm_term=.5dfc655eef35
[xxii] https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?noredirect=on&utm_term=.9259837202dc
[xxiii] https://www.washingtonpost.com/news/the-switch/wp/2018/04/26/facebook-didnt-read-the-terms-and-conditions-for-the-app-behind-cambridge-analytica/?utm_term=.eab4acde487f
[xxiv] https://www.blumenthal.senate.gov/imo/media/doc/Facebook%20App%20Terms%20of%20Service.pdf

CHAPTER VII

CONCLUSION

We started this essay with a broad review of the notion of privacy in history, which discussed the meaning of privacy, whether in philosophical, political, or legal writings, in contrast with publicity. We noticed that the contemporary concerns of privacy are not limited to the ones coming from the public, and thus in modern theories of privacy we considered privacy as an independent concept from publicity. We also saw that privacy, as a fundamental moral right, is not reducible to other rights. The right to privacy is a basic and necessary requirement for many human interests, such as love, trust, and friendship. Privacy is, indeed, deeply rooted in personhood, dignity, and autonomy. As an autonomous person, one has a right to have control over his information and respect for this right is respect for the person. We recognized that even though this right to control over information is a consequence of a right to privacy, it is not much useful for the protection of individual's privacy.

As an alternative we reviewed the theory of contextual integrity and reasonable expectations. Based on this theory, the hallmark of privacy should be consistency of behaviors with reasonable expectations of individuals, expectations that form within a context and follow its norms. A right to privacy will protect our interest in having our reasonable expectation to be met. An unviolated privacy right, then, would be possible when the environment in which we live and act is consistent with our reasonable expectations. In other words, the goings-on in this environment by following the informational norms preserve the contextual integrity, and thus individu11als' privacy.

After describing this theory of privacy, we looked at the modern information technologies and their possible privacy risks, along with the data privacy regulations. We observed that a comprehensive understanding of privacy is missing in the regulations and thus a privacy paradigm, useful for both legislators and businesses, is suggested to fill this gap. Such a paradigm, we argued, can be based on the theory of reasonable expectations and contextual integrity. And finally, we analyzed the privacy case of Facebook and Cambridge Analytica to see if the suggested privacy paradigm

would be helpful to recognize the problem and propose solutions for it. This privacy paradigm, however, needs further articulation and development in order to be fully functional.

BIBLIOGRAPHY

Acquisti, Alessandro, and Jens Grossklags. "Privacy and rationality in individual decision making." *IEEE security & privacy* 3.1 (2005): 26-33.

Benn, Stanley I. "Privacy, freedom, and respect for persons." *Privacy and Personality*. Routledge, 2017. 1-26.

Bork, Robert H. "The Tempting of America: The Political Seduction of the Law." *New York: Touchstone Press* 62 (1990): 66.

Cavoukian, Ann. "Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph. D." *Identity in the Information Society* 3.2 (2010): 247-251.

DeCew, Judith Wagner. "The feminist critique of privacy: past arguments and new social understandings." *Social dimensions of privacy: interdisciplinary perspectives. Cambridge University Press, Cambridge* (2015): 85-103.

Dewey, John. *The Public and Its Problems* (New York: H. Holt & Co.). (1927).

Feinberg, Joel, and Jan Narveson. "The nature and value of rights." *The Journal of Value Inquiry* 4.4 (1970): 243-260.

Fried, Charles. "Privacy [A Moral Annalysis]." *Yale Law Journal* 77 (1968): 21.

Gellman, Robert, and Pam Dixon. "Many failures: A brief history of privacy self-regulation in the united states." *World Privacy Forum*. 2011.

Griswold, V. "Connecticut, 381 US 479, 85 S." *Ct* 1678 (1965): 14.

Locke, John. Second treatise of government and a letter concerning toleration. (Jonathan Bennett ed., 2017) (1689): https://www.earlymoderntexts.com/assets/pdfs/locke1689a.pdf

Mill, John Stuart. "On Liberty, ch." *V (David Bromwich & George Kateb eds., 2003)* (1869).

Nathan, Daniel O. "Just looking: Voyeurism and the grounds of privacy." *Public Affairs Quarterly* 4.4 (1990): 365-386.

Nissenbaum, Helen. "Privacy as contextual integrity." *Wash. L. Rev.* 79 (2004): 119.

_____. "Respect for context as a benchmark for privacy online: What it is and isn't." (Roessler & D. Mokrosinska eds.), *Social Dimensions of Privacy: Interdisciplinary Perspectives* (pp. 278-302). Cambridge: Cambridge University Press. (2015).

Parent, William A. "Privacy, morality, and the law." *Philosophy and Public Affairs*, 12: 269–88 (1983).

Parker, Richard B., "A Definition of Privacy," Rutgers Law Review 27 (1974).

Prosser, W. "Privacy: A Legal Analysis'(1960)." *California Law Review* 48: 338.

Schoeman, Ferdinand. "Privacy: philosophical dimensions." American Philosophical Quarterly 21.3 (1984): 199-213.

Scanlon, Thomas. "Thomson on privacy." *Philosophy & Public Affairs* (1975): 315-322.

Thomson, Judith Jarvis. "The right to privacy." *Philosophy & Public Affairs* (1975): 295-314.

Warren, Samuel D., and Louis D. Brandeis. "The right to privacy." Harvard law review (1890): 193-220.

Westin, Alan F. "Privacy and freedom, atheneum." *New York* 7 (1967).

_____. "Social and political dimensions of privacy." Journal of social issues 59.2 (2003): 431-453.