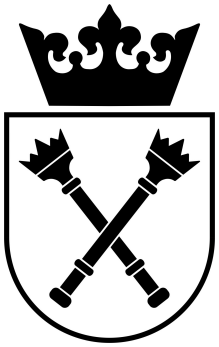
Uniwersytet Jagielloński
Wydział Studiów Międzynarodowych i Politycznych
Instytut Nauk Politycznych i Stosunków Międzynarodowych



POLITICAL PRIVACY
How Privacy Protection Empowers Democracy

Aleksandra SAMONEK

Praca doktorska przygotowana pod kierunkiem
dr hab. Doroty PIETRZYK-REEVES, prof. UJ

2022

Contents

Abbreviations

Legal Acts and Documents

1995 Data Protection Directive Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281 , 23/11/1995 p. 0031 - 0050 (31995L0046), url: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046 (Accessed May 5, 2021).

BDSG Bundesdatenschutzgesetz. Federal Data Protection Act of 30 June 2017, Federal Law Gazette I, p. 2097, as last amended by Article 12 of the Act of 20 November 2019 (Federal Law Gazette I, p. 1626), url: https://www.gesetze-im-internet.de/bdsg_2018/ (Accessed May 5, 2021).

BGB Bürgerliches Gesetzbuch, German Civil Code, 1747 (1896).

CFREU Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.

Chinese Civil Code 1986 The General Principles of the Civil Law of the People's Republic of China, promulgated April 12, 1986, in force since January 1, 1987 and changed by the Civil Code of People's Republic of China adopted on May 28, 2020, in force since Jauary 1, 2021, and other acts.

Chinese Civil Code 2020 The Civil Code of People's Republic of China adopted on May 28, 2020, in force since Jauary 1, 2021, cited in translation from www.npc.gov.cn/englishnpc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf (Accessed March 20, 2022).

Chinese Cybersecurity Law The Cybersecurity Law of the People's Republic of China, passed November 6, 2016 (effective June 1, 2017), enacted by the National People's Congress. Cited in translation by DigiChina project, url: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ (Accessed May 10, 2021).

Constitution of China The Constitution of the People's Republic of China of 1982 with Amendments through 2018, including *Xianfa Xiuzhengan* of 1988, 1993, 1999, and 2004. Cited in translation by the Constitute Project https://www.constituteproject.org/constitution/China_2018.pdf?lang=en (Accessed May 10, 2021).

ECHR Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5.

ePrivacy Directive 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). Official Journal L 201 , 31/07/2002, pp. 0037 - 0047.

FISA The Foreign Intelligence Surveillance Act of 1978 (Pub.L. 95–511, 92 Stat. 1783, 50 U.S.C. ch. 36), October 25, 1978, url https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286 (Accessed May 10, 2021).

French 2014 Anti-terrorism Law Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme (1), url: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000029754374/ (Accessed May 5, 2021).

French 2015 Intelligence Act Loi n° 2015-912 du 24 juillet 2015 relative au renseignement, url: https://www.legifrance.gouv.fr/codes/id/LEGISCTA000030934655/ (Accessed May 5, 2021).

French Civil Code Code Civil (1803/03/08). Loi n° 70-643 du 17 julliet 1970, url: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006419288/ (Accessed May 5, 2021).

G-10 Act Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10), 26 June 2001, url: https://www.gesetze-im-internet.de/g10_2001/BJNR125410001.html (Accessed May 5, 2021).

GDPR Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal L 119, 04/05/2016, pp. 1–88.

Genocide Convention The Convention on the Prevention and Punishment of the Crime of Genocide Approved and proposed for signature and ratification or accession by the General Assembly of the United Nations, resolution 260 A (III) of 9 December 1948, in force since 12 January 1951, in accordance with article XIII.

Grundgesetz 1949 The Basic Law for the Federal Republic of Germany. Parlamentarischer Rat, Grundgesetz für die Bundesrepublik Deutschland: Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das durch Artikel 1 des Gesetzes vom 13. Juli 2017 (BGBl. I S. 2347) geändert worden ist (1949), url: http://www.gesetze-im-internet.de/gg/BJNR000010949.html (Accessed May 10, 2021).

NIS Directive Also known as Cybersecurity Directive. Cybersecurity Directive Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Brussels, 6 July 2016.

RIPA The Regulation of Investigatory Powers Act (2000 c.23) (RIP or RIPA), Act of the Parliament of the United Kingdom, 28 July 2000, url: https://www.legislation.gov.uk/ukpga/2000/23/contents (Accessed May 10, 2021).

TEU European Union, Treaty on European Union (Consolidated Version), Treaty of Maastricht, 7 February 1992, Official Journal of the European Communities C 325/5; 24 December 2002.

Treaty of Lisbon European Union, Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, 13 December 2007, 2007/C 306/01.

UDHR The Universal Declaration of Human Rights (General Assembly Resolution 217 A), proclaimed by the United Nations General Assembly in Paris, 10 December 1948, url: https://www.un.org/en/about-us/universal-declaration-of-human-rights (Accessed May 10, 2021).

Legal Cases

Abernethy *v.* Hutchinson 1825, UK. Case number 47 E.R. 1313 (3 L. J. Ch. 209), High Court of Chancery, June 17, 1825, url: https://vlex.co.uk/vid/abernethy-v-hutchinson-802914393 (Accessed March 10, 2022).

Fu Qiang *v.* Union Press 2000, China. Also known as Fu Qiang *v.* Huaxia Times, Jinan Lixia District People's Court, June 3, 2000, cited after Yang (2008, p. 64).

Funes *v.* Instagram 2012, USA. Case number No. C 12-06482 WHA, United States District Court for the Northern District of California, December 21, 2012 (published January 24, 2013), url: https://casetext.com/case/funes-v-instagram-inc (Accessed March 10, 2022).

Griswold *v.* Connecticut 1965, USA. Case number 381 U.S. 479 (85 S. Ct. 1678), U.S. Supreme Court, June 7, 1965, url: https://casetext.com/case/griswold-v-state-of-connecticut (Accessed March 10, 2022).

Klass *v.* Germany Case number 5029/71, Council of Europe: European Court of Human Rights, September 6, 1978 , url: https://hudoc.echr.coe.int/fre?i=001-57510 (Accessed May 19, 2021).

Lawrence *v.* Texas 2003, USA. Case number 539 U.S. 558 (123 S. Ct. 2472), U.S. Supreme Court, June 26, 2003, url: https://casetext.com/case/lawrence-v-texas-6 (Accessed March 10, 2022).

NAACP *v.* Alabama 1958, USA. Case number 357 U.S. 449 (78 S. Ct. 1163), U.S. Supreme Court, June 30, 1958, url: https://casetext.com/case/national-association-for-advancement-of-colored-people-v-state-of-alabama-patterson (Accessed March 10, 2022).

Niemietz *v.* Germany Case number 13710/88, Council of Europe: European Court of Human Rights, 16 December 1992, url: https://hudoc.echr.coe.int/eng?i=001-57887 (Accessed May 19, 2021).

Prince Albert *v.* Strange 1849, UK. Case number 41 E.R. 1171 (EWHC Ch J20), High Court of Chancery, February 8, 1849, url: https://vlex.co.uk/vid/between-his-royal-highness-802701749 (Accessed May 19, 2021).

Rodriguez *v.* Instagram 2013, USA. Case number C 12-06482 WHA, United States District Court for the Northern District of California, May 14, 2013, url: https://casetext.com/case/rodriguez-v-instagram-1 (Accessed March 10, 2022).

Roe *v.* Wade 1973, USA. Case number 410 U.S. 113 (93 S. Ct. 705), U.S. Supreme Court, January 22, 1973, url: https://casetext.com/case/roe-v-wade (Accessed March 10, 2022).

Saravia *v.* Germany Also known as Weber and Saravia *v.* Germany (dec.). Case number 54934/00, Council of Europe: European Court of Human Rights, June 29, 2006, url: https://hudoc.echr.coe.int/fre?i=002-3235 (Accessed May 19, 2021).

Shi Zhaohui *v.* The People's Daily 1995, China. Cited after Yang (2008, p. 64).

Shimovolos *v.* Russia Case number 30194/09, Council of Europe: European Court of Human Rights, June 11, 2011, url: https://hudoc.echr.coe.int/fre?i=001-105217 (Accessed May 19, 2021).

Wu Jing (Ms. Liu) *v.* Guangdong Newspaper 2003, China. Guangdong Zhongshan Intermediate People's Court, December 21, 2005, cited after Yang (2008, p. 65).

Xiaoli (Alias) *v.* The China Times 2005, China. Beijing Chaoyang District Court, July 17, 2006, cited after Yang (2008, p. 66).

Yovatt *v.* Winyard 1820, UK. Case number 1J (W394), cited after Bartczak (2013, p. 6).

Institutions and Organizations

BLAT	Bureau de la Lutte Anti-terroriste (FR)
BGH	Bundesgerichtshof, Federal Court of Justice (DE)
CCP	Communist Party of China
CJEU	Court of Justice of the European Union
CNIL	Commission nationale de l'informatique et des libertés (FR)
COP21	Non-Violent Action COP21 (also known as ANVCOP21, FR)
ECtHR	European Court of Human Rights
GCHQ	Government Communications Headquarters (UK)
ICJ	International Court of Justice
ICO	Information Commissioner's Office (UK)
NSA	National Security Agency (USA)

Introduction

Research problem and hypotheses

In this dissertation, I introduce the concept of *political privacy* and describe its relationship to the principles of democratic state. Although the political aspects of privacy have been the subject of many studies and analyses, including, to name but a few, those by Shklar (1989), Solove (2011a), Landau (2013), Verble (2014), Schulze (2015), and Zuboff (2019), the original contribution of this work is that political privacy is defined in the context of a full-fledged theory of privacy. The outcomes of my research in this area are relevant to political science, but extend onto the law and European policies concerning privacy and surveillance as well. Additionally, the theory of privacy that I use also constitutes a novel proposal, which is likely to be of value to solving problems in philosophy, ethics, political theory and legal theory.

The topic of this dissertation has been increasingly gaining public attention ever since I started my research in 2014. Initially, the scandal which followed the Snowden case of 2013 was thought to be contained to the US and the European data and privacy protection policies seemed to have been headed in a direction very different from where we are today. Soon, it turned out that mass surveillance concerns the Europeans as well, and unless Europe wants to share the fate of the US, it has to catch up. In chapter 2 in section 2.3.5, I discuss how the moral panic surrounding the spying practices of the NSA brought about the European renaissance of privacy protection, of which the GDPR is but one result. Currently, the problem of privacy lies at the very center of the debate about the future of European democracies, having become a determinant of compliance with the rule of law, as opposed to discretionary government power.

One of the most critical problems in privacy debates was that, as I explain in detail in section 1.3.3, stakeholders use incompatible definitions of privacy to justify their arguments, causing conceptual inconsistencies at all level of discussion. Attempts to define the meaning of "privacy" have been overall unsuccessful, failing to address social

and political conflicts or explain the share of the state in citizens' oversight (see 1.2). Some, like Snowden, even went so far as to conclude that privacy is "somewhat empty", "essentially indefinable, or over-definable", that everyone has their own "privacy" and there is not much that can be done about it (Snowden, 2019, pp. 207-208). First and foremost, in this dissertation I contradict this view.

I claim that privacy is in fact definable. In section 1.3.6, I propose a novel theory of privacy, which I call *the gateway theory of privacy*. Not only does the gateway theory show that privacy can in fact be characterized, but it satisfies the conditions which I put forth for a politically relevant theory of privacy. First, the core of the gateway theory of privacy is independent of terms strictly related to the current state of technology. In my account, I only require that we develop intuitions concerning the notion of a *zone of activity* (see section 1.3.6), a collection of behaviors or relationships which people engage in as they live their everyday lives. Second, the framework of the gateway theory focuses not on the means of privacy protection, but around the ultimate value to which privacy is instrumental – human life, dignity and activity. Third, the gateway theory is by design cross-disciplinary and uniform throughout contexts and cultures, but allows for expressing the individual, group and cultural variations in the perception of privacy. Fourth, it allows for differentiating between individual and social (or communal) discovery of person's life and the discovery conducted by the state. I use this feature to specifically address political aspects of privacy later on. Finally, the gateway theory allows for abstracting away from those social, political and economic convictions which are not fundamental to the concept of privacy.

Having obtained a new theory of privacy, I use it to define *political privacy* (section 1.4). In the subsequent chapters, I am interested primarily in how political privacy, as opposed to privacy *sensu largo*, interacts with surveillance, especially mass surveillance, as well as with democratic principles and institutions. Aside from the notion of privacy, central to my work are the concepts of (mass) surveillance and democracy.

After Houston (2017, p. 3) and Privacy International, I take *mass surveillance* to mean "the subjection of a population or significant component of a group to indiscriminate monitoring". By this token, any system which generates and collects data on individuals without attempting to limit the dataset to well-defined targeted individuals is a form of mass surveillance.

Democracy is operationalized as in the democracy measurement methodology of the Varieties of Democracy (V-Dem), including seven principles, which characterize a democracy: the electoral principle, the majoritarian principle, the consensual principle, the liberal principle, the participatory principle, the deliberative principle, and the egali-

tarian principle. Each of these is explained and put in the context of political privacy in section 5.1.1. The principles proposed by Teorell et al. (2019) are based on, though not identical to, those in the theory of polyarchy by Dahl (2008).

My second central claim, aside from a proposal to consider privacy definable and adopt the gateway theory of privacy, is that political privacy is of special importance to democratic principles and institutions. In chapter 5, I list examples of such institutions, and I make policy recommendations regarding the development of European privacy and surveillance solutions.

The specific research questions (Q) and hypotheses (H) which I engage with in this dissertation are defined below in connection with each of the chapters.
Chapter 1:

(Q1) Which theory of privacy is appropriate to handle the conflict of values between the advocates of mass surveillance and privacy-oriented citizens?
(H1) The existing theories of privacy are not sufficient to facilitate a conversation on privacy and mass surveillance.
(H2) A novel theory of privacy based on desiderata specified in section 1.1 allows for creating a more informative map of the conflict of values in (Q1).
(Q2) How is political privacy different from personal privacy? How to conceptualize the difference between them using the gateway theory of privacy?

Chapter 2:

(Q3) What are the main legal models of privacy regulation?

Chapter 3:

(Q4) What is the position of the right to privacy among other human rights?
(H3) The right to privacy includes, in addition to being an individual rights, a collective aspect, justifying its extension to include a collective right to privacy.
(H4) The right to privacy, and especially political privacy, protects collective social and political agendas, examples of which are given in section 3.2.1.

Chapter 4:

(Q5) How does political privacy relate to surveillance capitalism, as defined by Zuboff?
(Q6) Which aspects of psychology contribute to the current attitudes and expectations concerning privacy and surveillance?
(Q7) What is the efficacy of mass surveillance *v.* traditional investigative methods?

Chapter 5:

(Q8) How can we conceptualize the zones of political activity appropriate for the three privacy protection thresholds defined in chapter 1?
(Q9) How does privacy contribute to the protection of democratic institutions?
(Q10) What role does surveillance, especially mass surveillance, play in human rights abuses, oppression of minorities and genocide?
(H5) There exists a close connection between political privacy and democratic principles. This connection translates into the fact that privacy protection tools and methods, including those described in section 5.3.4, contribute to the condition of democracy.

Methodology

In this dissertation, I rely on a variety of methods, including those typical of political science, as well as relatively new theoretical tools, popularized by the philosophical movement called conceptual engineering, which originated from modern analytic philosophy. I also use methods from law and legal theory, especially in chapter 2, where I analyze the legal frameworks behind privacy regulations in the EU, including France and Germany, the US and China.

Although my work is primarily focused on political theory (Dryzek et al., 2008), it contains issues where methods from comparative politics (Boix and Stokes, 2007) and international relations are relevant. From chapter 2 onward, I develop and assume three models of regulating privacy, all of which are obtained through *comparative model building*, a process which requires a comparative approach to the history and decisions of respective national and federal institutions. In some parts of this dissertation, for instance, where the international reaction to the practices of the NSA is described, knowledge of international relations is necessary to be able to make sense of the conditions involved in the case, as well as its consequences. The emergence of the EU model of regulating privacy was partly a reaction to the abuses of the American system of surveillance, made public by Edward Snowden and many more whistleblowers after him. Thus, the situation in Europe cannot be fully understood unless the US is taken into consideration as well.

The choice of case countries followed from the focus of the main research question. Since I was primarily interested in the relationship between the political aspects of privacy and democracy as such, it was necessary to consider the widest possible spectrum

of privacy regulation models. Authors such as Shipler (2011) have linked the limitations in citizens' privacy to an increase in undemocratic discretionary action of governmental power. Mass surveillance and surveillance in general are closely related to the right to search and seize, which Shipler argued was bound to be abused following the 9/11 attacks. In case of the US, he proposes that the constitutional guarantees of freedoms be treated as hard boundaries for public authority, without exceptions:

> Take a few steps from the Constitution and you will find yourself in the twilight of crime-ridden neighborhoods where cops frisk pedestrians and search cars without warrants, on the officer's sole determination that they have reasonable suspicion or probable cause. Their actions may be reviewed by the courts, so you can still watch government at work, but dimly. (Shipler, 2011, p. xxvi)

Although Shipler begins his considerations of privacy from Judge Cooley's notion of "the right to be let alone" (see section 1.2.1 for more details), which in today's world is already obsolete, he makes valid observations concerning constitutionality of searches without consent, frisking pedestrians, profiling citizens and using what he calls "secret suppression" in the US. Cases such as those analyzed by Shipler suggest that ubiquitous policing and surveillance, especially mass surveillance, is the point where the power of the people gives way to arbitrary government, thus violating democratic principles through loss of privacy. The countries chosen for comparative analysis in this dissertation took very different approaches to the problem of ubiquitous surveillance and government surveillance (the two being different because private firms working on surveillance capital, as well as smaller private and public entities, also engage in surveillance on a large scale). These stances adopted by China, the US and the EU, stemming from collective observation of social and political consequences of the early experiments with surveillance and national security, have developed into legal and political paradigms of how to balance privacy and surveillance.

In this landscape, China represents a stance of overt rejection of political privacy. The model of regulating privacy derived from the Chinese law and political practice is guided by what I called Big Brother principle (see section 2.5) and a complete removal of political privacy from the scope of privacy protections. Although China is not a democratic state, the model of privacy regulation used by the CCP and the Chinese government offer important insight into the role of privacy violation in the decline of democratic values, such as the freedom of election, freedom of speech, respect for minorities, and many others. Because of this fact, China is included in the three main models which I build in chapter 2, and specific cases relate to the Chinese model come

up in relation to multiple other privacy-related themes in subsequent chapters. Another aspect of the Chinese case, which makes it valuable for my work is that privacy regulations and limitations in China are usually communicated in an overt, official way. As section 2.4 will show, Chinese authorities do not bother making their methods and scope of operation a secret, which means that no whistleblowers' accounts are needed to get a relatively comprehensive picture of the state of surveillance and *de facto* privacy protection in this country. This opportunity allows for comparing what we know about European and US surveillance and privacy with a sort of "maximum" case, where no democratic institutions exist to protect political privacy.

The second case which I chose for model building is that of the US. I called the model of privacy regulation derived from American law and political practice *minimal*. This is because although the US government has no effective way to stop or challenge the public scrutiny of their surveillance programs after the revelations of 2013 (see section 2.3), or to do away with their conflict with the US Constitution and democratic principles, the trends in data protection with respect to surveillance capital market mark an overall positive attitude to mass surveillance, including surveillance and other forms of data collection aimed at generating profit and profiling. The state is then able to obtain any necessary information from the firms operating on data, which effectively expands the intelligence capacity of the US government onto all information gathered by the private market.

Finally, the third case is the EU, whose model of privacy regulation completes the list of paradigmatic approaches to privacy and surveillance. The EU differs from the US and China in many ways, including the fact that European decision-making is more distributed, hence no "federal" laws can be imposed on the member states concerning privacy and surveillance, as is the case in the US. Many of the member states are established democracies, which allows for a positive interaction between political privacy and democratic principles, distinguishing the EU from China. In turn, European citizens have more tools at different levels of organization, including local, national, regional and European, to combat undemocratic privacy violations, which makes their situation completely different from that of US citizens. Europeans entertain, on top of their own constitutional guarantees, a range of protections from data protection authorities (DPAs), ombudspeople, the ECHR and a number of EU bodies. And even though the application of these protections into law often falls short of delivering justice, European citizens have a documented history of making effective use of them (see section 2.1.3). However, the EU policies of privacy regulations are far from perfect. In section 4.4 I list a number of problems of current European approach to surveillance, security

and political privacy, indicating viable ways of solving them in section 5.3.

Because the description of the European model would not be complete without showing how the regulations interact with national privacy and surveillance laws, I include the case of France and Germany – two member states whose regulations of privacy are at the opposite sides of the spectrum, and which are also indicative of the friction between privacy-oriented and surveillance-oriented trends among the EU members. The cases of other states, including Poland are not discussed in this dissertation, because they typically fall somewhere in between the German and French privacy regulation model. For instance, Poland probably falls close to the French model, especially considering recent illegal surveillance scandals, such as that surrounding the use of Pegasus spying software (Nyzio, 2022), the rising over-regulation of security, and unproportional anti-terrorist initiatives (Soler and Górka, 2017). Hence, including Poland instead of, or even next to France and Germany, would not add much to the general point I am making about the existence of three paradigms of privacy regulation. Moreover, the legal aspects of privacy protection in Poland have already been widely analyzed by, to name but a few, Szpor (2000), Frączek (2013), Kuczma (2017), Chmielarz (2019), and Łakomiec (2020).

Aside from comparative study of privacy regulations in the EU, the US and China, I make use of techniques developed within conceptual engineering. Conceptual engineering is a philosophical movement, which acknowledges the constitutive power behind concept making, as opposed to the traditional approach, typical of analytic philosophy, of taking as the central point of reference the natural sciences and assuming that all relevant concepts are merely *discovered*, and not *created* by the scientists and scholars involved in the process of theorizing about a specific phenomenon.

In both law and political science, similarly to other social sciences, key concepts are often not rooted in physically tangible, observable phenomena. More importantly, legal theorists and political scientists are responsible not only for providing accurate descriptions of the observations of social and political reality, but also for creating workable theories and concepts, which have the potential for spurring social progress and promoting understanding of the conflicts surrounding established liberties and freedoms such as the right to privacy. Koch (2021, p. 1956) summarized the aims of conceptual engineering as follows:

> Conceptual engineering is typically described as a means of achieving at least two goals at once: the semantic goal of changing what certain terms or expressions mean in a language, and the practical goal of effecting certain real-world changes, such as changes in linguistic practices or people's classificatory behavior.

In my work, I postulate that the concept of privacy is one which is adaptible, that is, what "privacy" means is eligible for revision whenever the existing definitions fail to protect its target values – people, relationships and activities – in a new context. Similarly as is the case with the concept of democracy (Coppedge et al., 2021, p. 4), interpretations of privacy do not have an unlimited scope. In particular, the concept of privacy cannot be knowingly misinterpreted and still produce democratically valid regulations. Contrary to this, the attempts to restrict the right to privacy in this way are now observed in all case countries, which I consider in chapter 2.

Conceptual engineering of privacy has already taken place within the surveillance capital community. The conceptual transformations of terms such as "client", "user", "service", as well as the deflated notion of consent and agreement in so called "user agreements", which I describe in section 4.1 are in reality nothing other than engineered meanings of concepts, which we had been familiar with, but which have been re-designed to make our intuitions align with the business models of surveillance capital firms. We need novel conceptual solutions capable of dealing with privacy-related problems in a systematic way. Zuboff referred to this strategy as "naming and taming", and pointed out that:

> The point for us is that every successful vaccine begins with a close understanding of the enemy disease. The mental models, vocabularies, and tools distilled from past catastrophes obstruct progress. We smell smoke and rush to close doors to rooms that are already fated to vanish. The result is like hurling snowballs at a smooth marble wall only to watch them slide down its facade, leaving nothing but a wet smear: a fine paid here, an operational detour there, a new encryption package there (Zuboff, 2019, p. 62).

In the meantime, conceptual engineering has been identified as a way to "fix" language by creating new concepts, which would still be legitimately connected with our past intuitions, received a lot of attention from scholars. It has proved to be a methodologically novel and powerful way to break away from the normative *v.* descriptive dualism, adding value to all disciplines where ethical considerations play an important role in progress. This includes not only philosophy, but also technology, medicine, political science, sociology, and many others. Following the basic tenets of conceptual engineering, I assume that concepts such as privacy and democracy are ultimately *representational devices*, which require fixing and fine-tuning when they turn to be defective (Cappelen, 2018, p. 3).

The term "conceptual engineering" has first been used by Blackburn (1999), but other forms of referring to the same approach to conceptual work have been present in

Haslanger's work on race and gender (as "ameliorative projects) and Burgess and Plunkett's "conceptual ethics" (Haslanger, 2000; Burgess and Plunkett, 2013; Plunkett and Burgess, 2013). In this disseration, conceptual engineering is of particular importance in chapter 1, where I design a novel theory of privacy and connect it to historical accounts analyzed in section 1.2.

Aside from the comparative method and the theoretical framework of conceptual engineering, I use a range of methods from *analytical political theory*, a movement, which Blau (2017, pp. 14–16) characterized as involving the following assumptions:

- even in political theory, researchers may need to engage with empirical research; in case of my research problem, empirical research using big collections of data, as well as measurement indices for evaluating, for instance, the efficacy and scope of censorship and surveillance;
- in political research, it is common that researchers might not know about, or be using a method or an approach that would positively contribute to the research problem at hand help us, thus expansions of methodological toolkit should be an available option; in this dissertation, such expansion happens through intentional use of conceptual engineering in chapter 1;
- political research should be problem-driven, starting with a clear social or political problem, which requires theoretical attention in order to be solvable, or at least more approachable; in this work, the originator problem is the conflict between democratic principles and mass surveillance of citizens, as performed in the recent years by authorities of both established democracies and non-democracies.

Over the course of my work on the problem of political privacy and surveillance, I did my best to adjust to the advice by Goodin (2017, pp. 18–19) on how to write analytical political theory, including submitting early versions of my findings to be presented and discussed as widely as possible and eliminating unnecessary cases and information from my the main line of the argument concerning privacy and democracy. The latter also justifies my decision to rely on an already established notion of democracy in the form of V-Dem's seven principles, instead of theorizing about democracy alongside privacy. In case of the aforementioned originator problem, the need for theoretical contributions arises around the point of defining privacy – that is, it is not clear how to interpret "privacy", although this choice has major impact on the arguments which can and cannot be formulated in the public debate about privacy violations – and not in that we lack intuitions on how to understand democracy in that same context.

Also in agreement with Goodin (2017, p. 18), the key distinctions in this dissertation

can be treated as arguments, though some are more defeasible than others. In case of the distinction between political privacy and its remaining elements, there is little room for negotiation in how my argument is structured. Since my primary claim is that political privacy is uniquely connected with democracy, and that it needs additional, special protection, its existence is necessary for everything that follows. This of course does not mean that I postulate a sharp division between personal privacy and political privacy. As I will argue, political organizations cannot exist without individuals, and the success of political endeavors ultimately depends on the state respecting individual rights and freedoms of people who undertake these initiatives. The gateway theory of privacy, which I developed in section 1.3, has become a useful interpretative framework where political privacy can be defined in a relatively intuitive way, making it easier to apply.

Aside from conceptual analysis, which I use extensively in the initial segment of chapter 1 in order to understand how the concept of privacy was used in law, politics and ethics in the past, I make use of the following theories and framework related to analytical political theory: positive political theory, contractualism, reflective equilibrium, and interpretation of legal and political texts.

Positive political theory is a part of political theory, which comes into play when an attempt to go beyond description and normative analysis is made. Hamlin (2017, p. 193) said that "the ubiquity of positive political theory sometimes renders it invisible", but at the same time provides us with "explanations of political phenomena and behavior that are both crucial to our understanding of politics and essential to our normative discussion". In case of this dissertation, I tried to go beyond comparing what the particular governments and institutions do *versus* what they *should* be doing. Thus, I focused on the essential components of democratic state and show their connection to the zones of citizens' activity, which are made possible through privacy protection, or those which are crucially dependent on it.

Helping with this is *contractualism*, a method which allows me to address specific normative questions within moral and political philosophy *via* considering a group of idealized agents, who may choose to accept or reject particular solutions under specified conditions or constraints (Quong, 2017, p. 65). The conditions that I put forward are, in case of citizens, a willingness to see the seven principles of democratic state satisfied at least in the minimum. On the side of the governments, surveillance agencies and surveillance capitalist firms, I assume that they act and set their agendas according to the specific logic of operation, to which each category of stakeholder is committed. For instance, I follow Zuboff in considering surveillance capital as a form of economic

power which adheres to a knowable, describable trend emerging from, roughly, neoliberal economy and regulatory vacuum (see section 4.1).

The method of reflective equilibrium, a tool which allows bringing principles and judgments into a kind of agreement, is something that I adopt from Solove (2021) in claiming that the so called "privacy paradox" does not give rise to a valid anti-privacy argument. Solove characterized the "privacy paradox" a situation where respondents claim that they value privacy highly, but act in a way which stands in contradiction to their declared belief. In this case, a principle of respect for privacy is in an apparent conflict with the judgments made in contexts such as using the social media ran by surveillance capitalist firms, buying technology known to have a government "back door", and so on. Solove shows that there exist many factors other than the support for the general principle, which contribute to the final judgment in each situation. Similarly, I assume that there may exist a range of contributing causes behind people's everyday choices regarding privacy and surveillance.

Finally, there are methods, which appear in this dissertation indirectly, but without which many arguments which I make would not be successful. Studies and analyses appearing in sections 4.4.2 and 5.1.2, for instance, use quantitative and qualitative data analysis, and involve hypotheses which are testable only within data-rich environments. Historical institutionalism, rational choice theory and qualitative methods, such as surveys and opinion polls, also feature in many of the studies which I refer to. Because the general argument about political privacy that I am making is built upon these individual findings, the methods necessary to obtain them are just as relevant to the conclusions of my work.

Overview of the chapters

This dissertation deals with a variety of topics and themes, often requiring a separate review of literature and state of the art research. Hence, no general literature review will be summarized, either here in the introduction or later on. All relevant sources are mentioned in relation to specific questions and claims, which I take on as my arguments progress. This has an additional advantage of having produced little to no theoretical surplus. That is, every study and theory, which appear in the text are relevant to the main argument.

In chapter 1, I inspect the historical theories of privacy and propose a novel account of privacy in the form of the gateway theory of privacy. Based on the gateway theory, I then develop the concept of political privacy in section 1.4.

In chapter 2, I use comparative model building to derive three paradigmatic approaches to privacy regulation based on three case studies: the US, China, and the EU (with France and Germany as examples within the EU).

In chapter 3, I show that the right to privacy has a dual nature. On one side, it protects the individual, unique lives and freedoms. On the other, it protects collective agendas, which are necessary from the democratic perspective. I examine case studies of violation of privacy, which did demonstrable damage to valid social or political agendas.

In chapter 4, I discuss how political privacy relates to global economics and public security, relying on the notion of suveillance capitalism as defined by Zuboff (2019). The considerations about the psychological aspect of privacy are combined with the recap of the state of mass surveillance, both in terms of technical and technological efficacy, financial viability and the resulting rise in public security.

Finally, in chapter 5, I combine the thresholds of political privacy protection with the seven democratic principles. Next, I discuss limits to surveillance which ought to be satisfied to give minimal protection to democracies. I also make several policy recommendations concerning the European approach to surveillance and privacy regulation.

Acknowledgements

I would like to thank prof. Andrzej Mania and prof. Marek Bankowicz for giving me valuable feedback on the early versions of the gateway theory of privacy. Dr Paweł Sękowski, prof. Olivier Forcade and prof. Rainer Hudemann provided me with insightful remarks on how to improve my research on privacy in the context of migration. My thanks go the organizers of the Multidisciplinary Workshop on Migration in Kraków for giving me an opportunity to discuss my research in February 2017.

I also would like to thank the organizers of the essay contest "Beyond Polish and Ahead of Hungarian Presidency of the Visegrad Group" for awarding me the first place for my paper "Citizens' cybersecurity in the Visegrad Group. The role and progress of the V4 countries in protecting the right to privacy related to mobile and digital communication and information", and allowing me to present it at the V4 Youth Forum in Budapest in May 2017.

I developed my work on privacy and security thanks to the audience of the 18th Ethical Forum of the University Foundation "Academics as soldiers? Is defence-related research a scandal or a duty?" organized by the University Foundation in Brussels in December 2019. Special thanks to members of the Royal Military Academy, who provided

me with valuable insights concerning the attitudes within the Belgian and European defense and security sectors.

My interest in approaching the problem of fake news from the perspective of public security is due to my conversations with prof. Philippe Van Parijs, who was the first to ask me whether fake news constituted a cyber threat. I later worked on this issue during my stay with the Media, Policy and Culture Research Group Seminar at the University of Antwerp in the Spring/Summer semester of 2021. Many thanks also to my mentors during this stay, prof. Sean Phelan and prof. Pieter Maeseele, for giving me a platform to discuss my ideas on fake news and security.

Here, I also want to thank the organizers of Hack Belgium hackathon in March 2019 and my team, Ben Bornemann, Abali Essende, Gaetan Henry, Stéphanie Michaux and Danny Moeuthwil, with whom we won first place in the category "Credible, Engaging Media", for showing me that citizens can come up with meaningful ways to solve public security problems. The fact that our idea for a "credibility layer" to links shared online was independently implemented by some of the social media platforms shows that viable solutions to serious political problems can sometimes be thought up in three days by a small group of committed people with varied skill sets.

Lectures and feedback from prof. Stefaan Fiers improved my understanding of European lobbying, showing me that informed policy-making requires a third-person view, where all stakeholders with legitimate interest are treated in an unbiased way. Although in this dissertation I do not focus on interest groups, my experiences during the scholarship at KULeuven (Katholieke Universiteit Leuven) allowed me develop a clearer view of my research problem. Up to a certain point in my research on privacy and security, I had no idea whether my findings will confirm my personal intuitions and convictions. As it turned out, in many cases my beliefs had to be revised.

Many thanks to the open source community, especially to my friends and colleagues from FOSDEM *Free and Open Source Software Developers' European Meeting* in Brussels. Over the years of my engagement with open source initiatives I had the pleasure to talk to many talented and selfless individuals who contribute their time and code to various causes, often without much thought on how to best monetize their ideas. Fediverse is one free and open source project which supports democracy through web decentralization, and which provided us with a working alternative to surveillance capital-owned social media platforms. Tor is another open source, free technology, which protects millions of people from oversight and political prosecution every day. Thanks to the members of open community everywhere democracies are already well-equipped to fight back the discretionary power of their governments. The open source community is also

a force which counters the claim that surveillance and passivity are the price which we have to pay for participation in technologies. Our democratic future lies in open source.

An important component of my methodology involving conceptual engineering was discussed with the participants in the workshop "Conceptual Engineering and Socially Disruptive Technologies", organized in March and April 2022. I thank everyone who contributed their questions and points for discussion following my talk. I also thank Anna Szklarska and Szymon Helma, who read and commented on multiple versions of my work during research seminars at the Jagiellonian University.

To my supervisor prof. Dorota Pietrzyk-Reeves who encouraged me over the course of my research and saw value in my work even when I myself doubted whether to continue – thank you. Without your support and dedication this dissertation would never be completed.

I want to thank my partner Juliusz for being the first reader of my work and often the first person to discuss my ideas. Last but not least, I want to thank my mother, Małgorzata, and my friends, Karolina, Zofia, Katarzyna, Martyna, and Agnieszka, for their continuous support of my research and for their presence in my life.

Chapter 1

From the general theory of privacy toward political privacy

1.1 Criteria for the political theory of privacy

Despite its growing importance in politics in the recent years, the question of privacy remains understudied in political science. As I will argue in section 1.3.4, the results of this neglect are catastrophic to the civil society, because no reliable theoretical framework exists, which would allow the (often silent) majority of citizens to express their preferences and join the power struggle among the already organized stakeholders. Currently, the average citizen is presented with two choices. The first is to claim that privacy is a natural right of an individual and fully subscribe to the fundamental postulates of liberalism. This path is problematic, because, at least for some, a commitment to individual liberty over dedication to their community creates an undesirable landscape of social reality. But then, why would the only alternative to this stance be to authorize full governmental surveillance of citizens' behavior? The second alternative available to citizens is just that – a choice to cede the right to privacy, leave no aspects of their lives unobserved, in other words, have "nothing to hide".

In this dissertation, I will argue that the primary reason why citizens are forced to oscillate between these extreme attitudes is not because national security and freedom are mutually exclusive. Rather, the issue is that there exists no theory of privacy which allows the citizens to formulate the claims to protect their privacy from mass surveillance and other forms of governmental infringement without accepting a comprehensive ideology of liberalism and individualism, including social, cultural and economic attitudes, which many citizens find unacceptable. In the words of Edward Snowden:

> In contemporary life, we have a single concept that encompasses all this negative or potential space that's off-limits to the government. That concept is "privacy." [...] The word "privacy" itself is somewhat empty, because it is essentially indefinable, or over-definable. Each of us has our own idea of what it is. "Privacy" means something to everyone. There is no one to whom it means nothing. It's because of this lack of common definition that citizens of pluralistic, technologically sophisticated democracies feel that they have to justify their desire for privacy and frame it as a right. (Snowden, 2019, pp. 207-208)

In the light of this statement, the ultimate goal of this thesis is to bring privacy out the realm of indefinability or over-definability, based on an expectation that a common definition of privacy will be a tool which the citizens may use to their advantage in their quest to stop mass surveillance or other forms of government privacy violation. Moreover, this tool should be compatible with the varied intuitions citizens have concerning personal privacy and other areas which shape their individual and communal lives, including views on the economy, social structure and domestic politics.

The list of basic requirements with respect to the theoretical framework supporting the notion of privacy which I propose is as follows:

(a.) the core of the framework must be independent of terms strictly related to the current state of technology;

(b.) the framework must be centered not around the means of privacy protection, but around the ultimate value to which privacy is instrumental, that is, human life, dignity and activity;

(c.) the framework must support a theory which is cross-disciplinary and uniform throughout contexts and cultures;

(d.) but must at the same time allow for differentiating between individual and social (communal) discovery of person's life and the discovery conducted by the state;

(e.) the resulting theory must allow for abstracting away from those social, political and economic convictions which are not fundamental to the concept of privacy.

As for (a.), I will argue that, despite the tech industry trying to convince us of the contrary, technology does not change much in the concept of privacy. Our expectation of privacy depends significantly on culture and social-economic circumstances, but it does not depend on whether we use a smartphone or not. Moreover, even the fact that we rely on technologies which perceptibly infringe on our privacy does not mean that

we accept the infringement (Solove, 2021). A good theory of privacy must allow non-technologically fluent citizens to fight for their rights without mastering the specific language of technological progress or narratives of national emergency.

Related to this is (b.), which states that the concept of privacy suitable for wider public debate must not revolve around intermediary concepts, such as information. A step in the right direction was taken by Moor (1991), who proposed that instead of protecting information, we talk about protecting "situations" from happening in the public eye. I take this initiative a step further by requiring that the theory of privacy focuses on what privacy ultimately protects, that is, zones of personal activity which constitute our family, work and social life. In doing this I acknowledge the instrumental character of the right to privacy and postulate that privacy be seen as a necessary means of protection of human life. In other words, privacy regulates the relationship between shared and restricted realms of personal activity, in which it bears certain (though limited) resemblance to ownership of property. Further parallels between privacy and property will be drawn and explained throughout this dissertation (see section 1.4).

The requirement posed in (c.) addresses one of the most difficult aspects of defining privacy, that is the fact that it appears as a central problem in an overwhelming range of disciplines, including, just to name a few, health care and nursing (Mlinek and Pierce, 1997; Bäck and Wikblad, 1998; Leino-Kilpi et al., 2001; Lemonidou et al., 2003; Petronio et al., 2004; Malcolm, 2005; Appari and Johnson, 2010; Liang et al., 2011; Avancha et al., 2012; Al Ameen et al., 2012; Zhou et al., 2014; Patil and Seshadri, 2014), developmental and general psychology (Garbarino, 1977; Berscheid, 1977; Parke and Sawin, 1979; Altman et al., 1981; Newell, 1995; Van Manen and Levering, 1996; Barbopoulos and Clark, 2003; Bersoff, 2008; Smith et al., 2011), child advocacy (Feshbach and Feshbach, 1978; Melton, 1987, 1983; Jackson, 2004), data analysis (Du and Atallah, 2001; Clifton et al., 2002; Wang et al., 2005; McSherry, 2009; Hardt and Rothblum, 2010; Mohan et al., 2012; Wu et al., 2013), communication and social networks (Chen and Rea Jr, 2004; Gross and Acquisti, 2005; Zhou and Pei, 2008), job performance and satisfaction measurement (Duvall-Early and Benedict, 1992).

Considering this plurality of occurrences, can privacy be defined uniformly across disciplines? In section 1.2, I present historical attempts at creating a cross-disciplinary theory of privacy together with their criticism. Subsequently in section 1.3, I present a novel theory of privacy that allows for explanations related to various zones of personal or group activity, which fit into a multi-disciplinary context. The proposed definition of privacy, although general, easily lends itself to the specific fields of application, regardless of their scope or relation to technologies.

As for the variance in approaches to privacy across cultures, the theoretical framework which I propose allows for expressing in terms of the same theory different *philosophies of privacy* accepted by various cultural communities. Therefore, the framework itself does not enforce a range of decisions in specific cases, but instead allows for formulating plausible justifications for making a particular decision with respect to the protected zone of activity, *e. g.*, a relationship (I introduce the concept of a zone of activity in section 1.3). Similarly, we may use the framework to explain the differences between approaches to privacy across cultures, or explain and interpret the motivations behind specific decisions concerning privacy protection or infringement in a particular situation.

One of the novel features of the theory which I advocate for is that it differentiates between various forms of oversight, including the difference between surveillance and sousveillance and between the oversight conducted by the state or its representatives and that by fellow citizens or communities. What motivates this requirement is an observation that countering state surveillance should not require that we give up the tendency to spy on our neighbors, friends and children. Such motivation may seem paradoxical initially, but upon closer inspection it presents itself as rather practical. Of course, one might always use the mechanisms of democratic governance to better oneself through oversight, but I argue that self-improvement should not be taken as a prerequisite for securing the rule of law, especially where citizen's have no influence on the shape of institutions of oversight and the availability of public choice in the matter.

Finally, (e.) requires that in considering privacy we are able to abstract away from irrelevant social, political and economic convictions. I will argue that privacy in its political dimension is not an inherently liberal notion. At its core, political privacy is available to everyone, as long they believe that the role of the state is to serve its people. Later in chapters 4 and 5 I reconcile political privacy with national security and the rule of law. By relying on the flexibility of the framework which I develop in this chapter, in my further considerations I exclude the purely personal aspects of privacy, such as, for example the discomfort of a person being photographed at a public event. Intuitively, personal privacy depends much more than political privacy on personal convictions and beliefs. Nevertheless, as I analyze the historical literature on privacy, cases concerning personal privacy are mixed, by necessity, with those related to public life and the relationship between the public and the state.

1.2 Historical theories of privacy in law, ethics and politics

1.2.1 Privacy as nonintrusion

One of the few unchanging elements of the public debate on privacy is the resentment towards various forms of technological development for facilitating privacy infringements. In fact, the very first version of the right to privacy discussed in the context of public activity was called "the right to be let alone" and is closely related to the history of technological progress of the photography industry.

In 1884 George Eastman revolutionized the photography market. The photographic plates, which photographers had carried around together with all chemicals needed to develop a picture, were replaced by gelatin-based paper film with the application of dried gel. The invention has been first introduced to the market in 1888, when Eastman's first camera, Kodak, was advertised with the words "You press the button, we do the rest". The Kodak consisted of a box camera together with 100 exposures which were later to be sent to the company and developed by a specialist (Coe and Gates, 1977). In 1900 the Eastman Kodak company introduced an easy to use camera called Kodak Brownie, the price of which was $1. From then on photography became available to the mass-market consumer (Jenkins, 1975), including children, as well as military service men who documented the events of WWI.

With the introduction of further inventions like flash bulbs and compact cameras, the Golden Age of photojournalism began. Following the standard set by the *Berliner Illustrirte Zeitung* in 1901, journals started printing photographs inside every issue, thus creating the modern news magazine format (Ganeva, 2008, p. 53). It was now not only possible to report in the form of an image the news of war, but also to take pictures of people attending theater plays, concerts or simply enjoying a walk down the street. And so, photojournalism faced all the same ethical dilemmas as regular plain-text journalism, among them, privacy concerns and discomfort of those who the photojournalists picked as their subjects (Thomson, 2019). From the most prominent masterpieces of photojournalism like the work of Riis of 1890 (Riis, 2018, 1971) to the daily press coverage of the local cultural events, photographs available in the press were the source of fear of surveillance and anxiety of having one's private life become the object of public attention (Twigg, 1992, pp. 307-308). It was believed that, as Warren and Brandeis (1984, p. 76) put it:

> Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make

> good the prediction that "what is whispered in the closet shall be proclaimed from the housetops." For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private and the evil of the invasion of privacy by the newspapers, persons; long keenly felt, has been but recently discussed.

Quite in line with their times, Warren and Brandeis treated a violation of privacy primarily as a type of spiritual harm, which is not reducible to mere material damages caused by the fact of having one's images made public. Rather, they viewed the violation of privacy as far more damaging than bodily injury, because the mental pain and distress caused by the inability to withdraw oneself from the public attention make the individual incapable of handling the growing complexity of everyday life (Warren and Brandeis, 1984, p. 77). In other words, their approach to privacy stated that an individual stripped from their privacy is no longer able to meaningfully partake in social life and maintain control over their own everyday affairs.

In order to introduce privacy violation into the legal discourse, Warren and Brandeis make use of the classification of personal rights introduced in rulings and published later by Cooley (1906). The aforementioned "right to be let alone" originally consisted in the right of complete immunity against the effects of physical violence, including emotional and psychological damage (Cooley, 1906, p. 29):

> The right to one's person may be said to be a right of complete immunity: to be let alone. The corresponding duty is, not to inflict an injury, and not, within such proximity as might render it successful, to attempt the infliction of an injury. There is very likely a shock to the nerves, and the peace and quiet of the individual is disturbed for a period of greater or less duration. There is consequently abundant reason in support of the rule of law which makes the assault a legal wrong.

Warren and Brandeis proposed that the right to be let alone be extended to include the non-physical invasions into the private life of an individual. They claimed that the informational and emotional well-being of an individual should be protected on a par with their property and physical integrity. Otherwise the full scope of the right to let alone would lack sufficient legal protection. Moreover, Warren and Brandeis believed that as various technologies evolve, new measures of privacy protection will have to be developed in order to ensure the immunity of an individual from being observed.

This observation alone provides a valuable perspective on the relationship between privacy and technology as they have been perceived in the recent years. In particular, a popular view that the current technology, whatever it may be for the moment, challenges

our conception of privacy is trivial (Agre and Rotenberg, 1998). After inspecting this initial piece of history of legal discourse on privacy, it is natural to conclude that the social interest in privacy is typically due to some new technological development which brought with itself new forms of surveillance. And as far as the law is concerned, there would have been no talk of privacy without the disruptive technologies which continue to subject our society to discomfort and harm.

The theory of privacy proposed by Warren and Brandeis has become known as the nonintrusion theory of privacy (Moor, 1991). And although solid evolutionary justification for privacy is presented in the exposition of the theory, the definition of privacy as the right to be let alone proved simply inadequate. As Moor (1991, p. 71) pointed out, whenever we approach a person in the street we are not letting them alone, but at the same time, no invasion of privacy takes place. On the other hand, when we are subjected to surveillance, our privacy is violated, even though, strictly speaking, we are being let alone.

Despite its shortcomings, the theory of privacy as nonintrusion has been a groundbreaking accomplishment in the debate on privacy. In their original 1890 paper, Warren and Brandeis bring together a series of common law cases which until that time had remained unrelated, including Yovatt *v.* Winyard (1820) and Abernethy *v.* Hutchinson (1825), and Prince Albert *v.* Strange (1849), and defined privacy violation as their common element. The cases concerned, respectively, the theft and usage of veterinary medicines by an employee; an attempt by a student to publish in the *Lancet* lectures given by other people; and the usage of images of Queen Victoria and her husband Prince Albert without their consent. Warren and Brandeis demonstrated that the bases for rulings in such cases were regulations protecting personal rights and interests related to privacy, such as property, honor and personal image.

Post (2017, p. 261) called this version of nonintrusion theory of privacy *descriptive*. That is, privacy is identified through the factual feelings of the victim of intrusion while the corresponding general definition of the right to privacy remains vague. Bartczak (2013, p. 7) also pointed out that despite significant publicity, the ideas of Warren and Brandeis initially went unnoticed by the American judiciary and it was not until the seminal paper by Prosser (1960) that the theory of nonintrusion has gained considerable influence among the legal scholars of the time.

Prosser started off with the theory of Warren and Bradeis and by analyzing extensive jurisprudence related to the right to privacy, arrived at a *normative* theory of privacy. The main objective for Prosser was to unify the content of the right to privacy, that is, explicate what the right to privacy is *about*. His conclusion was that there are at least four

separate categories of torts related to privacy (Prosser, 1960, p. 389), namely intrusion, public disclosure, false light publicity and appropriation. Intrusion was understood as an illegitimate interference in seclusion and private matters of a given person, public disclosure as making public facts which humiliate a person. False light publicity brings a person into a false light in the public eye, while appropriation consists in usurping someone's name or likeness.

Prosser's legal classification of instances of privacy violation does not bring much clarity on what privacy is in general. Bartczak (2013, p. 11) indicated that since Prosser's paper in 1960, no equally groundbreaking concept of privacy has appeared in the American legal theory and that this impediment carries over to the European theories of the right to privacy. Should privacy violation be a single legal category, as Warren and Brandeis proposed, or a collection of various categories which relate to each other in some way? Bartczak argues that identifying the content of the right to privacy as it is to be defined by law requires obtaining a general definition of privacy first.

One conclusion which follows from observing the historical development of the non-intrusion theory of privacy is that law and legal theory do not provide a satisfactory answer to the question *what is privacy?* Consequently, the debate followed two rather separate paths from that point onward. For one, the philosophical and political interest in the problem of privacy resulted in a theory of privacy as control of information in the 1980s. However, the legal disputes related to the right to privacy had not ceased just because legal theorists and academics lacked a proper understanding of privacy. Hence, via a parallel path, appeared a short-lived theory of privacy understood as liberty or freedom to act in personal matters.

Section 1.2.2 provides a short exposition of the theory of privacy as freedom to act in personal matters. Similarly to the non-intrusion theory of privacy, the theory of privacy as freedom to act is an *ad hoc* legal construct, which nevertheless contributes to the task of finding an operational definition of privacy. A more theory-oriented discussion of the concept of privacy begins in section 1.2.3 with the theory of privacy as control of information.

1.2.2 Privacy as freedom to act in personal matters

The theory of privacy as freedom to act in personal matters arose from a judicial debate following the ruling in Griswold *v.* Connecticut case (1965). Although it is a perfect example of *ad hoc* legal philosophy and although both the justification itself and the application of the right to privacy to deliver the ruling for the case are debatable, the

considerations about the case contained some surprisingly accurate insights pertaining to the nature of privacy.

Griswold *v.* Connecticut (1965) is a landmark American case, but perhaps not so much due to privacy issues as for its meaning to the public debate on access to contraception. The case started with a physician, the director of the Planned Parenthood League of Connecticut, being convicted as accessory in a state law violation for giving a married couple information about how to avoid pregnancy. The end result of the case has been a judicial conclusion that the right to privacy prevents states from making illegal the use of contraception by married couples. The case became a foundation for further cases concerning personal liberties related to sex and family planning, including Roe *v.* Wade (1973) and Lawrence v. Texas (2003), both of which have been argued for on the basis of privacy.

The majority of the judges, including William Orville Douglas, Earl Warren, Tom C. Clark, William Joseph Brennan, Jr. and Arthur Joseph Goldberg, found various legal justifications for protecting what they called *the zone of privacy* which arises from a relationship of a married couple. Even Hugo Lafayette Black, who offered a dissenting opinion to the legal justification of the majority, called the law which prevented married couples from using contraception offensive (Moor, 1991; Grey, 1983). The source of disagreement in the case was in fact not the conviction of whether the right to privacy in the case demands protection or not, but rather, which particular laws implied its protection. For many years since the ruling in this case, the dominant view has been that the right to privacy imposes a limit on governmental power. Rubenfeld (1989, p. 737) thus summarized the role of the right to privacy in the legal order of the state:

> By all accounts, however, the right to privacy has everything to do with delineating the legitimate limits of governmental power. The right to privacy, like the natural law and substantive due process doctrines for which it is a late-blooming substitute, supposes that the very order of things in a free society may on certain occasions render intolerable a law that violates no express constitutional guarantee.

Despite its theoretical underdevelopment, the theory of privacy as freedom to act introduced several breakthroughs into the debate on privacy. It has been the first documented example of the right to privacy operating within a conflict between citizens and the state and not, as has been the case before, between citizens as legal equals. Note that the very idea of protecting the freedom of an individual to act in *personal* matters only makes sense in the context where the intrusion from the government is taken into perspective. Thus, the treatment of the right to *privacy of a citizen against the state* is a manifestation of the legitimacy or illegitimacy of the government.

Another revolutionary development linked to this particular theory of privacy is the idea that even in the absence of any laws to protect the right to privacy, the expectation of privacy and the entitlement to protect this expectation remain in full power. The first to submit this idea for discussion in Griswold *v.* Connecticut case was W. O. Douglas, who argued that the right to privacy (at least with regard to the marital relationship) predates the American constitution and all subsequent laws and that it derives from the natural law. Rubenfeld (1989) supported this argument by claiming that any law which imposes on the fundamental right to privacy is totalitarian in nature, because of the degree to which the consequences of such laws regulate the life of an individual. Rubenfeld contributed to establishing the right to privacy as the necessary means of maintaining control over one's own existence.

The theory of privacy offered in section 1.3 relies heavily on the above observations. It also aims to recover the notion of a *zone of privacy* and precisify its meaning. In the theories of privacy which focus on *information*, like those presented in section 1.2.3, the notion of a zone of privacy had been obscured. However, those theories offer further unique reflections on the nature of privacy.

1.2.3 Privacy as control of information

Despite its very general character (Israel and Perry, 1991), the concept information has brought about a powerful movement of conceptual transformations in philosophy of mind, epistemology, aesthetics, philosophy of science, philosophy of language, ethics and metaphysics (Floridi, 2002). The techniques rooted in information and data science have brought about new methods of research in natural and cognitive sciences (Bliss, 1967; Borne, 2009, 2010; Marx, 2013), economics (Einav and Levin, 2014; Varian, 2014; Collins, 2016; Mullainathan and Spiess, 2017), social policy (D'Amuri and Marcucci, 2017; Salganik, 2019) and security research (Kim et al., 2014; Akhgar et al., 2015; Crampton, 2015), to name but a few.

Many contemporary theories of privacy take as their foundational concept the notion of information. Moor (1991, p. 74) claims that this is due to the rise of information technologies, perceived as being capable of invading the privacy of individuals in a manner unprecedented in the history of technology. Moreover, in a wide range of contexts information functions as a currency or an equivalent of currency (Lennon, 1999; Berthold and Böhme, 2010; Harviainen and Savolainen, 2014; Stilwell, 2018). And since it is information that is exchanged, spent and monetized, it is natural to try to build a theory of privacy centered around the notion of information.

Fried (1984), Beardsley (2017) and Westin (1967) defined privacy in terms of *control of information*. Fried emphasized that it is not the quantity of information made known to a third party about an individual that demonstrates the level of privacy, but rather the fact whether the information has been made known or withheld according to the decision of an individual (Fried, 1984, p. 209):

> As a first approximation, privacy seems to be related to secrecy, to limiting the knowledge of others about oneself. This notion must be refined. It is not true, for instance, that the less that is known about us the more privacy we have. Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves.

Fried further argued that in order to be able to maintain control over their personal information, an individual should be able to not only decide what information is made known to a third party, but also to what degree of detail the third party should be informed (Fried, 1984, p. 210):

> Privacy, thus, is control over knowledge about oneself. But it is not simply control over the quantity of information abroad; there are modulations in the quality of the knowledge as well. We may not mind that a person knows a general fact about us, and yet feel our privacy invaded if he knows the details. For instance, a casual acquaintance may comfortably know that I am sick, but it would violate my privacy if he knew the nature of the illness.

Along with his theory of privacy, Fried presented many sound psychological and behavioral argument for privacy protection. However, most of his arguments operate independently from the theory which Fried presented. A similar theory was formulated by Westin, who defined privacy as follows (Westin, 1967, part 1, para. 3):

> 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. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve.

An important accomplishment in Westin's proposal is the idea that not only individuals have a claim to privacy, but also groups and institutions. Another noteworthy remark is that privacy in some way conditions social participation, though Westin only aimed his

thesis at the social participation of an individual, focusing on the relationship between an individual and a group. I will bring this claim to full generality later on in section 3.2.1, when arguing that privacy conditions social and political participation of groups and institutions as well, although perhaps for reasons different than those discussed by Westin, because the relationship between a group and an individual is not of the same nature as the relationship between the state and the subordinate groups, institutions and individuals.

In an attempt to strengthen the theory of privacy understood as control of information, Beardsley (2017, p. 65) went on to declare that the claim to privacy comes into realization in the form of a *right* of a person to decide when and how much of their personal information is revealed to others. However, even assuming the most amicable interpretation of privacy as control of information, its theories are not only insufficient in many respects, but also brought serious setbacks compared to previous theories of privacy. Below I discuss selected problems of this theory and then, in section 1.2.4, proceed to present a theory of privacy which shifts its focus from information to the concept of activity.

Moor (1991, p. 75) argued that although control of information bears some relation to privacy, it cannot be defined as privacy because there are frequent situations in which control of information is lost, but privacy has not been breached or invaded. For example, information about the tax reports of politicians is often discussed publicly or between individuals and while said politicians have no control over the spread of information, there is no violation of privacy to speak of. Moor also points out that if control is construed to mean direct, personal control of information, most everyday interactions are equivalent to giving up our control of information unconditionally and without restriction, because it is impossible to control how the information exchanged in a conversation will be disseminated. In other words, we are giving up privacy whenever we tell anyone anything about ourselves. Such formulated theory of privacy trivializes the pursuit of setting boundaries between privacy protection and admissible behaviors in everyday situations.

Having pointed out the lessons learned from previous conceptions of privacy, I will offer my own critique of privacy understood as control of information. Most importantly, the focus on *information*, although expressing the enthusiasm of having entered the information age, has dangerously obscured the power dynamic related to privacy violation. Privacy as control of information fixates upon the *what* instead of the *who* of privacy. And so, even though the claim to privacy has been granted to groups and institutions in some of the theories of privacy as control of information, the opportunity

to keep an eye on the relationship between an individual and the state and also that of a group and the state is lost for good. Once the control over a given piece of information is lost, it is not just our peers, but also the authorities and business agents who can exploit the information to their advantage. In my view, this flaw, that is, the fact that the discovery by peers *v.* by public authorities are not distinguished, is detrimental to the theories of privacy as control of information, as it effectively prevents the debate over political aspects of privacy.

A proponent of the control of information theory of privacy might claim that this is indeed a minor flaw. After all, the categorization of the recipients into groups with which information is shared could be an element of the specification of the extent to to which the information is shared. But would this prevent privacy violations? I argue that it would not and, as a matter of fact, does not. Even if we allow, in the spirit of full control over information, for hand-picking specific targets on case by case basis, we do not exclude many known privacy violations in the citizen-state dynamic. Consider for example the 2012 case of eight UK activists who were put under surveillance in relation to their political campaigning (Evans and Lewis, 2012). The undercover police officers, besides forming long-term relationships with the activists which included, in some cases, having children together, served as informants for the state throughout the relationship. Set aside the various ethical aberrations of justice which accompany this case, let us examine the information control which the activists had in the process of surveillance. Even though they could hand pick the specific person who receives each piece of information, they had no choice as to whether the information will be relayed to the surveillance authorities or not.

Clearly, the privacy of the activists has been violated, but where does the violation originate? For one, it does not come from the fact that personal information has been shared with a person who did not earn the trust of the activists. In fact, the undercover policemen worked continuously to earn the trust of their victims. The violation also does not originate from the idea of a person sharing the information they have with the authorities. If this were the case, reporting any crime, actual or suspected, would count as privacy violation. Even the theory of privacy as control of information must make an exception here.

So what goes wrong with privacy in cases like these? As I will argue later in more detail, the central problem which constitutes privacy violations in such cases is the fact that the state gets involved where it has no business being involved, namely, in the most intimate aspects of activists' lives. And so the problem was not that the activists did not know the identity of the people they share information with (because they did) and it

was not that the people who received the information relayed it to the authorities (they may chose to do so). Rather, the problem is in the deception of the information source, in the fact that the targets of information are not who they seem *with respect to the state*, *i.e.*, that they are falsely appearing as if they were not policemen, but regular citizens. In other words, the privacy violation is in that agents of the state are cleverly hidden from the sight of their victim. This problem, however, cannot be spelled out in terms of theory of privacy as information control.

Another serious problem with privacy as control of information is that control relies on the subjective preferences of an individual to share information about themselves. The theory does not impose any limits on the obligation to respect such personal preferences, making privacy a question of unrestricted and and unconditional personal freedom of an individual. This approach is not only utopian, but also simply unattainable. Proposing such theory of privacy in conditions of a complex social and political order misses the point entirely, particularly considering that even some the first theoreticians of privacy, such as Warren and Brandeis, accentuated the importance of defining privacy in a way that allows setting reasonable boundaries on social interaction.

1.2.4 Privacy as undocumented personal knowledge

Another concept of privacy focusing on the notion of information was proposed by Parent (1983), who also offered a critique of the theories of privacy then known, including the theory of privacy as control of information. Stemming from this critique is one of the desiderata which Parent defines for a satisfactory theory of privacy, which will become central towards the end of this chapter:

> To define privacy as the control over (all) information about oneself implies that every time I walk or eat in public my privacy is compromised. The implication flies in the face of common sense. An adequate conception of privacy must not allow for the possibility that a person's privacy can be violated simply by observing him openly engaged in public activities. (Parent, 1983, p. 344)

The core idea of this requirement is that a person should be able to maintain certain elements of privacy regardless of the situation. Although on the grounds of the theories we have inspected so far this requirement does not stir much controversy, it will become quite problematic for the theory of privacy as restricted access discussed in section 1.2.5, which relies on the notion of a *situation* in deciding when the privacy of an individual has to be respected and when it can be reasonably invaded.

In the context of the arguments discussed in the end of section 1.2.3, Parent formulates the following additional desiderata:

> Any adequate definition of privacy must allow for the possibility that persons can exhibit a lack of respect for their own [privacy –AS]. (Parent, 1983, p. 344)

Therefore, according to Parent, a good theory or privacy must allow for carelessness and ignorance to be reflected in the level to which an individual's privacy is protected. In other words, a good theory of privacy presents privacy protection as optional in the sense that privacy is seen as a depletable commodity which, once lost, may be impossible to regain.

Keeping these desiderata in mind, Parent defined privacy as "the condition of a person's not having undocumented personal information about himself known by others" (Parent, 1983, 346), where personal information is understood rather broadly as the information that one does not want known about themselves. Parent specifies two typical reasons to consider information personal. First, information refers to facts which most people in a given society choose not to reveal about themselves, except to friends, family, advisers and others with whom they form a confidential relationship. Second, information refers to facts about which a particular person is extremely sensitive and which he therefore chooses to conceal. As an example of the latter type, Parent discussed a man's height, which for a short person, may be a source of shame and therefore, relate to information which one chooses to never reveal.

Instead of focusing on the control of information, Parent addresses the *content of information* as the classifier for privacy protection. There are at least three critical flaws which follow from this type of formulation. The first one is that of *subjectivity* of the target of protection. Similarly as in the theory of privacy as control of information, in the theory of privacy as undocumented personal knowledge the issue of protection has to be decided on a case by case basis. The only difference between the theories in this respect is that instead of asking for an individual's preference, we evaluate their emotional connection to each piece of information. In practice, however, the only way we have of learning about an individual's emotional state is by asking them. Consequently, the theory of privacy as undocumented personal knowledge suffers the same weakness as privacy as control of information. It defines privacy as relying on subjective decisions of individuals, which in turn makes systematic privacy protection problematic.

Another problem of Parent's proposal is that the resulting theory is both too broad and too narrow. As Moor (1991, p. 76) pointed out, there are many ways in which we may learn that a given man is short and which do not require any privacy violation.

For example, we may observe during a public meeting that the man is wearing elevator shoes or simply notice his height compared to people around him. Similarly, some wide known facts, although undocumented, can be spread without the threat of privacy violation. Furthermore, a fact that a particular man is an alcoholic is a good example of information which people exchange without violating the man's privacy and which the man is likely to want to conceal from public knowledge. For a case in which the theory is too narrow, consider the following situation. Alice gets access to Bob's computer and copies Bob's diary to a folder shared between Bob and Carl. At no point Alice looks or gathers any information about Bob. However, it is clear that Alice has violated Bob's privacy. Moor notes that this situation would be correctly classified by the theory of privacy as control of information but not by the theory of privacy as undocumented personal knowledge. In this sense, Parent's proposal is a step back in formulating an adequate theory of privacy.

Finally, in my view, the most destructive flaw of Parent's theory is that the dependence on content as the classifier for protection defeats the purpose of protection altogether. Consider the following situation. Alice wants to reveal in public some information about Bob. Bob tries to stop Alice by claiming that the information to be revealed constitutes undocumented personal knowledge about Alice. The only way to decide whether the information can or cannot be revealed is by inspecting its content. However, the process of inspection by a third person is already making the information known to others. In practice, the third party would not be a single person, but most likely a group. It is not reasonable to expect that all members of such a group will respect confidence, unless they are so obliged by the law, *e.g.* as would be the case for a judge or legal counsel. In turn, every case of making the information public would have to pass the same content inspection every time that the person whom the information concerns claims that it constitutes undocumented personal knowledge. This means that, potentially, most publications in the press have to be first inspected by in a court of law or by another arbiter sworn to secrecy. Thus, a strong objection to the theory of privacy as undocumented personal knowledge is that it is immensely impractical.

1.2.5 Privacy as restricted access

The theories of restricted access are among the most successful contemporary theories of privacy. They are generally classified by indicating *what* it is that we are restricting access to, that is the range of states of affairs to which privacy is attributed. Among the candidates for this *range* are the following: (i.) information and persons themselves

(Allen, 1998; Gavison, 1980; Powers, 1996), or (ii.) situations (Moor, 1991). Both types of theories, despite their shortcomings, offer valuable insights into the social perception of privacy.

The initial theories of restricted access concern the limitations of access to persons in the physical sense and also to information or knowledge about them. Powers (1996) blended the two targets of protection in naming a theory of restricted *cognitive* access. Allen (1998) and Gavison (1980), despite agreeing on the basic range of protection targets, offer theories which have rather distinct motivations and consequences. While Gavison (1980) advocates the non-reductionist approach to privacy, that is a claim that privacy is not to be treated instrumentally as a means of protection of other interests, Allen (1998) relates privacy to liberal values and promotes what she calls *the liberal view of privacy*. In comparison, Gavison's theory does not enforce such broad ideological commitments, despite being qualitatively the same theory to Allen's in terms of core conceptual framework.

Allen (1998, p. 724) binds privacy with the liberal conception of private property and the liberal conception of private choice. The parallel between privacy and property is expressed as follows:

> We associate privacy with certain places and things we believe we own, such as our homes, diaries, letters, names, reputations, and body parts. At the core of the liberal conception of privacy is the notion of inaccessibility. Privacy obtains where persons and personal in- formation are, to a degree, inaccessible to others.

In sketching out this analogy, Allen derives from an earlier work of Hefferman (1995) who explicated the *seclusion privilege* as a key aspect of privacy. The notion of seclusion privilege will be of critical importance in section 1.3 and is characterized as a one of the *second tier* rights of an individual. The rights of the first tier are those which individuals can exercise in both public and private places. They include a variety of well-established rights, like the right to freedom of expression, but also other rights sometimes not captured by any legal act. The second tier rights impose a requirement of seeking seclusion on an individual willing to exercise them and thus yielding to social taboos. For example, it is common for the authorities to impose a *seclusion restriction* on sexual activity. At the same time, they extend the scheme of liberty constituted by the first tier rights. Hefferman (1995, p. 741) motivates this extension as follows:

> [P]rivacy rights presuppose a seclusion privilege. They rest on the premise that people should be able to engage in activities that run counter to widely shared norms when they do so in private places. Seclusion thus plays a special role in sustaining

> what the Court has termed "the right to differ." Seclusion allows for a flourishing of difference beyond that which society tolerates in public places because it cuts people off from direct contact with the outside world. As a general matter, then, privacy rights build on liberalism's traditional concern with individual development, creating a zone of liberty in private places that is more expansive than that in public places.

In what follows I will build upon this fundamental feature of privacy to enable us to *do within a zone of privacy what is unacceptable outside of it*. This notion contradicts the nowadays frequent argument against privacy protection known as *nothing to hide* argument.

Despite deriving from the strong motivation of the seclusion privilege, Allen's theory of privacy does not seek a guarantee for unconstrained execution of (potentially publicly unacceptable) behavior within the bounds of a zone of privacy, but rather relates privacy to independence in decision-making:

> The liberal conception of private choice is the idea that government ought to promote interests in decisional privacy, chiefly by allowing individuals, families, and other nongovernmental entities to make many, though not all, of the most important decisions concerning friendship, sex, marriage, reproduction, religion, and political association.

One of the critical flaws of this formulation is that it imposes an extremely vague limitation on privacy by making it contingent on the type of decision in question and whether it lies within the scope of individual's personal independence or outside of it. In other words, such defined privacy can only be properly described after it is settled what exactly a person can and cannot decide for themselves. Subsequently, access to means of making those decisions is either restricted or approved by the public authority. Even assuming that the decisions are categorized on the basis of type and not case-by-case, we are still left with a notion of privacy fluctuating with virtually every legal act and judicial proceeding. After all, it is the sole purpose of the law to determine what we can generally decide for ourselves and implement this assessment, either *via* deregulation or explicit acknowledgement, and what is decided for us. Thus defined notion of privacy, through its dependence on choice, is essentially undiscoverable and therefore meaningless. There is no doubt that privacy does allow for independent decision-making. However, I will argue in section 1.3 that uninhibited decision-making is but one of the many benefits which acting within the zone of privacy offers and should not be viewed as its defining element.

Gavison (1980) makes a case for a notion of privacy which requires much less background ideological commitments than Allen. Moreover, Gavison makes explicit the methodology of formulating a theory of privacy which is prevalent in legal, political, and psychological literature on the subject. Namely, theories of privacy are formulated in a way to make precise the nature of our concern and fear related to privacy loss. Consider, for example, the following statement (Gavison, 1980, p. 423):

> Our interest in privacy, I argue, is related to our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention. This concept of privacy as a concern for limited accessibility enables us to identify when losses of privacy occur.

This motivation is uniformly exhibited in all theories of privacy considered so far. In the most straightforward terms, privacy is the idea born out of our fear of being watched when we do not want to be watched, of being touched, moved and bothered when we seek to not be engaged with, of our actions being scrutinized when we want to act free from judgment. We intuitively recognize the limits of this need and accept that we will be watched, touched and otherwise engaged with when we do not wish for it, because such are the necessities of sharing territory and resources with others. However, we seek the right to build zones within which we cannot be interfered with, where we can do what in a wider context would be inadmissible, objectionable, offensive or disgusting to others.

Whether we chose to be inside our own home or go outside and regardless of the weather conditions, we have a human need for shelter. Even when there is no imminent danger to be encountered in our area and when it is perfectly possible to conduct all our everyday activities in the streets, hardly any person chooses to be homeless. After all, shelters do offer protection from various threats and inconveniences, which may be one of the reasons why the evolutionary history has fixed the need for shelter in the set of our mental competences (Taylor, 1988). A very similar and related evolutionary competence is that of seeking a balance between communal activity and privacy (Schaefer et al., 1999). Similarly to the need for shelter, we need to be alone at times, regardless of whether we have something to hide from our community or not (Schudy and Utikal, 2017). Our need for protection does not have a quantitative character (Benndorf and Normann, 2018), which suggests that we do not normally consider our privacy to be a tradeable resource.

That being said, it is important to note that as far as the fear which motivates the effort to develop a theory of privacy to be subsequently adapted into privacy protection

procedures is understandable, the methodology of developing the theory does not have to be limited to explicating neither instances nor the general nature of this fear. A theory of privacy does not have to be essentially the theory of when privacy gets violated, as long as privacy violations are explainable in terms of that theory. In case of the theory of restricted access like that of Allen or Gavison, the source of privacy violations is rooted in the fact that others have access to us or information about us. Consequently, the solution to the problem is offered in the form of the capacity to restrict the access necessary for violations.

A much more constructive version of the theory of restricted access is that proposed by Moor, who views the object of privacy protection in the notion of a *situation*. Thus, Moor describes privacy as *privacy in a situation* (Moor, 1991, p. 76):

> [A]n individual or group has privacy in a situation if and only if in that situation the individual or group or information related to the individual or group is protected from intrusion, observation, and surveillance by others.

Moor makes an effort to differentiate the direct target of protection from what we perceive as objects of privacy violations, that is persons and information. Thanks to this step, the proposed theory makes it possible to guarantee the protection of persons, information and other valued aspects of personal conduct, *through* legitimizing the expectation of privacy in a situation, as opposed to defining privacy simply as a state of affairs when persons and information are free from intrusion or access. Compared to the earlier theories of restricted access, Moor not only provided an explication of what is threatened by privacy violations, but also a notion of privacy *per se*.

In his definition of a situation, Moor comes close to Hefferman's notion of seclusion privilege (Moor, 1991, p. 77):

> The paradigm example of a private situation is a situation in which one is protected from the prying eyes of others. Private situations are islands of epistemological sanctuary.

However, the notion of a situation generates certain unique problems. Moor claims that the definition is purposefully defined in vague terms in order to allow for a wider range of states of affairs over which protection is to be extended. Consequently, situations are exemplified in (a.) living in a home, (b.) a relationship between a lawyer and her client, (c.) using information contained in a computer database, (d.) taking a walk in the forest, *etc.* At this stage, the first problem emerges. How is calling something a *situation* different from saying *just whatever a person does*?

Moreover, some situations have a spatiotemporal component, but not others. Some of them allow only for a single instance intrusion, but not general intrusions. For example, finding someone walking in a forest constitutes a single case of intrusion into someone else's situation, but not into the general situation of this person's habit to take walks in the same forest.

Further complications (as well as opportunities) follow from the distinction between *natural privacy* that is a set of situations in which we are as a matter of fact alone and unsupervised, and that of *normative privacy* which encompasses situations is which we *should* be left alone and proceed with our affairs without supervision or intrusion (Tavani and Moor, 2001). Assume, however, that a person maintains multiple situations simultaneously, which is necessary in order to qualify (b.) and many others as situations in the first place. Then it is conceivable that a person might combine (b.) and (d.) within the same spatiotemporally determined activity. Namely, a person is walking in the forest together with a lawyer with whom one consults the details of their ongoing legal case. A third person happens to be in a vicinity of the client and his lawyer and overhears the details of the case. The natural privacy of the duo has been interfered with, however, the violation is justifiable, for there can be no expectation of privacy in (d.), so normative privacy does not apply. On the other hand, (b.) is in fact within the scope of normative privacy. Does the third person have the right to gain access to (b.) simply by being authorized in their access to (d.)? Of course, the problem here is not how to interpret a scenario in which someone gains access to a situation by coincidence, but whether they are justified in listening in to the conversation simply because they have found themselves interfering (d.), where there is no normative privacy.

Such vague notion of a situation makes is extremely difficult for us to protect (b.) when it coincides with (d.) spatiotemporally. Analogous problems occur in much more grievous contexts. For example, are we justified in withholding information about our personal life from a police or immigration officer? Do third persons have the right to covertly take pictures of documents which we exchange with someone in a public space? Are there any limitations on searches performed at the airport security check? Those and other questions can be argued for and explained on the grounds of privacy but they are extremely difficult, if not impossible, to adequately spell out in terms of *situations*.

1.3 The gateway theory of privacy

In the theory of privacy I propose a person has the benefit of privacy when she can authorize or deny access to her *zone of activity*, and I define a zone of activity as the

domain of affiliated behaviors the consequences of which are restricted to the boundaries of this domain. In other words, the person will be said to have privacy with respect to a given zone of activity if she controls all its gateways, or points of access, which make observation possible. Hence, the gateway theory of privacy defines privacy as the ability to authorize (or deny) access to zones of activity.

1.3.1 The notion of a zone of activity

Zones of activity, although comprising of various instances of behaviors, are not reducible to them. For example, a zone of activity evoked by a marital bond is not reducible to the class of spatiotemporal events which the married couple undertakes. It would be counterproductive to attempt giving a comprehensive account of marriage purely in behavioral terms, even if one were able to consider all future and merely potential behaviors. Similarly, a zone of activity presents an *emergent* value, which, similarly to the notion of a situation, can gain communal recognition or not.

Despite certain similarities with Moor's situations, zones of activity are not spatiotemporally burdened, nor can they be summarized as *just whatever a person does*. Far from it, people can display behaviors which have no affiliation with other behaviors and do not belong to any known zone of activity. Moreover, zones of activity, although their catalog is open, are often conventional and it is by convention that their recognition as protected or unprotected is decided upon.

Certain zones of activity are goal- or value-oriented, other stem from biological or territorial necessity. Some of the typical originators of the zones of activity include the following:

(1.) a contract or an understanding between two individuals, *e.g.* marriage, a lawyer-client relationship;

(2.) a biological or emotional bond, *e.g.* a parent-child relationship;

(3.) a territorial, spatial or legal bond, *e.g.* one's relations with a neighbor, another passenger in an aircraft or another citizen of a city or a country;

(4.) a membership in a group, a club or a school, *e.g.* one's capacity as a member or a student;

(5.) a need for self-development and exercising the sense of agency, *e.g.* one's strive for unsupervised experimentation and interaction with oneself and the environment.

1.3.2 Protected and unprotected zones of activity

The key aspect of the notion of a zone of activity, which is missing from the situation-based theory of restricted access, is that no consequences are drawn outside the protected zone of activity for the actions taken within that zone. This condition does not hold for zones which are not recognized as protected. Note that *protection* is not understood as protection *from* privacy violations, but rather protection of the person acting within the zone to be free from consequences of her actions. In particular, these consequences include being judged by others, being put under investigation, losing prestige, face or social standing, suffering embarrassment, having a registered record of actions saved for future use and being overtly or covertly threatened.

A restriction of access, by which I understand the person's capability to authorize and unauthorize access of individuals or groups to each of her zones or activity, is a result of the attempt to exercise protection over those zones. Depending on whether a given zone of activity is recognized as protected by a wider community, the efforts of one or more members of the zone to restrict access to it will be either enhanced or handicapped. In some cases, like that of (b.) in section 1.2.5, courts would exclude evidence gained *via* unauthorized access to communications in order to protect the zone of activity endowed with attorney-client privilege. The exclusionary rule which classifies illegally obtained evidence as *fruit of the poisonous tree* is another good example of the social and legal effort to protect those zones of activity which receive high recognition and protection.

A theory of privacy based on how far we draw the consequences of a person's behaviors may seem unintuitive at first. Consider, however, a situation where there would be no consequences of our actions, by which I mean *no consequences at all*. Would we still care about who is looking at us? In most cases, we probably would not. In particular, the state of anarchy introduces new patterns of behavior in which the fear of consequences is diminished. In an anarchic community or context the struggle for power may just as well eliminate the need for privacy, as the behaviors which are normally suppressed or kept private increasingly occur out in the open (Goldgeier, 1997). A person's attempt to restrict access to one of their zones of activity is validated in that we recognize the legitimate interest of the attempt. Sometimes it happens retroactively, like by applying the aforementioned exclusion rules, and some other times, we recognize the need to create means of protection which enable the person to prevent unauthorized access altogether.

This formulation of the theory of privacy has several advantages. For one, the theory is completely independent of the current state of technology and habits of communication. The zones of privacy may include behaviors which involve various technological

solutions, some of which will offer better protection than others, but the only important aspect is that we require that there exist, for each zone labeled as protected, accessible and privacy-oriented ways to maintain and develop it. For example, even though not all channels of communication may be entirely private, we require that the person has a way to communicate with their lawyer within the protected zone and that, when due care to exercise protection has been taken, the fiction of effective protection is maintained even in conditions of a violation.

Another benefit of the presented theory is that it stays constant in various cultural, social and legal contexts, and allows for changes in the list of protected zones of activity. Many cultural differences relating to privacy can be explained in terms of a disparity in value which a society ascribes to a given zone of activity. For example, according to Khoo et al. (2002), Canada and the Scandinavian states are known to be more intrusive in the zone of activity shared between parents and children. An explication of this fact in terms of the presented theory is that those states do not agree that the consequences of actions taken within the child-parent zone should be limited to its bounds. In particular, they may act upon the belief that a parent ought to be socially and legally responsible for their actions towards a child, in particular those which consist in what is seen as maltreatment.

In my formulation, the social-political debate over privacy has as its goal to introduce or remove items from the list of protected zones of privacy based on their economic, humanitarian, strategic or practical merit. This type of approach fully accommodates the need for a cross-disciplinary characterization of privacy, while allowing a case by case analysis of various zones of activity.

Now I will show how the gateway theory of privacy allows us to engage with the contemporary debate on privacy. I summarize shortly the two stances in the conflict of power regarding the right to privacy and show their influence on the state of the art privacy research. Next, I will offer a middle ground stance formulated in terms of the gateway theory of privacy, which allows maintaining a normative standard of privacy.

1.3.3 The state of the art in privacy debates

Since the conception of access account of privacy, the academic debate on the topic became fixed upon contrasting it with the control account (Macnish, 2018; Moore, 2003). Menges (2020, p. 2) even argued that "discussing conceptual questions about privacy has fallen out of fashion" since the turn of the century.

Two immediate consequences follow from this fact. One, the academic community

gradually fell into irrelevance as a voice in the debate about privacy in the recent years. Instead, the conflict concerning the essence of privacy and the scope of its protection ensued between two camps of the representatives of radical views. The first camp is that of the signal intelligence agencies, such as the NSA or the GCHQ, and the representatives of surveillance capitalists, such as Google, Facebook, *etc*. The other is that of privacy advocates who often claim that any infringement of privacy is ultimately a violation of the inherent right of an individual. I will refer to this group of stakeholders, albeit simplifying the matter with such use of terminology, as *privacy-oriented organizations*. In between these two radical stances remains the majority of citizens, who, on one hand, value security, and, on the other hand, want to protect themselves, as well as their families and communities, from the social and political system in which the abuse of power is common.

The second consequence is that the theories of privacy remain centered around the notion of information since the opening of the debate between the control and access accounts. In this sense, the conceptual development of the available theoretical frameworks ceased to evolve around the time when the role of information in modern technology entered the academic debate. One of the serious disadvantages of this formulation is that any initiative related to privacy relies on the ability to formulate the claim to protection and the potential damage to protection in terms of information. Moreover, information-focused framework enabled the definitional loophole to be used in a legal justification of the controversial *Stellar Wind* program, a warrantless surveillance program initiated under the George W. Bush administration in 2001 and subsequent mass surveillance programs in the USA. A key argument for evading the necessity of a warrant for the surveillance operations was that, as the Bush administration assumed, the mass collection of data did not count as surveillance, spying or a breach of privacy as long as no human inspected the collected data. As I will explain in section 1.3.4, this line of reasoning can only be maintained in the information-based narrative and cannot be plausibly rephrases in terms of the zone-based gateway theory of privacy. This last observation will be expanded in section 1.3.6.

Note that the two consequences, that is, the underdevelopment of theories of privacy in the academic research and the exclusion of the silent majority of citizens from the debate on privacy in politics are related. After all, the interests of the general population are outside the scope of activity of both conflicting stances mentioned above. One of them aims at maximizing the control over the population and the collection of behavioral data, the other promotes a very specific idea of public interest in which the protection of privacy becomes a pretext to limit the security measures and communal activities often

perceived as normal. The latter often ignored the communal and cultural variance in the perception of personal privacy and cannot be said to be representative of the interests and attitudes of the citizens. An important factor contributing to the confusion and silence of the majority is due to the academic neglect of the debate, which allowed the debate to be framed by the surveillance agencies and the privacy-oriented organizations.

1.3.4 Dualism in the politics of privacy

The two aforementioned conflicting approaches to privacy are here bundled together not based on their institutional or ideological connections, but rather based on their distinct relationship with privacy. Namely, the surveillance agencies (which include both administrative and business organizations) benefit from weakening the expectation of privacy in the general population and the inflation of the definition of the privacy breach or infringement. From this perspective, there is little difference between agencies such as the NSA or GCHQ, and the surveillance capitalists such as Google, Facebook or Tencent. It does not matter for our current considerations what use these two types of agents have in mind for the collected data, because these goals do not influence their approach to privacy. That is, in the words of gen. Keith B. Alexander, their goal is to "collect it all, tag it, store it. And whatever it is you want, you go searching for it" (Nakashima et al., 2013). Both the surveillance states and the surveillance capitalists rely on information encoded in our behavioral data to be able to predict and ultimately control our behavior. The former primarily aim to control our behavior with respect to our social and political activity, the latter want to control our commercial activity, in the form of goods and services which we purchase.

As I said before, the account of privacy as control of information has been used to justify the mass collection of data by the administration of George W. Bush following the 2001 attacks in New York. An informative picture of the origin of the American mass surveillance programs emerges from a book by the Deputy Attorney General in the years 2003–2005 James Comey, who remarks that the legal justification behind indiscriminate mass collection of data, which was included in the 2001 memo issued by the Department of Justice's Office of Legal Counsel, was "so bad as to be *facially invalid*" (Comey, 2018, p. 87). The core of the infamous 2001 memo involved narrowing the definition of access to information so as to exclude certain types of information (metadata), as well as any method of collecting, searching and processing the information which would not require immediately involving a human employee. In section 2.3, I will discuss in detail the relationship between security and privacy and show how it is related to the justifications

behind the US surveillance programs. For now, however, it suffices to observe that the restricted access account of privacy was instrumental in enabling the secretive initiative to start the surveillance programs such as *Stellar Wind*.

On the other end of the spectrum when it comes to making available to others the aspects of our lives which are perceived as private are the representatives of the privacy-oriented organizations, a non-heterogenous group of activists and regular citizens who advocate for (often extreme) privacy protection measures, especially in the context of digital and mobile technologies related to mass data extraction. Corresponding to their claims are various legal and political proposals such as to make protecting one's own personal information an ethical obligation (Allen, 2012) and making privacy impact assessments mandatory for businesses (Wright, 2011). The privacy-oriented organizations are typically in favor of disengagement from social media, in particular when the network is owned by a surveillance capitalist. In many everyday contexts, some version of pro-privacy stance allows the activists to argue for limitations and obligations which the general population might consider inconsequential or outright irrelevant. For example, consider photographers who take pictures of strangers in the street and during public or commercial events. Many may not be bothered by being photographed in such circumstances at all, but street and event photography has been a constant and burning problem for some, dating back to the times of Warren and Brandeis, who took issue with the fact that the pictures of their relatives have been published in the newspaper (Warren and Brandeis, 1890). Regardless of how deeply normalized street and event photography has become in the recent years, there always remain those who ask whether there is a way to disallow street photography (Goldstein, 2008) or any covert photography without prior consent of the photographed (Zeronda, 2010).

Note that there is nothing wrong, at least in principle, with a pro-privacy stance. The privacy-oriented organizations are multi-faceted and their representatives often display the level of political and technological knowledge which the general population simply lacks. Moreover, pro-privacy stance makes sense for the majority of the citizens as long as privacy protection coincides with the values which the citizens take as their priority. If it were the case that for the majority of the citizens the harm from allowing unrestricted street photography outweighed the benefits, street photography should be banned. However, social values vary between cultures and social groups, and so the practical choices concerning what is and what is not allowed at the level of citizen-to-citizen interaction should not be decided by the theory of privacy from the get-go, but rather by the application of the theory to particular value setting appropriate for a given collective.

Pro-privacy stances favor the control account of privacy (as in section 1.2.3), because it allows for case by case consent concerning actions of others which target private information and private areas of life. Another important reason for them to rely on the control theory is that it is the only available alternative to the access view, which allowed the mass surveillance to be technically categorized as causing no loss of privacy. Hence, the two conflicting camps appropriated for their own purposes two flawed theories of privacy based on the concept of information, though their aims and applications of these theories were contradictory.

For the surveillance agencies, information access account (as in the opening of section 1.2.5) provided basis for the technicality solution which enabled the abuses of power aimed at kickstarting the unwarranted mass surveillance operations. For surveillance capitalists, it allows the justification behind unrestricted extraction of behavioral data by using the narrow definition of access to suggest that no violation of privacy will take place in relation to their service, because the offender is (in many, although not all cases) artificial intelligence and not a human employee.

In my thesis I will not defend or support any of these groups of interest. I acknowledge that the representatives of both may have legitimate interest in pursuing their respective strategies, even when their actions are not in line with the best interest of the majority of citizens (more discussion on this point will follow in subsequent chapters). I propose that instead of picking between two radical stances which do not represent the social needs of the citizens, we develop a theoretical framework accessible to an average citizen and use it to craft a political, social and economic reality which suits the needs of a modern society. I begin by analyzing the latest proposals in the debate on privacy and embedding the gateway theory of privacy (described in section 1.3) in this academic landscape. Next, in section 1.4, I will outline the political value of privacy and proceed in chapter 2 to characterize the relationship between a theory of privacy and statutory law, privacy laws in particular.

1.3.5 Practical implications of current theories of privacy

Macnish (2018, p. 417) summarized the current state of literature on privacy in the following way: there is a disagreement about whether privacy is a matter or control of information or access to information, as both accounts offer certain intuitive explanations, but also lead to fallacies in the sense that it is easy to find intuitive counterexamples which demonstrate that the definitions of privacy the accounts offer are not adequate. This long-standing debate has been further obscured by the uncovering of mass surveil-

lance programs conducted by signals intelligence agencies such as NSA and GCHQ (Landau, 2013; Lyon, 2014; Bauman et al., 2014).

A notion of privacy, all available versions of which have proven inadequate even in the 1990s, is now needed to make sense of a new reality in which privacy of citizens is infringed upon without agreed on legal bases, without legitimacy of executive decisions which lead to the infringement and in manner completely automatic, performed through mass collection and retention of personal information. Unsurprisingly, both of the information-focused accounts, that is access theory and control theory, do not deal with this new challenge too well. In the conditions of mass surveillance, the control account suggests that the collection and retention of data constitutes a serious breach of privacy of the citizens, as well as non-citizens who have been targeted by the surveillance operations. As long as the control has not been explicitly relinquished by each surveilled person or the decision of the court has not been used to overrule the potential lack of explicit consent, mass surveillance is unacceptable from the point of view of privacy protection.

Regrettably, it seems that the control account has been the only theoretical tool available to the supporters of privacy protection so far. The access account (understood as access to information and not as access to situations as proposed by Moor), adds power to the project of mass surveillance in that *access to information*, as used in everyday language is understood as an actual act of inspecting a piece of information performed by a human being. According to the interpretation of access to information used by the Bush administration, an invasion of privacy would require that a human employee goes through the collected data. This, however, almost never happens considering the volume of collected data and methods used to inspect it. Moreover, automated keyword search and other machine-based techniques allow the government to automatically identify what could qualify as probable cause for privacy invasion, meaning that a human component necessary to satisfy the conveniently rigid definition of access appears only after a potential reason for intervention is found.

Despite its undesirable implications in validating mass surveillance, the access account is far less problematic from a theoretical point of view, at least insofar as the state of affairs before the emergence of mass surveillance is concerned. Nevertheless, mass surveillance emerged as a practice met with resistance and protest, both among the citizens, and the legal and political scholars. Regardless of the received view on privacy, there has yet to emerge in the literature a view that mass surveillance is generally morally, socially and politically acceptable. This leads to the formulation of two immediate problems.

A problem which arises here is how to make sense of mass surveillance in the context of privacy. There is a growing need to construct a means of disallowing it, but the details are not clear. Here enters yet another problem, namely, whether a theory of privacy can help us in any way to invalidate mass surveillance or limit it in some way.

To address these problems one may choose to disregard the concerns about the uniform theory of privacy and aim our attention at the problems where our intuition tells us that the conflict arose due to the infringement of privacy. In particular, on this view the citizens would be encouraged to actively pursue the adoption of adequate privacy laws in their legal systems, even if the emerging concept of privacy is not consistent or does not offer much in terms of protecting future interest. Effectively, the first view aims at starting the never ending quest of lawmaking, but it has the advantage of "skipping" the many years of scholarly debate necessary to understand and operationalize the notion of privacy in all relevant fields. To put things simply, our first option is to start doing whatever we feel is right, even if we do not really understand what it is that we are doing. This *forget-the-definition* view was advocated for well before the public discovery of mass surveillance, among others by Allen (2013, pp. 21-22), Lever (2013, p. 2) and Solove (2002, p. 1088).

Another way to approach these two problems is to claim that mass surveillance is not a valid practice due to reasons other than privacy. Among the proponents of this approach is Macnish (2018, 2020) and Menges (2020). According to Macnish, who, similarly to the Bush administration, understands privacy as access to information, mass surveillance is unacceptable because it threatens the values which are incidentally among those which privacy protects. Moreover, mass surveillance is experienced as privacy loss, even though it is not, partly because it facilitates conditions in which privacy violation is (i.) rational from the point of view of the agent who collects information and (ii.) impossible to stop for the person affected (Macnish, 2018, pp. 428).

This approach is unsatisfactory for a number of reasons. The argument that mass surveillance does not constitute privacy loss even though it is experiences as such and invariably leads to it relies on invalid premises. First, it assumes that the restricted information access theory represents the notion of privacy in a novel context more adequately than our strongest convictions, all the more so in a situation where the theory had straightforward counterexamples even before the novel context became apparent (see section 1.2.5). Considering the fact that, from the methodological point of view, all theories of privacy put forward so far aimed at correctly describing our strongest intuitions about what we perceive to be related to privacy, this assumption somewhat invalidates the effort of theorizing about privacy. Treating a semi-descriptive theory

proposed in political, legal or ethical doctrine to be fully normative may be available to practitioners of law, but it is not a valid method for a scholar engaging with the theory at its origin, that is at a point where its adequacy is a deciding factor for its acceptance or rejection. If it is an accepted view that mass surveillance constitutes a loss of privacy, as indeed is the case in the current state of debate, then a theory of privacy which does not classify mass surveillance as a privacy infringement is no longer adequate. For this reason, the argumentation of Macnish (2018) and Menges (2020) about what would follow, had the information access theory been correct, is simply pointless.

There are even more reasons to be skeptical about Macnish's account of privacy. Assuming that privacy is control of information and that it is only vaguely related to mass surveillance, it is unclear why the values protected from mass surveillance should be considered to be unrelated to privacy. In other words, a situation where both counter-surveillance and privacy protection are supported by the same psychological, social and security motivations, and where they both protect the same values, what is the point of differentiating between them, other than to preserve the normative character of privacy as information access? A similar approach is taken by Menges (2020) who, while attempting to reform the control account in such a way that it does not treat the so called *threatened loss cases* as a privacy infringement, proposes that we understand privacy as control not of information itself, but of control of its source or leeway. His account mimics the access view in that it does not classify mass surveillance as privacy loss, but allows for sharing information between people without the loss of control, thus somehow mending an obvious flaw in a historical theory of privacy as control. Despite disagreeing with Macnish on the control-access issue, Menges argues that mass surveillance should be invalidated for other reasons, although he does not specify what those reasons could be. He simply concludes that "what is normatively and politically problematic in the NSA and GCHQ case is not that people's privacy is diminished but other harms and wrongdoings" (Menges, 2020, p. 19).

Finally, a weakness which Macnish notes himself about his proposal is that it leaves out a large proportion of the subject matter that a general theory of privacy is supposed to cover, a fact which becomes visible when the spatial (or territorial) aspect of privacy is considered (Macnish, 2018, p. 429):

> Throughout this paper I have concentrated on privacy of information, while acknowledging also that privacy is a concept that applies to space. I can have a private space and you can invade that private space without gaining any new information. Imagine I tell you the exact contents of my bedroom. Shortly thereafter you visit my house and, without my permission, go into my bedroom. You will have gained

> no new information but you will nonetheless have invaded my private space. Could a similar argument be made in terms of state intelligence agencies having access to my email?

If Macnish's account of privacy is to concern only information privacy and even that only outside the problem of mass surveillance and other forms of mass oversight, then the resulting theory does not carry much (or any) relevance to the contemporary challenges of public debate on privacy, other than a message comparable to the first solution to the problem of privacy and surveillance, which proposed to forget the definition and focus on lawmaking.

In what follows I propose that we treat the gateway theory of privacy as a compromise between the control and access approaches, but instead of focusing on information, treat privacy as means of protecting zones of activity as defined in section 1.3. The proposed theory satisfies the conditions put forth by Menges (2020) that threatened loss cases are not automatically classified as privacy loss, although mass surveillance is classified as such. It is not surprising that adopting the view of the NSA on the problem of surveillance, as Menges (2020) and Macnish (2018) effectively did, results in a temptation to justify that mass surveillance does not constitute a loss of privacy, despite our strong intuitions to the contrary. However, an adequate theory of privacy should avoid siding with any of the radical fronts described in section 1.3.4, especially when the theories they lay out have been proven to be mere pretexts for privacy violations.

Additionally, the gateway theory allows for incorporating the subject matter lost in the theory proposed by Macnish, including the territorial aspect of privacy protection.

1.3.6 The gateway theory of privacy as a middle ground

Access to a zone of activity is similar to having access to a house, or another protected physical space. Namely, it is enough to have a key or know of another infallible way of entering to have actual access to the house. This territorial understanding of access may be helpful in explaining the role of gate keeping in privacy. We are in control of our privacy if and only if we alone control all the gateways to the zone of activity which we wish to protect. We may allow others access to the zone or access to a particular gateway to the zone. In the former case, take a corporate executive who allows his secretary to open the work related mail that arrives at the office. The secretary is allowed to inspect the contents of the mail and process them according to the instructions provided by the executive, for instance, to destroy spam and relay all messages which the secretary deems important. In this case, the executive authorized her secretary to access

a gateway to the zone of professional cooperation, but not to the zone itself. Therefore, the secretary is not authorized to search other work related documents of the executive or to listen in on her phone calls.

Authorizing access to the full zone of activity is a much rarer occurrence. Take a smart watch which measures the speed and direction of movement, the heart rate and the geographical location of a runner throughout the training session. The runner may chose to give access to her zone of activity, *e.g.*, training in preparation to a marathon, either to her coach or to a non-person, that is, to the application installed on the device which automatically generates statistics and returns recommendations based on collected data, without relaying the data further or using it for any other purpose. If, however, the owner of the app chooses to make use of the provided information to tip the insurance company about the life expectancy of the runner, it constitutes a breach of privacy and not because of the lack of control or access to data (information), but because the company used access to one zone of activity (training) to invade without consent another zone of activity (relationship with the insurer) of the runner. In light of the gateway theory of privacy, the catalog of authorized uses for collected data should always be exclusive, not open. In other words, the company cannot guarantee the legitimacy of its use of data simply by making the user agree that company processes the information as its see fit. Those zones of activity which are private (that is, the gateway to which are protected by the user), remain outside reach of the company and other parties as long as an explicit consent for accessing the specific zone of activity or a specific gateway to it are not given.

From now on whenever I will refer to *privacy* it is to mean privacy in the sense of gateway theory. For each case and context, to talk about privacy I will need to identify what zones of human activity are involved and what number and types of gateways provide access to these zones.

1.4 Embedding political privacy in political philosophy

In section 1.3, I proposed a general definition of privacy, where a person, group or a collective has (or maintains) privacy *relative to a given zone of activity* when they can authorize or deny access to this *zone of activity*. Such defined notion of privacy allows for a relatively straightforward transposition onto the realm of political activity of the citizens.

For each case of interest, one asks: does this particular citizen, a group of citizens or a collective maintain their privacy relative to the defined zone of activity? And since identification of relevant citizens, groups and collectives usually poses little problem,

the only question critical for applying the general notion of privacy to political activity lies in listing all the specific zones of activity which require protection. Zones of activity which are related to political privacy will be referred to as *zones of political activity*. And since in this dissertation I am primarily interested in the privacy solutions needed for facilitating a democratic system with the rule of law, I will consider three approximate thresholds of democracy's privacy conditions.

The first threshold to pass is that of *critical political privacy*. If this level of protection is not reached, citizens of a given state have no privacy relative to *the critical zones of political activity*, such as choosing (directly or indirectly) their political representatives in areas where representation is standard (*e.g.* their parliament), exercising their freedom of speech or organizing political gatherings without the threat of retribution or violence. Essentially, the critical zones of political activity are those without which one may no longer speak of a democracy, even when labelling it as "crippling" or "struggling". Accordingly, I define *critical political privacy* by referring to the notion of critical zones of political activity. An important caveat here is that all three categories for political privacy which I propose here are relative to a catalog of specific zones of activity which are needed to satisfy the conditions mentioned in the definitions below. For instance, in case of critical political privacy, one needs to ask which specific zones of activity must be protected to ensure minimum active involvement in the political system. This catalog is up for debate to a certain extent, but I will propose how it may be formulated in chapter 5.

Definition. *A person, group or a collective has (or maintains) critical political privacy when they can authorize or deny access to the critical zones of political activity, that is those zones of political activity which are necessary for their minimum active involvement in the political system of a given country.*

The next step from the perspective of privacy development is to reach the level of *baseline political privacy*. At this stage, one likely starts to categorize the state as democratic, though perhaps flawed, based on the zones of political activity which are *de facto* (and not just *de iure*) available to the citizens. In a state classified at this level, citizens enjoy protections of some of the most basic rights and freedoms as a consequence of protecting their privacy in critical zones of activity. However, some of the services related to health care, social welfare, justice system, and so on, may be significantly flawed. For instance, social welfare may be conditional on allowing surveillance, which infringes on an important zone of political or personal activity.

Definition. *A person, group or a collective has (or maintains) baseline political privacy*

when they can authorize or deny access to the basic zones of political activity, that is those zones of political activity which are necessary for and which sustain their active involvement in the political system of a given country, with possible exceptions.

Finally, a flourishing democratic state in the context of privacy is one which reaches the threshold of full political privacy.

Definition. *A person, group or a collective has (or maintains) full political privacy when they can authorize or deny access to all standard zones of political activity, that is those zones of political activity which sustain and encourage their active involvement in the political system of a democratic state.*

Of course, there are many ways to fill in the skeleton of the three proposed definitions of political privacy with specific solutions. However, the most beneficial development here is that we may reduce some of the most worrisome controversies around privacy, for instance the question of whether the NSA had the right to conduct mass surveillance of the US and EU citizens, to specifying the relevant zones of political activity and the mode of authorization appropriate for each of them. One no longer needs to ask: but what do you mean by "privacy"? One only needs to indicate which zones of political activity were harmed and find the agent (directly or indirectly) responsible for the infringement. One is also free from the need to argue that *all surveillance is harmful* by definition.

In subsequent chapters, especially in chapter 5, I will indicate some of the most important zones of political activity related to the market and economic operation, participatory democracy and activism. For now, though, the notion of political privacy calls for more theoretical context. More specifically, one must place the question of privacy and political privacy in the theoretical framework typical of characterizing political philosophies. This framework involves five fundamental concepts, that of an individual, society, property, authority and the state.

In political philosophy, many of the classical stances may be characterized by referring to the concepts of an individual, society, property, authority and the state (Rau et al., 2018, pp. 20-26). First, one defines the features for each of these elements. Here I will briefly mention two examples of political philosophies, that of John Rawls and James Buchanan, as an illustration of how the five concepts can be made concrete in different ways.

John Rawls (1971) viewed an individual as a rational agent, a being conceiving of justice. Rawlsian society is a result of contract and a forum of social cooperation, while the state is the institution which guarantees social justice, including just redistribution

of goods. The meaning of property and authority are instrumental for Rawls. The latter is an instrument of redistribution of goods, the former – a condition needed for living an acceptable life and its rational planning (Ober, 2021).

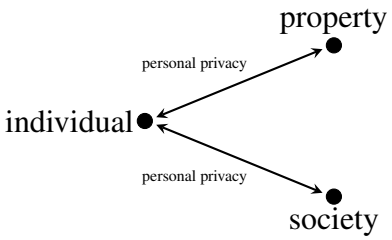


Figure 1.1: Personal privacy in relation to the society, individual and property.

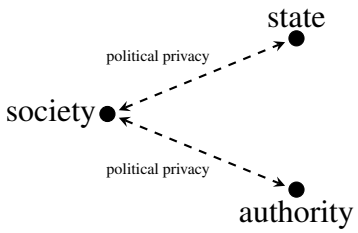


Figure 1.2: Political privacy in relation to the state, authority and society.

James M. Buchanan proposed very different definitions of these concepts. Namely, an individual is equated with *homo oeconomicus* (Kirchgässner, 2014), while society is defined as a simple aggregate of individuals, being approximately reducible to them (Buchanan and Tollison, 1984). For Buchanan, the state (and not the society) is the result of contract. Moreover, Buchanan pays a lot of attention to the role of property, as the guarantee of freedom and security of its owner, and the state, defined as a collection, an institutionalized bundle of guaranteed such as property (Brennan et al., 1980; Buchanan, 1968).

When addressing the question of privacy, one does not need to immediately choose any specific political philosophy, but it may be helpful to develop one's intuitions about privacy in relation to the five central concepts of a political philosophy. In differentiating privacy *sensu largo* from political privacy, I argue that their relations to the five concepts are different, as shown in figures 1.1 and 1.2.

While political privacy creates a direct link between the society, authority and the state, and only indirectly concerns the individual (insofar as political privacy depends on personal security and freedom), the *remaining* scope of privacy, which I will refer to as *individual privacy* or *personal privacy* relates an individual to society and property.

A lot of the confusion behind public conflicts concerning privacy is due to a mistaken view that the problem of privacy concerns primarily the relationship between an individual and the society. Often enough, communal or national security is framed as "public" good opposed to the individualistic, particular interest of one citizen. This way, the surveillance authority may try to follow the same logic as they would in case of any

other communal contribution. For example, taxation is also something that an individual has to endure in order to contribute to an emergent value, the national or regional budget. Similarly, the positive effects of this contribution may remain unnoticed at an individual level. Individuals sacrifice a part of their income and receive security in the form of public services, which ultimately benefit them more than their untaxed capital would otherwise.

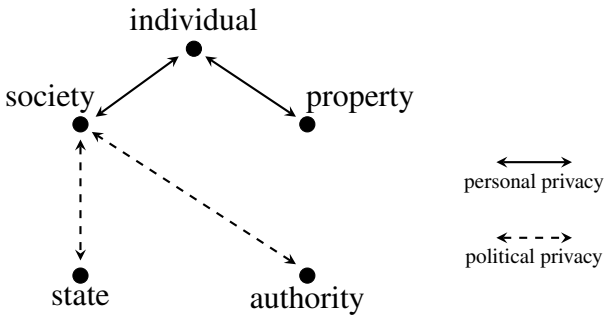


Figure 1.3: Orienting personal privacy and political privacy among the five key concepts of political philosophy.

In trying to reinforce the intuition that privacy violations are like taxation, surveillance authorities often focus the public attention on the benefits of surveillance, suggesting that, similarly as in case of capital redistribution, privacy also can be an object of cost-benefit analysis. However, not only there does not exist any sort of market where privacy redistribution may serve as a regulatory force, privacy, at least in the political sense, is nothing like taxation or other social contributions. One the reason for this is that, in the political dimension, privacy concerns the relationship between the state, authority and the society, and only indirectly between the first two and individuals.

This connection becomes clear when the fundamental notion on which privacy is built shifts from superficial vehicles (such as information or situation) onto more substantial building blocks, such as zones of (political) activity, rooted in social relationships and social structures. Of course, one can only conduct surveillance of groups and collectives *via* surveillance of individuals, which is why privacy as an individual right will always require protection in the context of political activity. In the context of surveillance, the primary target of which is the process of communication, society

together with its groups and collectives may be reduced to an aggregation of individuals, where each individual is a vertex in a large graph of information flow, emitting and receiving information. But of course, communication theory, or graph theory for that matter, do not yield a satisfactory representation of political activity in a society, and especially of its projective, normative goals. Moreover, the protection of social relationships and other zones of activity which *emerge* from (hence, are not reducible to) the involvement of individuals, cannot be fruitfully discussed using a language which presupposes said reduction. My proposal for the new theory of privacy aims to level the ground for privacy debates, allowing the stakeholders to (i) identify and defend specific zones of activity of strategic political importance, and (ii) demand the introduction of specific legal and technical solutions necessary for protecting political privacy. Conversely, surveillance authorities may rely on the proposed theory of privacy in proving that their activity is socially beneficial and does not necessarily infringe on the zones of political activity which are of strategic importance.

1.5 Summary

In this chapter I discussed some of the most fruitful theories of privacy proposed in law, politics and philosophy since the early 20th century, when Cooley (1906) argued for "right to be let alone", later developed into the first American notion of privacy by Warren and Brandeis (1890, 1984). I highlighted the valuable aspects of the historical theories of privacy, as well as analyzed their most serious problems. In this endeavor, I aimed to identify among them a theory which would satisfy the following aforementioned criteria:

(a.) the core of the framework must be independent of terms strictly related to the current state of technology;
(b.) the framework must be centered not around the means of privacy protection, but around the ultimate value to which privacy is instrumental, that is, human life, dignity and activity;
(c.) the framework must support a theory which is cross-disciplinary and uniform throughout contexts and cultures;
(d.) but must at the same time allow for differentiating between individual or social (communal) discovery of person's life and the discovery conducted by the state;
(e.) the resulting theory must allow for abstracting away from those social, political and economic convictions which are not necessary.

Since none of the existing theories of privacy allowed for obtaining a satisfactory framework, I proposed my own general theory of privacy, which I called *the gateway theory of privacy*. According to the gateway theory of privacy, a person has the benefit of privacy when she can authorize or deny access to her *zone of activity*, defined intuitively as the domain of affiliated behaviors the consequences of which are restricted to the boundaries of this domain. The name *gateway* is due to the observation that the person will be said to have privacy with respect to a given zone of activity if she controls all its gateways, where a gateway is understood as a point of access (physical, digital, or otherwise). Note that, as I argued before in section 1.3, the zones of activity, although comprising of various instances of behaviors, are not reducible to them. Rather, a zone of activity presents an emergent value, which, similarly to the notion of a situation, can gain communal recognition or not.

Based on this general theory of privacy, I proposed a theory of political privacy. Instead of focusing the theory on the person of a politician *v.* a civilian or a citizen (as is customary, *e.g.* in the French legal discourse on privacy), I gave the theory of political privacy bases in *political activity*, which gives rise to *zones of political activity*. Since in this dissertation I am predominantly interested in the privacy tools facilitating a democratic system with the rule of law, I introduced three approximate thresholds of democracy's privacy level, to be made more precise later in chapter 5.

First, a person, group or a collective has (or maintains) critical political privacy when they can authorize or deny access to the critical zones of political activity, that is those zones of political activity which are necessary for their minimum active involvement in the political system of a given country.

Next, a person, group or a collective has (or maintains) baseline political privacy when they can authorize or deny access to the basic zones of political activity, that is those zones of political activity which are necessary for and which sustain their active involvement in the political system of a given country, with possible exceptions.

Finally, a person, group or a collective has (or maintains) full political privacy when they can authorize or deny access to all standard zones of political activity, that is those zones of political activity which sustain and encourage their active involvement in the political system of a democratic state.

In section 1.4, I presented a way of placing privacy in a general framework of political philosophy and argued that the confusion behind public conflicts concerning privacy is often due to a view that the problem of privacy concerns primarily the relationship between an individual and the society. I also argued against the view that in the context of privacy communal or national security is a "public" good as opposed to the individualis-

tic, particular interest of one citizen. Hence, it is not a valid behavior for the surveillance authority to follow the same logic as would obtain for just any other communal contribution requiring individual sacrifice.

Chapter 2

Three models of regulating privacy

The relationship between privacy as a political, ethical and philosophical concept and *the right to privacy* (together with appropriate *privacy laws*), that is, privacy as a legal institution, is strictly hierarchical. While the right to privacy often guides our intuitions about solving privacy-related problems, it remains, at least from the scientific perspective, secondary to the political and ethical discourse on privacy. This is not to say that privacy at the most basic level is a purely normative concept. On the contrary, societies often differ in their perceptions and expectations related to privacy, including certain solutions regarding political privacy. However, if one is interested in the relationship between privacy and the rule of law, privacy becomes a projective concept, one subject to conceptual engineering methods (see section). One asks: what kind of privacy theory facilitates the needed legal and social solutions in the context of modern democracies? This question differs in nature from both a purely normative "what *should* privacy be like?", and a descriptive "what *is* privacy like in the current state of affairs?". Legal analyses typically focus on the latter, while ethics targets only the non-political aspect of privacy. Some of the more prominent ethical and philosophical theories were discussed in section 1.2. In this chapter, I discuss case studies, which will reappear in the subsequent chapters, namely, the right to privacy as it functions in the legal systems of France, Germany (together with the EU regulations), the US and China.

But why discuss the law when, as was just indicated, the law is only a by-product of the political considerations on privacy? And, also, what motivates the choice of the case studies? The answer to the first question follows from the feedback between the law and socio-political attitudes of the stakeholders. Although the law does not provide any definite or reliable indication on what privacy or political privacy actually is or should be, it does influence stakeholder's intuitions, simply because being born or living

in an ecosystem of specific laws shapes one's thinking. This, in turn, is likely to have strong effects on the types of arguments, theories and tools which emerge within privacy debates and controversies. The choice of case studies is guided by this perspective as well. The European privacy solutions often revolve around two major forces in European international politics, France and Germany. The US and China compare sharply with the European solutions, both because of the historical developments, but also because they both take a different approach to democracy and modern governance. Socio-political intuitions concerning privacy will be extremely different in China and those will be reflected in the Chinese privacy laws. In case of the USA, political solutions have been documented to exceed the bounds of the national constitution as well as violate the public's borderline expectations of privacy. Hence, the introduction into privacy laws is of methodological value – the three legal and political systems give rise to three main models of how privacy may be regulated. Knowing the current state of the law, one may adjust the evaluation of the arguments and solutions with respect to the legal and economic state of affairs which facilitated them.

2.1 The right to privacy and privacy laws in the EU

From a legal perspective, the right to privacy and the related laws and regulations are interconnected with regulations regarding other issues. For instance, Gonschior (2017) investigated the correlation between privacy law in the European Union and the laws concerning data protection. Although data does carry information, sometimes concerning the zones of activity protected by the right to privacy, the capacity for protecting privacy *via* protecting data is limited. Essentially, as was argued in section 1.2.3, privacy cannot be successfully interpreted as being about information or data, understood as the carrier of information. And so, although the legal landscape often suggests that the two domains, privacy and data protection, share a rather close connections, this is not to say that discussing privacy at a political (or even policy) level requires that one also decides the many problems of data protection.

In the legal system of the European Union, the right to privacy is considered a fundamental human right and is protected under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). Article 8 of the ECHR defines the right to privacy as a universal right to respect for private and family life, home and correspondence. It also imposes a limitation on the interference of the public authority to cases where the following conditions are satisfied: (1) there exists a law which permits the interference, and (2) the interference is necessary in a democratic

society in the interest of national security, public safety or the economic well-being of the country, prevention of disorder or crime, protection of health and morals, or for the protection of the rights and freedoms of others. In this rather general form, Article 8 does not constitute a functional basis for the system of privacy protection.

As Gonschior (2017, p. 241) indicated, the EU privacy protection system had to emerge somewhat independently from the initial versions of the Treaty on European Union (TEU), together with systems for protecting other fundamental human rights, which did not systematize the protection of fundamental human rights. In order to make up for this omission, the Court of Justice of the European Union (CJEU) within its judicial activity included fundamental human rights in the general principles of the EU legal system, which obtain in the process of interpreting and applying the laws and regulations following from the European treaties, including the TEU. Of special relevance here was the ECHR. Finally, in the Treaty of Lisbon, the rights and freedoms included in the ECHR have been acknowledged in Article 6 of the TEU. Thus, the ECHR was explicitly declared to hold the same legal value as the TEU and other EU treaties. Following the Treaty of Lisbon, the Charter of Fundamental Rights of the European Union (CFREU) came into force in 2009, bringing into one legally binding document the right and freedoms previously included in the EU Treaties, the ECHR, case law of the CJEU and the national constitutions.

Hence, at the most general level, the EU is bound to protect the privacy rights included in Article 8 of the ECHR. In the Treaty of Lisbon, Article 7 of the CFREU has been modified to concern a more robust interpretation of the right to privacy and refer to the rights guaranteed by Article 8 of the ECHR, except the word "correspondence" being replaced by a more contemporary "communications". As a result, the limitations which may legitimately be imposed on the right introduced in Article 7 of the CFREU are the same as those allowed by Article 8 of the ECHR. Notably, Article 8 of the CFREU regulates *separately* the right to *informational privacy*, that is, the right to protection of personal data. According to Article 8 of the CFREU:

> 1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
> 3. Compliance with these rules shall be subject to control by an independent authority.

Unfortunately for privacy protection, no counterpart for paragraph 3 has been established for controlling the compliance by public authorities with privacy regulations. Arguably, the European Commission currently functions as the privacy and anti-surveillance authority in relation to internal and foreign business agents, such as Facebook and Google. For instance, the European Commission conducted investigations into the process of Facebook's acquisition of WhatsApp, including privacy-related decisions, such as automated account merging between the two services. The Commission found that:

> When Facebook notified the acquisition of WhatsApp in 2014, it informed the Commission that it would be unable to establish reliable automated matching between Facebook users' accounts and WhatsApp users' accounts. It stated this both in the notification form and in a reply to a request of information from the Commission. However, in August 2016, WhatsApp announced updates to its terms of service and privacy policy, including the possibility of linking WhatsApp users' phone numbers with Facebook users' identities. (European Commission, 2017)

As a result of this misinformation by Facebook, the Commission has imposed a fine of 110 million euro. However, the investigation has been conducted under the trade and internal market scope of competence of the Commission, and not within a mandate of any privacy-focused body or authority. Similarly, the EU pursues privacy protection policies *via* data protection regulations. A good example of such regulation is the ePrivacy Directive. In December 2020, the ePrivacy Directive was expanded, including its regulations on user data retention period, the use of online and mobile platforms by the businesses and the standards concerning scraping data from messaging tools. Additionally, the expansion of the ePrivacy Direcitve has been accepted after the GDPR effectively upended Facebook's current business model (Denton, 2021) based on mass collection and practically unlimited use of user data. Although similar policy and regulatory decisions may be cited for other surveillance capitalist giants operating in the EU, a significant portion of the enforcement and oversight over compliance with, *e.g.*, the GDPR still lies in the hands of watchdog organizations, such as the Irish Council for Civil Liberties(Chan, 2021). Hence, although there seems to be potential for further development in privacy regulations in the Commission and other EU institutions, many elements necessary for full and functional privacy protection are missing, such as the effective channels of regulation enforcement and appeal.

Barnard-Wills (2013) conducted a horizontal analysis across a set of European legal documents, focusing on how the topics of privacy, security and surveillance are viewed within the EU policy-making process. Although the analysis offers limited generalization capacity, due to including only a selected sample of documents, the emerging trends

and patters are suggestive of the development of EU policy-making around security and privacy. The study found that although the policy discourse concerning security and privacy is not homogeneous, especially across the member state regulations, the EU-level governance has a strong impact on security and privacy practices. Barnard-Wills (2013, p. 175) indicated that the emerging position of the EU towards the conflicting solutions around privacy and security respect the fundamental rights and freedoms, rather than "balance" them with security. In other words, security solutions must be developed in a way which complements (and not contradicts) the fundamental rights and freedoms. However, although there seems to obtain a broad agreement across the EU policy documents about the core principles or privacy and data protection, the interpretation of these principles varies across member states (*cf.* sections 2.1.1 and 2.1.3). Even more worrisome is the fact that the EU and its member states seem to favor increased individual responsibility and control over systematic solutions, such as privacy by design (PbD) or developing privacy enhancing technologies (PETs). Although this approach strengthens the right of the "data subject" (or user), it falls short of providing default safe solutions to uninformed individuals.

Another major issue when interpreting the study by Barnard-Wills (2013) is the fact that state surveillance within the member states remains virtually unregulated at the EU level. Thus, to know more about the limitations on political privacy in the EU, it is necessary to examine in more detail the surveillance, security and privacy regulations in at least some of the member states. In the following sections I will analyze the regulations in France and Germany, the two countries which are major voices in the pan-European discourse on privacy and security.

2.1.1 The right to privacy and privacy laws in France

Similarly as other member states of the EU, France is in the process of implementing the regulations from the CFREU, the GDPR and the ePrivacy Directive, having previously implemented the minimal protections stemming from the ECHR. In this dissertation, the description of the relationship between the French legal system and pan-European law is left outside the scope of my considerations insofar they do not concern specific implementation issues. At the national level, the basis of the right to privacy is rooted in Article 9 of the French Civil Code:

> Chacun a droit au respect de sa vie privée.
> Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire

> cesser une atteinte à l'intimité de la vie privée : ces mesures peuvent, s'il y a urgence, être ordonnées en référé.[1]

The capability of a judge to prescribe urgent provisional privacy protection measures in a manner unlimited by the considerations of material (or other) damages incurred as a result caused Eko (2000, p. 16) to evaluate the French legal system as ultra privacy-focused: "Contemporary France has one of the most stringent privacy law regimes in the world. This regime is bolstered by a battery of statutes against invasion of privacy by the mass media." However, in the context of political privacy, two important provisions must be made here.

First, Eko (2000) and a number of other scholars who attempted to characterize the right to privacy in the French legal system (Trouille, 2000) consider privacy to be fully captured by "the intimacy of the private life" (*l'intimité de la vie privée*). This definition closely resembles the theory of privacy as freedom to act in personal matters (*cf.* section 1.2.2), and thus not only falls short of satisfying the goal of including political privacy, but compares unfavorably even with the dated theories such as privacy as restricted access (*cf.* section 1.2.5).

Even more worrisome is the way that Article 9 is used in the French legal practice. The usual cases of Article 9 in action concern politicians and celebrities, such as François Mitterrand, and help them protect their public image (Trouille, 2000, p. 199). By relying on the sharp division between public and private, the French Civil Code offers an extremely limited and outdated perspective on privacy violation (or infringement). Namely, surveillance of any kind does not, at least in principle, constitute a privacy violation on the basis of Article 9 unless the discovery of the private life does not become, in some sense, public. And so, contrary to the evaluation of Eko (2000), the French legal system by way of Article 9, welcomes all forms of state oversight, including mass and targeted surveillance, while deploying the measures of privacy protection to serving the interests political and financial elite against the scrutiny of the media and the public. In fact, rather than "privacy", a more appropriate word for *l'intimité de la vie privée* would be "limited transparency of a public figure".

There remain other ways to demand privacy protection in the French legal system, including legal actions based on employment law, administrative law, the French Criminal Code, as well as the so called "petition for civil liberties" and other solutions. Actions

[1] "Everyone has the right to have their private life respected.
The judges may, without bias towards the need for compensation for the damage suffered, prescribe all measures, such as sequestration, seizure and others, appropriate for preventing or putting an end to an invasion into the intimacy of the private life: these measures may, in urgent cases, be prescribed as a provisional measure" (Translation – AS).

in relation to data protection may be undertaken with the assistance of the French data protection authority CNIL (*Commission nationale de l'informatique et des libertés*, or the National Commission on Informatics and Liberty).[2] However, these practical pathways do not make up for the fact that the notion of privacy, hence also the full scope of the right to privacy, remain undefined on the grounds of the French legal system, as Eko (2000, p. 17) and Wagner (1971, p. 45) pointed out.

2.1.2 France as a surveillance state

In this section, I briefly sketch the legal aspects of the surveillance solutions adopted by the French government and various policing and oversight agencies. Dambrine (2015) offered a summary of surveillance law as of 2015, when the state of emergency has been introduced, following a series of terrorist attacks which saw as many as 130 people killed, with the Islamic State claiming responsibility.

Since 2015, the French National Assembly considered the counter-terrorism legislation proposed by Emmanuel Macron's government, where the state of emergency allowed extended powers of repression and tools of surveillance to state authorities. McQueen (2017) claims that since the application of the law about the state of emergency in 2015, the existing regulations have widely criticized as enabling human rights abuses. Based on the proposals by the Macron administration, some of the most controversial elements of the state of emergency powers were to be constituted as permanent powers of the French state authority, including, but not limited to: granting police the right to place individuals under house arrest without trial, to raid homes and meeting places without judicial consultation, and to ban public gatherings. What is important here, these measures have been applied almost exclusively against Muslim citizens, especially those who were "visibly Muslim" (McQueen, 2017). What these changes demonstrate is a trend to direct surveillance measures against citizens and communities whose background has been designated as undesirable or in some way problematic by the state authorities. Here, a default link has been established between Muslim identity and terrorism though a premise that Islam automatically leads to political "radicalization" and aggression. This link, although not formally declared, can be inferred from how the state of emergency laws have been applied in practice. Another community which has been demonstrably discriminated against *via* extended surveillance mechanisms is the African migrant community, where the politicization of state surveillance fulfilled multiple goals, including discouraging and limiting migration of African nation-

[2] See Rachel and Amrani-Mekki (2012) for a detailed exposition of the available legal actions.

als to France, reverse the migration, and enable the creation and testing of tools which can be used outside the context of migrant communities (Glaes, 2018). I will discuss the psychological aspects of surveillance used in the process of "othering" in section 4.2.5.

One of the fundamental reasons why robust surveillance practices are viable in France is the lack of protection against surveillance in the French civil and constitutional law, as explained in section 2.1.1. Another important observation concerning the *de facto* evolution of state surveillance in France was offered by Gillis (1989). From the historical perspective, state surveillance, despite being marketed to the public as a class of measures targeting primarily violent crime, including major crime such as terrorism, has been demonstrably effective in preventing property crime in the second half of 19th and 20th century, but its impact on violent crime in urban environment has been minimal. Moreover, based on extensive historical and statistical evidence, Gillis (1989, p. 307) indicated that:

> A reversal of the equations shows that crime rates had little or no effect on the growth of national policing. This, and historical evidence, suggests that state surveillance expanded less from a specific intent to control crime than from a broader interest in repressing "dangerous classes," new repertoire of social protest, and political challenge to the state.

Tréguer (2016, p. 34) pointed out that the French legislative proposals, especially since the French 2014 Anti-terrorism Law, "greatly reinforced the power of intelligence and police agencies by circumventing traditional criminal procedures". A clear shift can be observed in the development of surveillance state in France in the recent years: from a court-controlled, publicly mandated surveillance, the country is moving towards a covert, discretionary toolbox of policing solutions. As for the 2015 Intelligence Act, Mastor (2017) observed that the focus of the French surveillance regulations was not on counter-terrorism, a solution which would require judicial oversight of policing and surveillance activity, but aligns with the prioritization of property protection in French state surveillance efforts as postulated by Gillis (1989).

2.1.3 The right to privacy and privacy laws in Germany

The protection of privacy in Germany is often proxied through data protection laws, such as the federal Bundesdatenschutzgesetz (BDSG) and related laws in *Länder* and other area-specific regulations. However, as was said in section 2.1, data protection is not quite the same as privacy protection, as privacy extends far beyond the activity expressed in data.

According to Krause (1965), the emergence of the laws protecting the right to privacy in Germany was followed by over 50 years of bottom-up efforts to interpret privacy protections out of the existing law on the side of German legal community. Similarly as was the case with Warren and Brandeis, who postulated *the right to be let alone* on the grounds of the American legal system (*cf.* section 1.2.1), in Germany the original initiative in privacy came in the form of *a general right of personality* proposed by Von Gierke (1895, 702). Krause (1965, p. 485) noted that:

> [T]he German right of personality derives from von Gierke, who first dealt with the problem in 1895. Many German jurists who were contemporaries of Gierke supported his suggestion that the law should recognize a "general right of personality." Thus, the right of personality met with early success in terms of theoretical acceptance, but it did not find a place in the German Civil Code (BGB) of 1896.

The right of personality, remaining outside the code of law, has not been met with support in the courts either. Cases which involved the right of personality were decided on the basis of other laws, such as the copyright law, or *via* judicial constructions over laws such as that in Article 826 of the BGB (Bürgerliches Gesetzbuch, the German Civil Code of 1747), interpreted so as to include protections against intentional invasions of privacy violating "good morals" (Smoschewer, 1930; Krause, 1965). A breakthrough came in 1954, when the Bundesgerichtshof (BGH, the German Federal Court of Justice) derived court derived the right of personality from Articles 1(1), 1(3) and 2(1) of the 1949 West German constitution (Grundgesetz 1949), which included an extended catalog of basic human rights (Spevack, 1997, p. 411). The first two articles of the 1949 Grundgesetz have the following form:

> Artikel 1 [Menschenwürde, Rechtsverbindlichkeit der Grundrechte]
>
> (1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.
>
> (2) Das Deutsche Volk bekennt sich darum zu unverletzlichen und unveräußerlichen Menschenrechten als Grundlage jedermenschlichen Gemeinschaft, des Friedens und der Gerechtigkeit in der Welt.
>
> (3) Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht.
>
> Artikel 2 [Freiheit der Person]

> (1) Jeder hat das Recht auf freie Entfaltung seiner Persönlichkeit,soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.
>
> (2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.[3]

Hence, the right to express one's personality freely (*das Recht auf freie Entfaltung der Persönlichkeit*) became the basis for privacy protection. Interestingly, this provision corresponds to one of the most fundamental zones of activity (in my sense of the term) necessary for living a fulfilling life, that is a need for self-development and exercising the sense of agency, *e.g.*, one's strive for unsupervised experimentation and interaction with oneself and the environment (*cf.* section 1.3). The right of personality thus formulated also allows for extension onto the relationships with others as far as these relationships are considered a natural part of self-expression. Standard limitations on privacy infringement and violation, possible only on the basis of the code of law, echo the solutions of the ECHR. The German Civil Code was promptly amended so as to reflect the protections included in the 1949 Grundgesetz, but the right of personality in its totality was omitted in the codification process, because it was considered too difficult to define and was left for further informal maturation.

Regardless of its position in the codified civil law, the right of personality was considered a source right (*Quellrecht*), from which other rights are *de facto* derived in judicial interpretation. Among them are, *e.g.*, the right to protection against undue invasion of privacy of employees and employee candidates, the right to have a dog, the right to inquire into one's own parentage in court, and many others (Krause, 1965, p. 501).

Taylor (2002, pp. 75-76) observed that on the basis of the subject matter of Niemietz *v.* Germany (1992), a case involving German state surveillance regulations, the Eu-

[3] Article 1 [Human dignity, legally binding nature of fundamental rights]

(1) Human dignity is inviolable. It is the duty of all state authorities to respect and protect them.

(2) The German people are therefore committed to inviolable and inalienable human rights as the basis of every human community, of peace and justice in the world.

(3) The following basic rights are binding on legislation and executive power and jurisprudence as directly applicable law.

Article 2 [Freedom of the person]

(1) Everyone has the right to free expression of his personality, as long as he does not violate the rights of others and does not violate the constitutional order or the moral law.

(2) Everyone has the right to life and physical integrity; the freedom of the person is inviolable. These rights may only be encroached upon on the basis of a law .

(Translation – AS)

ropean Court of Human Rights found that individual's privacy must by necessity extend beyond the most "private" (*i.e.* personal) matters and relationships. Therefore, the Court's interpretation of the individual's "inner circle" echoes the basic intuition behind the notion of zones of activity. Namely, the "circle" or the zone in which the individual may be free in living as she or he wishes must not be limited so as to completely exclude the outside world. To respect the private life of an individual, the Court concluded, is to recognize and protect her or his right to develop relationships with other human beings.

Moreover, the Court pointed out in the context of Niemietz *v.* Germany, that:

> There appears, furthermore, to be no reason of principle why this understanding of the notion of 'private life' should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest opportunity of developing relationships with the outside world (Taylor, 2002, pp. 75-76).

Thus, as Taylor (2002) also observed, the idea that "privacy vests in people", not places, situations or information, took root in the judiciary solutions at the EU level, as a response to the limiting interpretations of the right to privacy followed by German national judiciary in the case. An important lessons follows from this trend, that is, privacy can and should be exercised and protected also in situations and contexts which one would consider intuitively "public". In the words of Harris et al. (2014, p. 309): "the expanding understanding of private life set out in the Niemietz case indicates that a formal public/private distinction about the nature of the location will not always be decisive". This is to say that the traditional public/private intuitions, in operation especially in the French legal interpretations of privacy (*cf.* section 2.1.1), but also persisting in German judicial rulings as in case of Niemietz *v.* Germany, are no longer a reliable indication of the scope of privacy protection.

2.1.4 Germany as a surveillance state

The social and institutional circumstances which facilitate the emergence of mass surveillance and state surveillance in Germany are rather special. While legitimacy deficits to state surveillance are still significant in Germany, the state authorities look to legitimize surveillance operations based on the *possibility* of retroactive investigation of national security threats (Schulze, 2015). However, the social reception of state surveillance activity is much more negative in Germany than, for instance, in the USA. This includes strong social opposition to the covert system of policing, which Ross (2007) linked with a high degree of conflict with higher-order norms accepted in the German society.

Consequently, German law imposes stricter regulatory constraints on the initiation and conduct of undercover operations as compared to most EU member states and the USA.

In this section, I signal the main legal solutions which enable state surveillance in Germany as well as the ramifications concerning the *post factum* transparency of the surveillance process, which are typical of the German legal system and law enforcement (Broeders, 2009).

One of the characteristic elements of state surveillance in Germany is the fact that the German government and surveillance authorities have implemented, at least to a certain extent, limitations and due countermeasures which the citizens may take to retroactively challenge the rightfulness of their own surveillance. One of these solutions is known as *the right to notification* and followed from the 1978 ruling of the European Court of Human Rights (ECtHR) in Klass *v.* Germany (Hert and Boehm, 2012). Referring directly to Article 8 of the ECHR, ECtHR laid down basic criteria limiting the power of the EU member states to conduct surveillance. The catalog of limitations was further specified in subsequent rulings, while the right to notification was transplanted into the 1995 Data Protection Directive, based on the relative proximity of measures supporting data protection and those against state surveillance.

In Shimovolos *v.* Russia ruling, to which German privacy protections laws refer to, the ECtHR indicated that the surveillance measures must be worded clearly enough for the citizens to be able to understand the conditions and circumstances in which the authorities are in power to entertain any measures of secret surveillance or collection of data. Moreover, a series of *minimum safeguards* is to be specified in statutory laws, including the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise the measures, as well as appropriate countermeasures available. These safeguards, especially the countermeasures to surveillance, are meant to increase the level of public scrutiny and decrease the risk of abuse of the system of surveillance, the risk which is very high in the context of full secrecy. Hence, the ECtHR clearly linked secrecy to the potential for abusive discretionary actions. In terms of data protection, the right to notification is well-established in the EU legal system, as well as the national systems of the member states, Germany included. However, the right to notification for state surveillance is a relatively recent development and so far has been only implemented in Germany. Essentially, the right to notification requires that individuals be notified about the fact that they had been under surveillance, though only after the surveillance ceased.

In case of Germany, the impulse to increase state surveillance safeguards came again in 2006, after the ECtHR ruling in Weber and Saravia *v.* Germany, where the amendment

of German G-10 Act[4] was contested. The name of the act refers to Article 10 of the German Basic Law, which enables the protections of the right to privacy of communication, and from which the G-10 Act derogates.

As for the right to notification, the ECtHR stated that the right is directly linked to the effectiveness of surveillance remedies before the courts and court scrutiny of surveillance. Consequently, the right to notification is one of the milestones, although by no means a sufficient one, in preventing abuse of power in surveillance. The ECtHR stressed that the measures against circumventing the right to notification, *e.g.*, by claiming that the notification might reveal the working methods and fields of operation of the intelligence service, must be put in place, so as to make the intelligence possible without undue infringement on the surveillance countermeasures. This can be partly guaranteed by putting in place an independent commission, such as the G-10 Commission in Germany. The G-10 Commission supervises the application of the G-10 Act and decides whether the notification of an individual is due.

What the case of the right to notification in Germany demonstrates is that the solvability of the surveillance-security conundrum is much higher than commonly anticipated. Moreover, some appropriate anti-surveillance measures and tools have been put in place *via* the rulings following the cases which German citizens brought against their state. This of course does not mean that Germany as of 2021 is not a surveillance state, or that the German government is actively limiting itself to necessary surveillance measures in the name of democracy and the rule of law. But the success in societal pressure for the full implementation of the right to notification in Germany signals that pro-democratic security solutions are not only possible, but also feasible.

2.2 The right to privacy and privacy laws in the USA

Due to the fact that the right to privacy in the American legal system suffered a major practical restriction after 9/11 attacks on the World Trade Center and the Pentagon, a detailed analysis of the laws which had been in power before this event would tell us little about the current state of privacy protection in the USA. Some theories of privacy, including strictly legal theories, such as, for instance, the theory of privacy as freedom to act in personal matters presented in section 1.2.2, had emerged in reaction to the impact of the laws and technologies of the time on the quality of life of individuals. This theme in the construction of the notion of privacy proved detrimental to the modern debate

[4]The G-10 Act is the German counterpart of the 2000 Regulation of Investigatory Powers Act of the UK, or the Foreign Intelligence Surveillance Act of the United States.

on mass surveillance, in that it facilitated the argument that privacy is not diminished, unless an individual knows that they are being under surveillance (or their data collected) and a subjective feeling of shame or humiliation is inflicted upon them.

What is constant in the landscape of privacy protection in the USA, however, is the lack of constitutional bases for the right to privacy. This problem prompted a range of creative legal solutions, including (1) approaches which aim to reinterpret the text of the the United States Constitution and the United States Bill of Rights[5] in a way which makes the most of the available limitations on the powers of surveillance of the government, and (2) approaches which focus on state protection of privacy and case law. The latter is well exemplified in adopting explicit privacy protection clauses and acts by the states of Alaska, California, Florida, Montana and Washington. These and other states have independently adopted various solution concerning consumer privacy, citizen privacy, freedom of the press and freedom from censorship or oversight. Similarly, a number of cases have strengthened the judicial protection of privacy (see Strahilevitz (2010) for a thorough review of privacy-related cases), but at the same time resulted in even further diversification of the patchwork of state protections and regulations of the right to privacy. This prompted Strahilevitz (2010, 2012), Baude and Stern (2015) and Schwartz and Peifer (2010), among others, to stress the need for reunification of American privacy laws and creating a positive (as opposed to partial and implicit) model of privacy in the American legal system.

The former approach, that is, a program of reinterpreting the existing constitutional provisions in a way which makes explicit the minimum privacy protections, is in itself a philosophically progressive stance, especially considering the baseline of the American legal theory and philosophy. One of the key interpretative frameworks used in American legal theory and doctrine, especially favored by conservative and ultra-conservative jurists and judges such as the late associate justice of the Supreme Court of the United States Antonin Scalia, is originalism and its even more regressive form, textualism. Originalism requires that in interpreting any legal text, but Constitution and other foundational documents in particular, one only aims to recapture the original intent and meaning of the text, and refrains from adding to or updating even the most straightforward elements of the legal clause(Whittington, 2013, p. 379). Textualism goes even further in that it requires that a legal interpreter only seeks the ordinary meaning of the legal text and pays no attention to any of the extra-textual elements of the law, including the intention of the law. Fortunately, as Weis (2013, p. 842) observed, originalism

[5]Transcripts of both documents may be found US National Archives, url: https://www.archives.gov/founding-docs (Accessed May 10, 2020).

and textualism are "typically thought to reflect uniquely American anxieties about the judicial expansion of rights and the place of popular constitutional culture in judicial review" and have of been of little to no interest to legal and constitutional scholar outside the American conservative circle, especially since a number of justifications behind originalist interpretations do not hold without relying on the existence of a higher power or some such instance, which makes a legal text in some way similar to a religious text. In the USA, however, any reinterpretative legal project stands in direct opposition to both of these formalist theories of legal interpretation and may therefore be considered progressive in spirit, at least by the conservative wing of the American judiciary. Having acknowledged the specificity of the American context, one must note that in the legal culture of the European Union, as well as most other legal cultures around the world, reinterpretation of legal text according to new meanings of words and phrases is absolutely standard and is considered a normal process related to so called open texture of the legal language. As such, reinterpretation is commonly used by both progressive and conservative jurists outside the US.

One of the reinterpretative projects of the US Constitution was described by Heffernan (2016), where attention is given to the Constitutional limits to the government's intrusion into the right to privacy of individuals, especially those worded in the First, Fourth, Fifth, Ninth and Fourteenth Amendments. The First Amendment establishes the right to free assembly, which in itself broadens privacy protection requirements, as well as freedom of speech and the press (*cf.* transcript in the US National Archive):

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

The Fourth Amendment originally aimed to protect the citizen's spiritual and intellectual integrity, which echoes the early versions of the German general right of personality (see section 2.1.3). It states that (*cf.* transcript in the US National Archive):

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

In requiring that searches and seizures be *reasonable*, the Fourth Amendment placed itself in the very center of the contemporary conflicts between the American surveillance

authorities, such as the NSA, and the American citizens. One of the guiding questions in the debate on mass surveillance in the US is whether the mass collection of data constitutes a search (even before the authority inspects the collected data), and if so, whether the search is reasonable. One of the most dangerous pitfalls in this debate is the claim that the authority does not violate the Fourth Amendment by merely collecting the data *en masse* (hence no search takes place at all) and that the data is only actually inspected (searched) when probable cause arises, for instance, when specified keywords are used or when an individual is singled out independently as an element of a network of interest. Of course, this argument relies on wrongfully equating data collection with a search and not a seizure, but it suffers from other problems as well. The most critical is that of oversight and discretionary actions of the surveillance authority. Based on the case law related to German privacy regulations, one can conclude that there exist ways to limit discretionary actions and surveillance abuses without compromising the intelligence prorities of the state. The fact that this observation does not even emerge in the American context is in itself telling of who decides on the structure of the legal discourse in this case.

If the government of a surveillance authority violates the Fourth Amendment in order to collect evidence against a citizen in a criminal case, the Fifth Amendment is likewise violated automatically. The Fifth Amendment states the following (*cf.* transcript in the US National Archive):

> No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

The US Supreme Court also recognized the Fourteenth Amendment as a basis for substantive due process of right to privacy. This was also reflected in case law, including the aforementioned Griswold *v.* Connecticut from 1965, Roe *v.* Wade from 1973, which concerned the role of the right to privacy in protecting the right to an abortion, and Lawrence *v.* Texas from 2003, which concerned the right to privacy regarding the sexual relations of same-sex couples. The Ninth Amendment is also considered as relating indirectly to the right to privacy in stating that (*cf.* transcript in the US National Archive):

> The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.

The Ninth Amendment gained relevance only in the 1980s and afterwards, when it helped oppose the arguments of some jurists that unless the right is explicitly listed in the US Bill of Rights, it does not obtain in the US legal system (Lash, 2004, p. 422). In its straightforward declaration of an open catalog of rights and liberties of the citizens, the Ninth Amendment also invalidates the legitimacy of textualist theories of legal interpretation in relation to the US Constitution and the US Bill of Rights.

2.3 The US as a surveillance state

The right to privacy, and especially its intricate relation to security which emerged in the context of mass surveillance technologies, took center stage in the American public debate after the public discovery of evidence collected and released to the press by a whistleblower, Edward Snowden. This event prompted immediate attempts to refute the motivations and meaning of Snowden's whistleblowing. For instance, Inkster (2014) claimed that no mass surveillance proper took place, because the NSA did not take action against all persons whose data it collected, that Snowden did not understand the meaning of evidence he collected, and that the entire operation was nothing but a particularly dangerous form of stealing for a government authority. Almost immediately, positions such as this one have been overtaken by voices of appreciation and calls for scrutiny of the revealed evidence. Among them was the former Vice President Al Gore, who famously said (Goldenberg, 2013):

> [The NSA] in my view violates the Constitution. The Fourth Amendment language is crystal clear. It isn't acceptable to have a secret interpretation of a law that goes far beyond any reasonable reading of either the law or the Constitution and then classify as top secret what the actual law is.

The development of the US surveillance state has as of 2021 been the subject of a massive body of literature, both academic and political. For the purposes of a brief sketch of legal changes and their consequences, I will discuss only the four critical turning points. Namely, the legal-political fallout of the 9/11 attacks on the World Trade Center, the resulting NSA abuse of power as revealed by Edward Snowden, the strong push toward encryption on the side of surveillance capitalists such as Apple and Google, and the consequences of the breakthrough following the whistleblowing initiative of Edward Snowden.

2.3.1 The 9/11, privacy, and the American war on terrorism

As a response to the American wars in the Middle East, including Iraq, which aimed at gaining control over natural resources of the region, as well as to the American backing of the neocolonial military policies and actions of Israel against the Arab nations, the Wahhabi Islamist group *al-Qaeda* founded in 1988 by a Saudi Arabian economist and religious scholar Osama bin Laden initiated four surprise attacks against the US in the morning of September 11, 2001.

According to the statement put forward by bin Laden, the aim of the attack was to target the American economy and force the US to withdraw its military and financial support for Israel (BBC News, 2001). In subsequent statements, bin Laden urged the American citizens to pressure the White House leaders to "cease the wars and US support to Israel, rather than succumb to what he called *the ideological terrorism* exercised by neo-conservatives" (News Wires, 2009). As for the economic and property damage, Rose et al. (2009) estimated the total economic impacts using (1) the collection of data on the relocation of firms displaced by the attack, (2) an estimation of the major source of impacts off-site, including, in particular, the ensuing decline of air travel and tourism resulting from the social amplification of the fear of terrorism and (3) an estimation based on Computable General Equilibrium (CGE) analysis reflecting the direct effects of external shocks. They found that the economic impact of the attacks was in fact lower than initially estimated and had no destabilizing effect on the national economy of the US (Rose et al., 2009, p. 23):

> Our best estimate of the economic consequences of these attacks $109 billion in losses to the U.S. GDP. This represents 1.0 percent for the 12 months following the attacks. However, there is an indication that the impacts of decreases in business travel and tourism extended well into a second year, so that this number would be lower for that extended period.
>
> We conclude that the events of 9/11 did not have a destabilizing effect on the economy of New York State or that of the U.S. as a whole.

As for the political motivations behind the attacks, the US maintained its support for Israeli expansion in the Middle East and used the attacks as a justification to launch a massive international military campaign known as the war on terror (WOT), initiated by the administration of President George W. Bush. Gouvin (2004) observed that WOT internally severely undermined the system of checks and balances in the American political system. Moreover, WOT prompted an overwrought and unproportional American

response on the international arena, motivated by what Mueller and Stewart (2012) referred to as *the terrorism delusion*. The growth of counter-terrorism industry in the US led to a project of finding a domestic terrorist adversary on one hand, and developing a system of finding pressure points and connections on the other.

In order to be able to proceed with the project, the Bush administration had to invalidate a range of protections around privacy and due process, especially the privacy of data and communication. This led to the abuse of both the American law on the side of the US government and the discretionary abuses of surveillance powers on the side of the NSA.

2.3.2 The NSA and the abuse of surveillance powers

The abuse of surveillance powers which followed the WOT and the expansion of surveillance industry in the US, was preceded by the abuse of constitutional powers of multiple institutions in the American government. James Comey, Deputy Attorney General in the years 2003 – 2005 with the Bush administration and later Director of the Federal Bureau of Investigation (FBI) recalls the legal hurdles related to the NSA domestic wiretapping. The legal opinions based on an invalid interpretation of the law in case of NSA surveillance originated in the Justice Department's Office of Legal Counsel (OLC), which Comey called "a kind of Supreme Court within the executive branch" (Comey, 2018, p. 76). According to Comey, when Jack Goldsmith, as the new head of OLC, "inherited" the legal opinions written by his predecessors following the 9/11 attacks in 2001, it became clear that the opinions were flawed to the extent of being unwarranted. Comey recalls about the lawyers who issues the opinions (Comey, 2018, p. 76-77):

> Those lawyers had attested to the lawfulness of aggressive counter-terrorism activities by the Central Intelligence Agency and the National Security Agency. The president and the intelligence community had relied on those opinions for more than two years. The opinions were dead wrong in many places, Goldsmith concluded. And the debate within the Bush administration over them was getting nasty.

In a nutshell, the classified NSA surveillance program code-named *Stellar Wind*, which the legal opinions in question concerned, was already active at the time. The Bush administration relied on the flawed opinions for over two years, which meant that, were the opinions to be subtracted, a significant part of the program would turn out to had been conducted illegally. *Stellar Wind* facilitated the NSA surveillance operations against suspected terrorists and citizens without the need for judicial warrants. The Bush

administration government became reliant on these operations in carrying out the WOT campaign, as well as for investigating domestic terrorism.

However, the NSA overstepped even the unconstitutionally extended capacity for surveillance activities. According to Comey:

> What Bush appeared not to know was that the NSA was engaging in activity that went beyond what was authorized, beyond even the legally dubious, and into what Goldsmith and Philbin concluded was clearly unlawful.

An intense conflict ensued between the representatives of the new OLC, joined by James Comey and the United States attorney general John Ashcroft, and the White House officials Alberto Gonzales and Andrew Card, who pressured the attorney general to sign papers reauthorizing the domestic surveillance program. In early January 2006, *The New York Times* revealed the incident in which Comey and other Justice Department officials refused to certify the legality of central aspects of *Stellar Wind*, although not all details were part of public discovery at the time. The revelation was part of the publisher's investigation into the then-rumored Bush administration's warrantless domestic surveillance program. In the end, the Department of Justice officially found that the domestic wiretapping under the Terrorist Surveillance Program (TSP) was unconstitutional if conducted without a court warrant. Under White House procedures, Justice Department approval was required in order for the program to be renewed, which meant that equisite changes had to be made to the program. Despite his declaration that the changes were indeed to be applied, President Bush saw to it that the warrantless wiretapping, initially authorized for a "limited period", was seen as permanent, and that processes and technologies would be made available to accommodate the shift (Landau, 2013, p. 56).

2.3.3 Edward Snowden and the 2013 act of whistleblowing

The original news of the secret NSA program to collect domestic telecommunications metadata from Verizon Business Networks Services by Greenwald (2013) appeared in *The Guardian* on June 6, 2013. On June 7, another news piece appeared, which revealed the existence of PRISM, the NSA program targeting online communication and collecting data of non-US citizens outside the US, together with the data of people in communication with them. The extent of cooperation between the NSA, the US government and the US surveillance capitalists was also revealed in the same piece, while subsequent revelations concerned the surveillance of EU leaders, among others, ahead of the 2009 G20 Summit and the US and UK mass surveillance of online communications. Similarly as is the case in China, the American surveillance industry requires

immense human, technological and financial resources, which makes necessary the hiring of large numbers of contractors and employees with extensive access to personal data. Edward Snowden, who later became known as the first mass surveillance whistleblower in history, was a contractor employed by Booz Allen Hamilton (Landau, 2013, p. 54).

Snowden was in Hong Kong when the disclosures were published and, soon afterwards, his American passport was revoked. Russia granted him a one-year asylum and later extended his stay. As of 2021, Snowden still resides in Russia and is unable to return to the US. The charges against him under the Espionage Act for intentionally revealing secret national security information allow up to 10 years of imprisonment *per document revealed*.[6]

Despite bringing strong backlash against Snowden himself, his 2013 public disclosure of *ca* 1.7 million documents of secret data from the NSA brought about the global awakening when it comes to discretionary mass surveillance and privacy protection. The American government struggled to make a decision on how to properly handle the situation with both Snowden and the NSA. Although in his speech on January 17th, 2014 President Barack Obama defended the necessity of the NSA surveillance program, changes in the American surveillance system felt imminent at the time (Verble, 2014, 14). The impact of Snowden's disclosures, especially in the USA, has been actively undermined by the government officials. This strategy is possible largely because many of the legal documents in the case and the communications within the government following the 2013 leak are still confidential. As Snowden (2019, p. 244) argues:

> Even now, years after the fact, I would not be allowed to argue that the reporting based on my disclosures had caused Congress to change certain laws regarding surveillance, or convinced the courts to strike down a certain mass surveillance program as illegal, or influenced the attorney general and the president of the United States to admit that the debate over mass surveillance was a crucial one for the public to have, one that would ultimately strengthen the country. All these claims

[6]Just to put this possibility in perspective, were Snowden to receive maximum penalty for the crime under the Espionage Act, he would need to spend 17 million years in prison. Considering that the *homo sapiens* only emerged around 300 thousand years ago, this sentence would be over 56.5 times longer than the time of existence of our species. Assuming that Snowden would live to see the end of his sentence, he will have witnessed the reversal of Earth's axial tilt causing summer and winter to occur on opposite sides of Earth's orbit. He would also see Sahara turn back into having a tropical climate. Later still, the proper motion of stars across the celestial sphere will have rendered the observable constellations unrecognizable by today's configuration. After 10 million years, sometime beyond his mid-sentence milestone, Snowden will have borne witness to the full recovery of biodiversity after the ongoing Holocene extinction. Finally, by the time he is released, two moons of Uranus, called Cupid and Belinda, may have already collided. That is a long time to spend in prison for releasing documents to the press.

> would be deemed not just irrelevant but inadmissible in the kind of proceedings that I would face were I to head home. The only thing my government would have to prove in court is that I disclosed classified information to journalists, a fact that is not in dispute.

The positive impact of the 2013 events is presently not a subject controversy, at least not in the EU. Multiple non-governmental organizations (NGOs) and human rights and privacy advocates, including Amnesty International, called for a full pardon for Snowden, as well as an actionable protection policy for whistleblowers worldwide (Amnesty International, 2021).

2.3.4 Apple and Google push for full encryption

Meanwhile, Snowden's act of whistleblowing "dealt a devastating blow to [the USA's] ability to collect intelligence" (Comey, 2018, p. 137-138) and prompted a massive migration towards fully encrypted communications. In 2014, Apple and Google declared a shift in the mobile devices to default encryption. Hence, the line of friction in the conflict about privacy was crystallized.

The Obama administration officials, including the FBI Director James Comey, were unable to strike a balance between security and the rule of law, while the US surveillance capitalists forced their hand by making available the encryption technologies, which made possible communication without content oversight. Comey (2018, p. 138) argues that the decision about the availability of encryption technologies must be made democratically:

> The divide between the FBI and companies like Apple can be explained, in large measure, by how each sees the world, and the limitations of each of those perspectives. (...) We [the FBI] see humankind at its most depraved, day in and day out. Horrific, unthinkable acts are what the men and women of the FBI live, breathe, and try to stop. (...) I thought the tech community did not fully appreciate the costs when good people from law enforcement were unable to use judicial orders to get evidence. I also think it would be fair criticism to say we focused too much on those costs, given the darkness outside our windows all day long.
>
> Because both sides are biased by our places in the world, I thought it critical that the resolution shouldn't be dictated by either Apple or the FBI; the American people should decide how they want to live and govern themselves. But what exactly that means as a practical matter is an incredibly hard question to answer.

The reason behind including here this extensive quotation is that the conclusion by the FBI Director Comey aligns with the main conclusion of the research presented in this dissertation. Namely, since privacy in modern times in largely a political matter, and since the availability of encryption is one of main *focii* of political privacy, the decisions concerning encryption must be made democratically, with full legitimization of the people. In particular, in a democratic state, these decisions are not up to the surveillance capitalists and not up to the surveillance authorities or government administrations which support them.

2.3.5 European awakening

In Europe, Snowden's whistleblowing helped save the GDPR and completely change the direction of privacy and surveillance policies. Rossi (2018, p 95) indicated that between January 2012 and the summer of 2013, the overall approach of the European Parliament to privacy changed rapidly. This resulted in passing the GDPR, but more importantly, invalidated the default authorization for the Silicon Valley lobbyists to influence the EU privacy policies at a massive scale. In the time "after Snowden", the surveillance capitalist corporations were politically defeated, their organized corporate power giving way to the primacy of privacy at the EU policy level.

Wahl-Jorgensen et al. (2017, pp. 16-17) investigated the European responses to the 2013 event in the press and non-traditional media. Content analysis of 249 blogs and 538 newspaper stories examined a range of variables relevant to the reception of the surveillance revelations. Among the coded types of variables, were those categorized as opinions on surveillance, targets (coded as, *e.g.*, elites, members of the public, journalists, *etc.*), and the perceptions concerning Snowden himself (hero, traitor, whistleblower, *etc.*). The analysis revealed disparities between debates across platforms, especially for traditional and non-traditional media. Wahl-Jorgensen et al. (2017) established that, although the traditional news outlets tended to position foreign politicians, world leaders, and terrorists as targets, the bloggers and citizens predominantly identified members of the public as the targets of surveillance, in line with Snowden's concerns. Consequently, the revelations served to completely reshape the European public discourse on the nature of digital citizenship, as well as the role of privacy and surveillance techniques in protecting modern democracies. Extensive account of judicial, societal, economic and institutional responses can be found in (Wright and Kreissl, 2013).

2.4 The right to privacy and privacy laws in China

Among the main models of data protection, Pernot-Leplay (2020) referred to the Chinese data protection system as "the third way", suggesting that data protection in China in not as strict as in the EU, but also not as neglected as it is in the USA. Currently, China is undergoing development of its data processing and transfer frameworks, with the EU and the US serving as two reference points, both based on different background assumptions. While the EU data protection model is globally perceived as favoring strong protection, the US model could be called minimalist. However, although China may choose to adopt solutions from the two antagonistic models, it does not mean that it can place itself in the middle of the data and privacy protection spectrum. This is because, although the Chinese government is searching for a proper data protection system, it does not bind data protection with any guarantee of privacy, either within or outside the context of data.

While in the EU privacy is considered a priority and surveillance and business capabilities are, at least in principle, accepted only insofar they do not threaten the core of privacy protection objectives, the US government prioritizes state surveillance and unrestricted data processing, hoping to nurture economic growth and develop further its intelligence capabilities. In both cases, privacy takes center stage in governmental considerations of privacy and security policy, which subsequently informs data protection policy. In this sense, one could day that in the US and the EU data protection policies *follow* privacy protection strategies. In China, this is not the case. Data protection is seen as politically and legally independent from privacy considerations, and the data protection framework, which is under development currently, will in no way restrict, influence or invalidate the large-scale state surveillance, as well as the no-privacy conditioning which the the Communist Party of China (CCP) inflicts upon the Mainland residents, as well as the citizens of semi-autonomous territories, such as Hong Kong, Macau.[7] Pernot-Leplay (2020, p. 54) suggested that the data protection strategy for China is likely to take shape of "data privacy with Chinese characteristics", echoing Deng Xiaoping's notion of "socialism with Chinese characteristics" presented in his opening speech at the 12th National Congress of the Communist Party of China on September 1, 1982.

The project of "data privacy with Chinese characteristics" originates from two assumptions. First, the principle of cyber-sovereignty (cyberspace sovereignty), which

[7]Hong Kong and Macau are two special administrative regions (SAR) of China, which means that, at least officially, under the "one country, two systems" principle, they have their own governments, multiparty legislatures, legal systems, police forces, monetary systems, separate customs territory, immigration policies, academic and educational systems, and substantial own competence in external relations.

subordinates the cyberspace to the interests and values of China, as if extending state sovereignty to digital space. The principle was established in Article 1 of Chinese Cyber Security Law, here quoted in English translation after (Pernot-Leplay, 2020, p. 104):

> Article 1.
> This law is formulated in order to ensure cybersecurity; safeguard cyberspace sovereignty and national security, and social and public interests; protect the lawful rights and interests of citizens, legal persons and other organizations; and promote the healthy development of the informatization of the economy and society.

According to Baezner and Robin (2018, pp. 32-33), this geopolitical interpretation of cyberspace was born from the 2013 Snowden revelations, especially concerning foreign access to data on population communications and the Chinese nationals security. In addition, the Chinese strategy is directly opposed to what is called a multi-stakeholder governance model, which supports (at least to some extent) a free and open Internet. In a Chinese unique-stakeholder data management model, the interests of businesses and users like come second to the unrestricted competence of the CCP and their intelligence service.

The second fundamental principle of "data privacy with Chinese characteristics" is the separation between *privacy from surveillance by citizens and businesses* and *privacy from state surveillance*. This division in itself has also been adopted in this dissertation and, in my opinion, is based on a valid assumption that the relationship between an individual and society is different in nature from the relationship between an individual, a group or a community and the state. However, the application of the division in case of the CPP is not at all benevolent. In the Chinese variant of the privacy bifurcation theory, an individual may be allowed certain degree of privacy against other individuals or businesses which are not authorized by the state to exercise their power of surveillance. An individual is not entitled to privacy from state surveillance, regardless of the level of discretionary action. I will come back to this problem later on in section 2.5. However, as far as data protection is concerned, the principles of cyberspace sovereignty and unrestricted state surveillance, which from now on I will refer to as *the Big Brother principle*, are by now considered a given in the ongoing domestic political debate on data protection in China.

Historical records validate this trend of development of the data protection framework in China. Back in 2005, a draft privacy regulation, mainly related to processing of data of non-Chinese users outside China and somewhat inspired by EU regulations, has been put forward as "expert's suggestion" to the Chinese Informatisation Office of

the State Council, but even then legal analysis did not expect that the law would be passed in China (Treacy and Abrams, 2008). Yang (2008, p. 60) observed that even before the data protection reform, the right to privacy of correspondence was included in the 1982 Constitution of China (*Xian Fa*) and acknowledged in legal discourse, but it's interpretation was limited to protection against fellow citizens and the media (or other semi-private enterprises), and did not allow protection from state surveillance. Similarly, *the right to dignity* and *the right to protect one's reputation* is assumed to be effective against civilian violations, but not state initiatives. The bases of the right to privacy laid out in Articles 38–40 of the *Xian Fa*[8]

> Article 38 (Human dignity. Right to protect one's reputation)
> The personal dignity of citizens of the People's Republic of China is inviolable. Insult,libel, false charge or frame-up directed against citizens by any means is prohibited.

> Article 39 (Regulation of evidence collection. Right to privacy)
> The home of citizens of the People's Republic of China is inviolable. Unlawful search of, or intrusion into, a citizen's home is prohibited.

> Article 40 (Right to privacy)
> The freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law. No organization or individual may, on any ground, infringe upon the freedom and privacy of citizens' correspondence except in cases where, to meet the needs of state security or of investigation into criminal offenses, public security or procuratorial organs are permitted to censor correspondence in accordance with procedures prescribed by law.

According to Yang (2008, p. 61-62), despite the lack of implementation of constitutional guarantees of privacy, the Supreme People's Court supported the direct interpretation of the *Xian Fa* in order to grant compensation to individuals whose *individual* right to privacy was infringed upon by the press (*cf.* Shi Zhaohui *v.* The People's Daily, 1995; Xiaoli (Alias) *v.* The China Times, 2005; Fu Qiang *v.* Union Press, 2000; Wu Jing (Ms. Liu) *v.* Guangdong Newspaper, 2003). Moreover, the General Principles of Civil Law of China (GPCL) of 1986 gives recognition to the right to reputation, albeit

[8]The Constitution of the People's Republic of China of 1982 with Amendments through 2018, including *Xian Fa Xiuzhengan* of 1988, 1993, 1999, and 2004. Analogous regulations became a part of 2020 Chinese Civil Code.

without referring to privacy (Ong, 2012, p. 172), which further disconnects *individual privacy* from political privacy and surveillance:

> Article 101.
> Citizens and legal persons shall enjoy the right to reputation. The personality of citizens shall be protected by law, and the use of slander, libel or other means to damage the reputation of the citizens or legal persons shall be prohibited.

Due to the fact that privacy is understood so strictly in the Chinese legal interpretations, the judicial decisions in privacy-related cases make up for a "vague and inconsistent" individual privacy protection scheme (Ong, 2012, p. 178). This reaffirms a claim by Zhu (1997, p. 214) that an independent right to privacy in China's legal system has yet to emerge. Part of the difficulty stems from the linguistic obstacles, which disable linking the notion of privacy with political competence. Zhu (1997, p. 208-209) explains the semantic aspects of the concept of privacy in everyday Mandarin, which carry onto the legal language (Jingchun, 2005, p. 646). In particular, the difference between the word *yinsi*, which stands for a shameful secret, and a similarly transcribed word *yinsi*, but one meaning privacy, is not widely known among the ordinary Mandarin speakers:

> These two words were very often used alternately for their pronunciation is almost the same except for a slight difference of the tones. Even in a widely used Chinese dictionary, *shameful secret* is defined as a hidden bad thing, usually in connection with sexual affairs; while *privacy* is defined as a personal thing people do not wish to tell others or to disclose in public.

Similarly as was the case with other words of strategic political importance, their meaning and use are carefully crafted in the mainstream Chinese news outlets, while their "alternative", more permissive or rights-oriented meanings are systematically censored throughout social and non-traditional media, even when citizens actively lobby for the specific use of the terms. A good example of such systematic censorship and citizen's organized counter-action is to be found with the word *feminism* (Fincher, 2020), which I will discuss again in section 2.5. Due to this formative power of government policy on the use of common words, *privacy* remains to be defined as meaning *personal privacy*, as opposed to *political privacy* by the standards laid out in section 1.4. This effect decreases the rate of public engagement in the privacy debate by raising the literacy requirement threshold to a level comparable to that of an academic debate.

Yet another critically important feature of the domestic privacy debate in China is that the theories of privacy put forward in the literature are, at least in general, not

aimed at *informing* policies, but rather at *explaining* them in a way which makes the reception of the privacy and surveillance laws more effective. For instance, Yao-Huai (2005) proposed an analysis of the Chinese approach to privacy based on the historical development of social respect for personal matters. In his analysis, Yao-Huai (2005) argues that privacy is to be seen as an instrumental good, of little intrinsic value, and argues that the social changes which brought about an expectation of privacy (in the sense of *personal* privacy, meaning an expectation against other individuals) have largely been destructive to traditional Chinese values. Following Liu and Wei (2004), Yao-Huai (2005, p. 11) lays out four principles, which are assumed to be descriptive of the Chinese approach to personal privacy:

(1.) the principle of respect (roughly reiterating Article 38 of the *Xian Fa* and tapping into the ideals of a doctrine referred to as *socialist humanitarianism*),

(2.) the principle of informed consent (regulating the relationship between social media and other data collectors and the users, but excluding the state-mandated data collection),

(3.) the principle of equilibrium, and

(4.) the principle of social rectification.

The latter two principles will be of special importance to the considerations of surveillance society in China in section 2.5. This is because the principle of equilibrium, although it recognizes the need to seek balance between ("the safety of") personal privacy and "safety of society" (especially state security), gives full validation to total and unrestricted surveillance of private communications. According to Yao-Huai (2005, p. 11), the principle of equilibrium "emphasizes that personal communications on networks should be recorded, so that the relevant organization can check them in order to guarantee social safety".

In a comparative study between China's and the USA's privacy protection frameworks Wu et al. (2011, p. 614) indicated that China should make effort to strike a more genuine balance between personal privacy and state security, suggesting that the principle of the equilibrium, as proposed by Yao-Huai (2005), is insufficient to develop or sustain a healthy social environment. Moreover, they proposed that *the principle of technological neutrality* be adopted instead.

The last principle on the list, the principle of social rectification, means that the society (or the state which represents society) is authorized to rectify a violation of personal privacy "so as to guarantee the stability of the social order" (*ibidem*). In light

of this principle, group activities such as *the human flesh search* (Han, 2018) are given a legal-theoretical and socio-political justification.

2.5 China as a surveillance state

All computers sold or manufactured in China after July 1, 2009, are required to include the so called *Green Dam filter*, a software "back door" to the records of all user activity, including communications. Initially, the public outcry against the Green Dam delayed its implementation, but eventually the solution was implemented (Watts and Branigan, 2009). Together with what is known as *the Great Firewall of China* (*Fánghuǒ Chángchéng*), they allow for near total control and manipulation of digital communications. The Great Firewall is a system of legal and technological tools, which focus on active filtering, active probing and blocking designated information sources and communications. Since its implementation, it has led to limiting access to foreign information sources and search tools, such as Google, Facebook, Twitter, Wikipedia, *etc.*, as well as a number of mobile apps which did not comply with Chinese domestic standards, especially those which did not include the Green Dam filter.

In her seminal work on China's system of online control and censorship, MacKinnon (2011) called it *networked authoritarianism*. This policy enforces a hierarchy of stakeholders, where surveillance capitalists must satisfy the criteria laid out by the state surveillance authority and the CCP (Communist Party of China) in order to share in China's massive online market. In turn, the users must accept their position as a resource to data-collection businesses, as well as the extensive state moderation and surveillance of all online communication. Adopting these legal-technical solutions, which overpower any civic engagement and free speech online, together with the widespread CCTV and physical surveillance, I proposed to call *the Big Brother principle*.

Historically, the emergence of domestic surveillance capitalist market is closely linked to political repression of politically disadvantaged groups. For instance, the initial blockages of foreign social media resulted from the need to block the flow of information about the violent political protests in Xinjiang province in July 6, 2009, where the Han Chinese residents clashed with the native Uighur residents, resulting in 156 deaths and over 1000 wounded. The blockage on internet access in Urumqi and certain other regions of Xinjiang was then effected for the first time, as a means of informational damage control, as well as a tool of slowing down the spread of the protests (Fincher, 2020). Soon afterwards, in July 2009, the blockage was extended onto most foreign information services, including Twitter, Facebook and others. The very next month, *Sina Weibo*

launched, as a replacement of all the blocked foreign platforms. Weibo was the brainchild of Charles Chao and came with censorship and surveillance included (Zhang and Negro, 2013), introduced simply as *built-in functionalities* in compliance with the Green Dam filtering condition. The perception of Uighurs as a designated domestic terrorist adversary is therefore intertwined with the inevitable growth of the Chinese domestic surveillance capitalist market.

As of 2021, the policing system implementing the Big Brother principle is used as a standard tool for near total elimination of political dissidence, ranging from the Uighur cultural and religious independence and Hong Kong's demand for respecting the "one country, two systems" organizing principle, to issues such as women's rights movements in Chinese society, which met with violent repression, including extra-judicial imprisonment and torture of activists associated with *the Feminist Five*: Wei Tingting, Li Maizi (Tingting), Wu Rongrong, Wang Man, and Zheng Churan, also known as *Da Tu*, or "the Big Rabbit" (Fincher, 2016). On March 6, 2015, just before the International Women's Day, the Chinese police in Beijing arrested the Five for preparing to engage in activism protesting sexual harassment in public transportation. The Five, together with other activists, were preparing to hand out informational leaflets about the rate of harassment in city trains, which was identified as a national security threat (Zheng, 2015, p. 476).

Later in section 5.2.3, I will analyze Chinese surveillance methods and their use as aid in genocide of the Uighurs of Xinjiang. In section 3.2.1, while showing how political privacy helps protect democratically valuable social agendas, I will also discuss the case of the Weiquan movement in China, a grassroot legal aid and education movement which had been near eradicated using surveillance.

2.6 Summary

In this chapter, I analyzed the fundamental elements of the contemporary legal frameworks which enable the three dominant privacy protection models: that of the EU (with special attention to the EU's driving forces, France and Germany), that of the US (called a minimalist model, reflecting the trend in data protection), and the Chinese model, which divorces personal privacy from political privacy, only to implement what I referred to as the Big Brother principle.

Comparative analysis brought to light stark differences between the models, ranging from the goals and strategic bases for implementing privacy solutions, to the role which theories of privacy play in the domestic and foreign policies of the analyzed countries. I found that the theories of privacy developed in the EU and the US predominantly

aim at informing the policy and statutory law, while the theories of privacy in Chinese scholarship mostly focus on explaining the already implemented policies and legitimize them in light of the designated desirable socio-political values.

However, there seems to be more convergence on the methods and the practice of surveillance between the US and China, than there is between the US or China and the EU. Since 2013, the EU implements a strong protection model, which is the most promising from among the three dominant models, in the sense that it is currently closest to allowing for full political privacy and encouraging the member states to comply with respecting its necessary supporting solutions.

Chapter 3

Political privacy, individual and collective rights

In this chapter, I present the right to privacy in selected liberal approaches, together with their criticism. I also discuss, in section 3.1.2, some of the non-liberal approaches to privacy, with special attention to arguments, which reject the right to privacy (either in whole or in part) because of the skepticism towards universal human rights. This brief philosophical overview is not meant to be exhaustive of the topic of privacy in either of these orientations in political philosophy. Rather, it aims at lying the groundwork for a presentation of cases in section 3.2, in which the right to privacy emerged as a *collective* human right, in parallel to being the right of an individual.

In section 3.2.1, I give examples of collective social and political agendas, which are valid from the perspective of liberal philosophy, as well as from the perspective of many of its critics, as long as they don't reject the idea of human rights and the rule of law altogether. Through these examples I want to show that privacy, as it functions in the contemporary world, is not an inherently liberal concept. I argue that the right to privacy be expanded to include the collective aspects of citizens' initiatives, many of which (though requiring individual rights and freedoms as a guarantee of the ability to take action) are not reducible to individual rights, agendas, or personal well-being.

3.1 Privacy as an individual right

3.1.1 Privacy in liberal political philosophy

Historically, the right to privacy occupied a problematic position in liberal political philosophy. On the one hand, Posner (1977, p. 233) saw privacy as a hindrance on the

exchange of information in a free society (Sandel, 1998). On the other, privacy has been accepted as one of the facilitating conditions for informed choice at least since the 1980s, even by legal and political scholar critical of unlimited privacy protection, such as Allen (1987), Seidman (1986), and Etzioni (1999).

Introna (1997, p. 261) noted that many of the historically relevant liberal philosophers – among them John Locke, Jean Jacques Rousseau, Wilhelm van Humboldt, John Stuart Mill – did not pay explicit attention to the role of privacy in maintaining social order and ensuring a baseline quality of life for individuals and groups, and had not formulated a clear definition of the right to privacy. This is despite the fact that the problem of protecting the rights of an individual *versus* the society was often a major theme in their work. An interesting question in this context is the following: why did the systematic consideration of privacy and the right to privacy appear so late in the legal, political and philosophical literature?[1]

As indicated in chapter 1, the modern legal understanding of privacy dates back only to the 1890s and the works of Warren and Brandeis (1890) on *the right to be let alone*. Some traces of the right to privacy may also be found in, relatively contemporary to Warren and Brandeis, work by Von Gierke (1895, p. 702), who proposed a so called *general right of personality*. Considering that the right to ownership of property was present in philosophy and politics since the ancient times, what made privacy so irrelevant for so long? Introna (1997) went so far as to ask: is the right to privacy *an invention* made by Warren and Brandeis in response to an intense personal situation?

I argue that the answer to this question is to the negative. And, in this case, comparing privacy to property may actually well inform the solution to the origin problem. Observe that the debates concerning property, together with a need for producing theological, political and scientific justifications of the right to property, revolve around the need to prevent violations of the projected right. Aristotle argued for the need for private property in *Politics*, saying that shared property naturally falls into neglect. Thomas Hobbes and John Locke marked the shift from theological to contractual projected origin of property. Locke (2015, IX, §§ 123–124) argued that people put themselves under government in order to secure their property, because property protection makes for safe and secure enjoyment of the natural need of ownership.

Note, however, that in the absence of high tech surveillance tools, governments

[1]This is not to say that there had been no historical attempts to characterize privacy or the right to privacy. In many historical philosophical and political works, certain theoretical elements or observations may be linked with what nowadays is interpreted as privacy. Introna's claim is merely that a full-fledged theory focused on (the right to) privacy as we know it was not proposed until relatively recently. For a comprehensive review of historical attempts at discussing privacy, see Binicewicz (2021, pp. 97-131).

played little to no role in preventing, *e.g.*, privacy violations. No government can stop people from spying on each other, if such is their inclination or culture. At the same time, up until the digital age, the state needed to rely heavily on human intelligence (HUMINT), and only gradually developed technical (including medical) intelligence (TECHINT, MEDINT), and financial intelligence (FININT). Other forms of state and organized intelligence only became possible as technologies needed to implement them emerged and expanded. These relatively new types of intelligence include (i.) cyber or digital network intelligence (CYBINT or DNINT) gathered from digital spaces, (ii.) signals intelligence (SIGINT) gathered from interception of signals, including communications (COMINT), and (iii.) all forms of electronic intelligence (ELINT), including foreign instrumentation signals intelligence (FISINT). Before the advent of electronic communications, COMINT required targeted physical interception and processing, such as, for instance, opening physical mail and having a human employee read its contents. Hence, it is not as surprising as Introna (1997) suggested that privacy received little attention in the pre-modern political and philosophical literature.

Moreover, privacy violations and infringements which were feasible in the pre-digital era called for relatively little in terms of effective means of privacy protection. After all, a home which one owned to a large extent guaranteed privacy. The control of correspondence also allowed one to draw analogies from property protection measures: violating the private exchange of letters resembled violating the trade of currency or any other physical object. Nowadays, the ownership of electronic devices, or even home and other physical spaces, no longer naturally guarantees privacy. Hence, technologies, especially digital intelligence technologies, allow for new methods of privacy violations, in the same way as they enable new methods of property theft. Importantly enough, the emergence of new methods to commit violations does not modify the nature of the need for privacy or ownership, nor the nature of the associated rights. Thus, similarly to property, privacy is inherently pre-technological. The right to privacy is not invalidated by invention of new ways to violate it – contrary to the rhetorical claims made by, among others, the CEO of Sun Microsystems Scott McNealy, who famously said: "You have zero privacy anyway. Get over it" (Sprenger, 1999).

Another reason why the problem of privacy emerged only after the camera technology came about is that this new type of violation – infringement through taking photographs – felt, quite veridically, perfectly preventable. The notion of descriptive and normative privacy proposed by Moor (1991) echoes this exact problem: not all privacy (or property) violations are preventable, even by the violator himself. Hence, a person may have an expectation of privacy, for example, while in one's home, but being un-

able to entertain descriptive, *actual* privacy when the walls are thin or when sharing the living quarters with other people. In many of such situations, violations are not reasonably preventable, because the economic and living conditions of the society do not permit it (Mizutani et al., 2004, p. 123). However, Warren and Brandeis (1890), just as many scholars after them, viewed benefits of surveillance technologies (including press photography) as optional, or at least inferior to the need of protecting the most basic, familial zones of activity, including the enactment of relationships among family and friends during a closed event. And, similarly to the violations of property, the more preventable the violation feels, the firmer the proposed measures. Consider the RFID-blocking (radio-frequency identification) wallets, which are meant to prevent a type of theft called RFID skimming, which gained popularity despite the fact that the rate of RFID theft is negligible and the process itself, highly risky for the thief. The ease of preventing skimming still convinces many people to buy a protective wallet, despite the risk of theft being extremely small. All in all, it is only natural that privacy remained unnoticed in early liberal (and non-liberal) philosophy. Likewise, only the emergence of mass surveillance technology could spur considerations concerning political privacy and give it due relevance.

Since the 1970s, Wasserstrom, Posner, and others advocated against privacy in general, arguably because they only considered privacy in the sense of personal privacy and not political privacy, and thus defined privacy seemed like a minor goal compared to their long-term projects of encouraging transparency in the society and gradual reduction of uncertainty. Wasserstrom (1984, p. 328) observed that a society with a permanent record would automatically facilitate a life which is "less spontaneous and more measured" for individuals, which ultimately will benefit the society as a whole, though perhaps only in the economic sense (assuming that preventing, mitigating or ignoring crime *etc.*, all come with associated economic costs).

Allen (1998) attempted to develop *the liberal conception of privacy* along *the liberal theory of private choice*. In this way, Allen planned to bind privacy protection with one of the fundamental concepts of liberal philosophy at the time. In Allen's case, the essence of the liberal conception of privacy is the claim that the government is obliged to respect and protects interests in physical, informational and proprietary privacy, understood as, respectively, physical seclusion and solitude, data protection and control over personal information, and "control over names, likenesses, and repositories of personal identity" (Allen, 1998, pp. 723-724). Allen then argues that there exists an overlap between thus defined liberal conception of privacy and the liberal conception of private property. There are two major differences between this liberal take on privacy

and property and the way of embedding privacy into a general framework of political philosophies, which I presented in section 1.4. First, Allen's argument about the overlap between the two concepts relies primarily on psychology (*ibid.*):

> We associate privacy with certain places and things we believe we own, such as our homes, diaries, letters, names, reputations, and body parts. At the core of the liberal conception of privacy is the notion of inaccessibility. Privacy obtains where persons and personal information are, to a degree, inaccessible to others.

Second, the liberal philosophy of privacy and property presented by Allen, runs the risk of *conflating the society with the state* in the political dimension. This is due to the fact that, on the one hand, liberal philosophy, by putting an individual in the center of all considerations, tends to classify both society and the state as two forces which threaten the fundamental freedoms of an individual. On the other hand, because in liberal philosophy, as a general rule, the individualist approach to social-political systems is preferable to, *e.g.*, collectivism, the consideration of the role of privacy (especially political privacy) to social development and political stability is grossly neglected. By this token both the government and the society ought to abide by the same standards towards the individual, reincarnating the ancient division between the private *oikos* (Greek for *household*, later developed into the Roman *res privatae*) and the public sphere of the *polis* (*res publicae*).

For Allen, both privacy and private choice are meant to restrain the government in its own violations against privacy, as well as ensure privacy protection in relation between the individual and the society. Social conventions, political culture and communal standards concerning privacy and discovery of familial, group and personal zones of activity play no role in shaping privacy protections and surveillance policies. This outcome makes the liberal conception of privacy rather suspicious. After all, a theory of privacy which leaves outside its scope of interest the cultural and societal contributions is bound to be inadequate and applicable only within a very specific, limited legal-political context.

The concept of private choice plays into the primacy of economic characterizations of social policies. In the context of private choice, privacy is a social good, which can be overdispensed or misdistributed, but it also plays an instrumental role in protecting *private choice*. The principle of private choice states that: "[the] government ought to promote interests in decisional privacy, chiefly by allowing individuals, families, and other nongovernmental entities to make many, though not all, of the most important decisions concerning friendship, sex, marriage, reproduction, religion, and political as-

sociation" (Allen, 1998, pp. 724). A driving motivation behind these protections is a strive for efficiency in social and political organization, typical of the liberal political philosophy. Note that, although privacy is accepted by Allen and others as a fundamental freedom with inherent value, when considering the limitations or privacy and private choice, it is the instrumental, economic value of the freedoms that comes to the fore.

Yet another problematic element in liberal considerations of privacy is the allegation of a so called "conservative tilt" of privacy protection, particularly in its relation to women's rights. Although the right to privacy played a central role in enabling American women to exercise their right to self-determination, including motherhood and abortion (McClain, 1992, p. 173), arguments about the negative impact of privacy protections on women's and minorities' rights were developed, including (Allen, 1998, p. 747):

1. privacy being an obstacle to *beneficial public interventions*, which help instate new norms of behavior and eliminate (or at least decrease) underparticipation of women in social and political life, as well as male aggression and harassment (including domestic violence);

2. privacy slowing down the execution of egalitarian laws by closing women inside the sphere of the *oikos* in the name of protecting their right for solitude and seclusion, and the sanctity of their familial life;

3. privacy may be used against sexual minorities as a method of silencing and repression, based on the fact that public displays of sexuality may be said to belong to the *oikos*.

This last argument Allen calls *the conservative ideology of privacy*, though it is based on the same ancient private *v.* public division which the liberal approaches use. Moreover, none of the three arguments undermines privacy as such, which Allen admits as well. The argument from public interventions is one of the most general ones and could be posed in relation to virtually any other norm of behavior, positive or negative. As such, it is not so much an argument against privacy, but rather an observation concerning how privacy acts in counterbalance to social or governmental control enacted through interventions, both beneficial and detrimental. The second argument is also not one against privacy, but rather against using privacy principles as elements of justifications to unfair social solutions, such as forcing women into domestic work and underparticipation. A similar rhetorical structure may be produced using, *e.g.*, the notion of woman's well being in place of privacy, to claim that participation in politics

is generally stressful and may pose a threat to a pregnancy. None of the structures undermines the need for privacy or health protection. Finally, the last argument, though dubbed "conservative" by Allen, mimics the division into the public and the private, which underlies the principle of private choice. In this sense, the argument is invalidated as soon as one includes social and cultural context into the considerations of privacy, and places privacy into a more sophisticated, non-dualist framework of politics.

A liberal defense of the value of privacy was also taken up by De Bruin (2010), who presented a case for privacy based on a purely negative concept of liberty, understood only as freedom from interference. De Bruin argues, against Posner, that the expectation or pursuit of privacy is not a self-interested economic behavior and that it does not automatically threaten freedom of speech, or the security and freedom of market transactions. He considers four arguments for privacy protection, which all assume that the chief dimensions of privacy as psychological and, as the behavioral approach to economics underlies the debate here, economic. Moreover, according to de Bruin, all four arguments fail to convince *the liberal skeptic*, a person who fully supports the liberal agenda, but is not convinced that the protection of privacy is necessary or even useful if one were to pursue this agenda.

The first argument is an argument from perspective change, which states that once an individual is discovered by another during a given activity, the individual is no longer a genuine participant of the activity, but rather becomes an observer of it, due to the psychological effects of being conscious of surveillance, oversight and evaluation by another. According to de Bruin, the liberal skeptic would claim that the argument is not valid, because the activity can still be carried out, albeit with a certain amount of psychological discomfort or even suffering. Similarly as will be case with subsequent arguments, the liberal skeptic only accepts economically relevant arguments and refuses to bother with psychology or the problem of quality of human life insofar as they influence the macroeconomic portfolio of the society (De Bruin, 2010, p. 507). The skeptic, as presented by de Bruin, refuses psychology and other motivators of individual behavior as subjective, while viewing economy and social order as objective ground for sound arguments on privacy, as well as all other social-political matters.

The argument from relationship states that privacy is a necessary condition for many human relationships, including essential relationships such as family, marriage or partnership, or the child-parent relationship. If violated, the privacy of these zones of activity decreases, which leads to inhibitions in developing the relationship and lowering the quality of live for the parties involved. The skeptic, as sketched by de Bruin, would reply here that the people could in principle learn to not be inhibited by oversight, espe-

cially when surveillance is not followed by public discovery of the private information or activities within the protected zone of activity. Clearly, both components of the skeptic's argument are deeply flawed. First, the fact that humans could in principle change their behavior does not mean that the change is possible within a single generation or that it can be implemented on a scale large enough to claim that the society now accepts oversight which previously has inflicted psychological and emotional distress on them. Humans could in principle learn to accept or reject many things, but political arguments based on this premiss are not practical, because humans cannot be expected to change their psychological makeup simply in order to better fit the capitalist economy.

The third argument and its skeptical critique follow a similar line of reasoning as the argument from relationships. The argument from human dignity says that the violation of privacy goes against the dignity of the individual being observed. Here, the skeptic may try to alleviate the affront to dignity by introducing consent as the invalidator of privacy. Namely, assume that consent is the ultimate indication of what the individual considers against their dignity. Hence, disrespecting consent constitutes the utmost violation of dignity. What happens when an individual consents to the violation of their privacy? Is there a way to *not* act in violation of their dignity, either by infringing on their privacy or the respectability of their consent? This "skeptical" argument does not concern the value of privacy as such, but rather the place of privacy in the order of social-political values. In all theories of privacy reviewed and presented in this dissertation, individuals may yield a zone of activity to another, include them in what was previously controlled or owned only by themselves, based on choice, need, or fancy.

The last argument is that from autonomy and states that it is in the interest of an individual to control and customize their own public or social outlook. What other members of the community know about the individual influences their interactions, transactions and the success of the individual in the society generally. Here again, the skeptic would presumably say that as long as the individual may still physically engage in the same activities as they would without oversight, their freedom is not violated. De Bruin deals with this overly simple argument by observing that certain activities are qualitatively different when performed under surveillance, thus, an original activity *per se* becomes impossible in the presence of an unauthorized observer. For instance, sexual intercourse, giving birth or even friendly feedback are ruined by the humiliation which arises in the presence of a third party (De Bruin, 2010, p. 509). On this basis, de Bruin argues that *disclosures of private information* lead to changes in negative freedom and in the knowledge an individual has concerning the extent of their negative freedom, strongly influencing their disposition to exercise actions in an unrestricted way. Here, de Bruin's

concept of privacy is limited to information, but his arguments are easily extendable onto more modern theories of privacy, such as the situational accounts or the gateway theory, which I have presented in sections 1.2.5 and 1.3.

Note that all four arguments assume that privacy is instrumental and that the only values at stake are those relating to the individual. Therefore, liberal critique and defense of the right to privacy presented by de Bruin only concerns personal privacy and not political privacy. Moreover, only arguments from behavioral psychology *v.* arguments from economy are confronted. Fuchs (2011, p. 140) noted that liberal approaches to privacy "ignore the political economy of privacy in capitalism that can mask socio-economic inequality and protect capital and the rich from public accountability".

This observation aligns with the conclusions of the analysis put forward by de Bruin and echoes what Allen called the feminist critique of privacy from the 1990s and the 1980s, except that in Fuchs' exposition, patriarchy is substituted by capitalism (exemplified by the predatory business model of Facebook and other surveillance capitalists, see section 4.1) as the force which potentially threatens the oppressed *via* targeted instrumental use of privacy protections. Hence, it seems that the liberal debates on privacy of the 1980s resembles those of the 2010s.

Etzioni (1999) presented what he called *a communitarian perspective* on privacy, which kept alive the idea that liberal political philosophy unequivocally supports privacy – an idea which in light of the aforementioned considerations by Allen, de Bruin, and others is not justified. This, in turn, fed into the idea that liberal political philosophy, associated by Etzioni with American politics in the late 1990s, facilitates a belief that "strengthening privacy can cause no harm" (Etzioni, 1999, p. 13). Due to this conflation of liberal philosophy and an unequivocal pro-privacy stance, especially outside liberal philosophy itself, the critique of unlimited privacy protection came to be affiliated, at least in the public reception, with non-liberal approaches to privacy. In the following section, I will examine some of these approaches, focusing on the insight they offer with respect to the notions of personal and political privacy, and their limitations.

3.1.2 Non-liberal approaches to personal and political privacy

Approaches to the right to privacy in non-liberal political philosophy constitute a rich enough topic to make for a full-length dissertation on its own. Thus, the short summary which I present here is not meant as their exhaustive presentation. Rather, I aim to give an overview of the relationship between privacy and other human rights in various non-liberal philosophical proposals and national policies. In particular, I argue that

the approach to political privacy in case of a particular state is often determined by its approach to human rights in general. On this axis, I distinguish three types of situations:

(1.) where the state accepts formally and materially the basic rights and freedoms, such as those listed in the Universal Declaration of Human Rights (UDHR);
(2.) where the state formally accepts the UDHR or a similar legal act, but it is governed in a way which gives rise to complaints about its implementation or material adherence to the protection clauses; or
(3.) where the state formally and materially rejects the UDHR and the human rights protections.

Non-liberal policies typically fall under (3.) A good example here is China and its rejection of the internationally accepted system of human rights protection in favor of what is called *human rights with Chinese characteristics* (Ren, 2018). China's legal scholarship promotes two controversial claims with respect to human rights, including privacy (Chan, 2015). First, that the scope of human rights available to people living under the authoritarian government is in some sense sufficient. This means that the UDHR is seen as "extra" in many respects, limiting the capabilities of the national government to achieve greater economic and strategic good. The second claim which China is advocating is bi-partite: (1) that the people of China generally have no expectation of their human rights being respected by the national authorities, and that (2) the consequence of this is that the authorities would not contribute positively to the social development by in fact respecting these rights, meaning that in some sense human rights are alienable or marketable, especially when economic progress comes into perspective. This rhetoric, containing striking misinterpretations of the nature of human rights, gave rise to a number of studies and analyses, which are relevant to the perception of privacy as well. For example, Staerklé and Clémence (2004) demonstrated that there exists a principle-application gap, which causes individuals committed to the idea of protecting human rights to tolerate or even mitigate violations, especially ones coming from the state authorities. Moreover, back in 1988, Mitchell and McCormick (1988) argued based on the examples ranging from the Soviet Union and the British colonies in India to African undemocratic regimes, that the governments *typically* explain the violations of human rights using economic or security factors. Yet others have pointed out how the policies of *minority rights with Chinese characteristics*[2] led to severe limitation on sovereignty in Tibet and Hong Kong, among others, and over 1.5 million Muslim Uighur residents of Xinjiang being detained in concentration camps (Zenz, 2019). In this light,

[2]See He (2005) for a prospective exposition of the policy.

China is clearly categorized as a state which rejects, both formally and materially, the project of inalienable human rights as described in the UDHR.

An important element of the relationship between the human rights project, including privacy, and non-liberal approaches is that there exists a parallel in scholar's propensity to offer critique of the human rights as emancipatory force as their exploration of alternative philosophies, including political and social philosophies, which concern the pursuit of happiness and freedom. The system of "human rights with Chinese characteristics" proposed by the CCP is but one such alternative philosophy, and rather extreme at that.

A number of other non-liberal proposals have been offered in the literature, including that by Kapur (2014), who argued that the liberal humanism of human rights has failed to address the needs of the Indian society. She offers a feminist and post-colonial critique of liberal humanism as applied to India and explores the *Advaita*, a non-dualist philosophical tradition. The focus of Kapur's critique is that the human rights project, although it is but one type of emancipatory project aiming at facilitating universal enjoyment of freedom and happiness, has effectively cut short the alternatives, especially in countries which at some point in history found themselves under a colonial rule of the West. These alternatives, argues Kapur, also include essentially non-liberal traditions. In Kapur's approach, the relationship between the rejection of human rights and seeing alternatives to liberal political traditions is significant.

This postulated closing-off of alternative facilitators of freedom and happiness demands more attention at this point. Did human rights project indeed marginalize or negate feasible alternative social and political solutions? According to Kapur, the human rights project hindered the development of its alternatives by the sheer power of its success. Kapur relies on the following claims made by Kennedy and Brown:

> But there may be something to the claim that human rights has so dominated the imaginative space of emancipation that alternatives can now be thought only, perhaps unhelpfully, as negations of what human rights asserts – passion to its reason, local to its global. (Kennedy, 2004, p. 9)

> Human rights activism is a moral-political project and if it displaces, competes with, refuses, or rejects other political projects, including those also aimed at producing justice, then it is not merely a tactic but a particular form of political power carrying a particular image of justice. (Brown, 2004, p. 453)

Based on these passages, Kapur argues that the human rights project is by nature not "a universalizing project for human betterment" (Kapur, 2014, p. 28), but a project of

governance relying on political power for its execution. This claim is widely accepted among the human rights scholars, negotiators, and politicians engaged in human rights protection. What testifies to this is the very fact that (1) the projects of describing the nature of human rights in the language of law are continuously open and active, and (2) the scope of acknowledgment of human rights is globally negotiated through law and politics, as opposed to social philosophy and intercultural exchange. Regardless of whether this critique of human rights is aimed at their legal-political form, or their philosophical underpinnings, Kapur identifies the central flaw of the human rights project in that its implementation can never be complete, thus marking the project with imperfection. This, in turn, "produce a yearning for a nostalgic past when politics appeared more potent and social justice agendas more achievable" (Kapur, 2014, p. 34).

In will now I briefly summarize Kapur's own proposal, meant to replace the *entirety* of the human rights project, including privacy as described in the UDHR. She suggests that the philosophical tradition of non-dualism, *Advaita*, may be seen as a non-liberal tradition of pursuing freedom and happiness, and one which is not confined to human rights or their liberal humanist underpinnings. On the basis of what she calls the non-liberal understanding of the concept of time, the subject, freedom and happiness in the tradition of *Advaita*, Kapur contests the claims made by Martha Nussbaum and Catharine MacKinnon in feminist political philosophy to the effect that the happiness of women and minorities can be achieved through rights and freedom of actions. According to Kapur, freedom can also be achieved by "perception and discernment", that is, passive acceptance of the social-political events and actions of others. Kapur challenges the claim that there exists a connection between happiness and freedom, and the satisfaction derived from the quality of live, including good health, money and comfort. In other words, Kapur argues on the ground of the *Advaita*, that (i.) happiness is not necessary for a good life, and that (ii.) freedom is satisfactorily attained by accepting one's fate, as opposed to having tools to exercise one's rights taking appropriate actions.

Note that when applied to privacy, Kapur's proposal is suspiciously similar to the classical liberal proposal described by De Bruin (2010) as representing the liberal skeptic. Both approaches embrace the strictly instrumental value of privacy (or human rights more general). Similarly, both postulate that comfort, especially material, economic comfort has to weighed against individual human dignity or psychological well-being. It seems that the *Advaita* yields similar consequences in replying to the argument from perspective change and the argument from autonomy as those produced by de Bruin's liberal skeptic. This confluence between liberal and non-liberal critique of human rights is clearly paradoxical, especially since both approaches rely on the opposition between

the underlying values postulated by liberal and non-liberal political philosophy.

Observe also that Kapur proposes a qualitatively different understanding of *freedom*, which does not correspond to actionable, inalienable property rooted in the tradition of the human rights project. This makes debating the human rights along this differentiation a purely nominal, spurious endeavor. The criticism of human rights as such, and privacy in particular, presented so far relied on the proposal to simply forego the project of actionable freedom and human rights in favor or another, more economically beneficial way to organize the law and society. The legal acts such as the UDHR are fundamentally political in that they openly reject this proposal, regardless of whether it is put forward by a government which identifies as liberal or non-liberal. This has far-reaching consequences for the critique of the right to privacy in its various legal and political forms. Namely, the opposition against privacy protection cannot be automatically identified with either liberal or non-liberal political philosophy. Conversely, privacy protection cannot be unequivocally ascribed to either liberal or non-liberal political agenda.

3.2 Political privacy as a collective human right

In this section, I focus on the role of privacy, and especially political privacy, in protecting collective social agendas and rights. My aim is to show that privacy of individuals, regardless of whether we see it as having an inherent or instrumental value, is necessary for protecting collective values and initiatives. In this sense, privacy is *at the very least* instrumental to the success of processes which allow groups and communities influence the social, political and economic reality.

I start by presenting two case studies, one from China and one from France. In both cases, individual citizens attempted to maintain certain collective values, including doing so *via* a claim to privacy. In China, collective social initiatives concern both ordinary citizens, who are not directly involved in political activity, as well as activists, who attempted to promote a particular social cause without a direct relation to state security. I analyze the case of a decentralized activist movement, operating with the intention of supporting democratic rule in China through changing the operations of the government without violent action. For France, I discuss an instance of state surveillance concerning climate activists.

Through these case studies, I challenge the assumption that the conflict between privacy protection and state competence (including competence in the area of security) is the question of a trade-off between strictly *personal* freedom (hence an egoistic good,

serving primarily the individual) and collective benefit. To the contrary, many modern cases of privacy violation are motivated by the state's strive towards targeting and limiting *collective*, not individual, values and agendas. In the context of modern surveillance technologies, states are rarely interested in any particular person. Rather, they try to modify the trends and behaviors which concern entire communities. Privacy, and political privacy in particular, emerges here as one of the very few protections in the conflict between state's politics and collective values of the communities subjected to the state's authority.

3.2.1 Collective social agendas and privacy: case studies

Case study: the Weiquan movement

The conflict between the CCP and the Weiquan movement (*wei quan* meaning *rights' defense* in Mandarin) concerned a dispersed group of lawyers, legal experts, and intellectuals aiming to protect and defend the civil rights through litigation and legal activism. The movement drew in some of the most influential lawyers and activists in China, such as Chen Guangcheng, He Weifang, Xu Zhiyong, Guo Feixiong, Gao Zhisheng, Teng Biao, Zheng Enchong, and Li Heping, as well as a number of so called *barefoot lawyers*. The latter are citizens without formal legal education, who learn to file civil complaints, engage in litigation, deal with the police and other state authorities, as well as promote the knowledge about civil rights among their fellow citizens (Nesossi, 2015).

The Weiquan lawyers engaged in a number of collective and minority causes (Hualing et al., 2008). Their defense of ethnic minorities followed, among others, the 2008 protests in Tibet (which resulted in the imprisonment of at least 670 Tibetans and at least 4 executions), when Teng Biao, Jiang Tianyong, and Li Fangping offered legal aid to the prosecuted Tibetan community. On behalf of the Tibetans, the Gongmeng[3] challenged the government interpretation of the protests, which claimed that they were essentially an attempt at domestic terrorism, masterminded by the Dalai Lama to disrupt the Beijing Summer Olympics in 2008. In May 2009, the Gongmeng issued a paper in which they suggested that the Tibetans protested in response to the rise of economic inequities, the overwhelming Han Chinese settling in the region and religious persecution. Moreover, the Gongmeng's proposed solution to the protests was for the CPP and the local authorities to better respect and protect the rights and interests of the Tibetans, especially their

[3]The Gongmeng (actually: *gōngméng*), or the Open Constitution Initiative (OCI) was an organization consisting of lawyers and academics, including Xu Zhiyong and Teng Biao, established in 2003 and shut down by the Chinese government in 2009 (Zhou, 2018).

religious freedom, and to reduce the economic inequality between the Tibetans and the Han Chinese.

The range of measures used against the Weiquan lawyers and similar initiatives in China relied, among others, on the possibility to conduct surveillance. To introduce surveillance measures more effectively, a model of communications network was built, connecting lawyers, activists and other citizens who engaged in civil rights protection. From the get-go, the movement was described by the CCP as a domestic security threat. Li Heping, for instance, was famously called "more dangerous than Bin Laden" and soon detained in what is known as the 709 Crackdown (or the 709 Case), a mass arrest incident involving 709 civil rights lawyers (Halliday, 2016).

Clearly, neither the causes defended by the Weiquan lawyers or the Gongmeng, nor their own initiative, can be reasonably evaluated as security threats or terrorism. The most radical proposals in the movement included, *e.g.* Yu Wensheng calling for the removal of Xi Jinping and reforms in the legal and political systems. Certainly, well-justified criticism of the political authority does not warrant anti-terrorist measures. Note also that none of the causes which the Weiquan lawyers supported was strictly about respecting the rights of an individual. On the contrary, the freedom of expression cases, those involving land rights, judicial independence, women's rights, as well as minority repression, involve entire communities of citizens.

The surveillance measures used against the Weiquan lawyers led to the shut down of the movement, and a range of repressions, including various forms of intimidation and harassment by the security forces. For instance, on September 28, 2007 the public security bureau in Beijing told Li Heping and his family to leave the city. On September 29, Li was abducted by a group of 12 plainclothes men and held for eight hours, beaten, shocked with electric batons, and later dumped in the woods around Beijing. In the meantime, his house has been ransacked, his computer wiped out and his legal licence stolen. Less than three years afterwards, Li was abducted and interrogated by security forces because of his attempt to meet up with Tang Jitian, also a lawyer. Li knew that his home was under constant surveillance and the police (in teams of up to four men) followed him wherever he went (MacLeod, 2011). Li was abducted again on July 10, 2015, as a part of the 709 Crackdown and as of 2021 was still missing.

Similar measures were taken against other lawyers and activists associated with the movement. In trying to address a question of *why* such drastic measures were put in place against the Weiquan – all of whom are communally engaged people, intending to work for the benefit of their country and fellow citizens – one can engage in a political analysis of the CCP's domestic policy and explain how the civic rights threaten the future

of these policies. Ultimately, however, these measure were taken up, simply *because they were available* to the Chinese government at the time. A government, totalitarian or not, can be assumed to use all forms of pressure and influence which are at its disposal, regardless of whether the specific solution is socially mandated or not. In the context of privacy, the case of the Weiquan lawyers suggests that as a society, we should not put in place the tools which we are not able to control and oppose. Of course, in China there was no possibility to oppose the surveillance and repression tools. However, the EU member states' governments have also been attempting to define socially disliked groups as "internal enemies", as a pretext for developing surveillance tools later used at the majority of their citizens.

Case study: climate activism as domestic terrorism

Non-Violent Action COP21 (ANVCOP21) is a grassroot movement of French citizens who fight "climate change and the social injustices it engenders".[4] Their methods include many forms of non-violent resistance and protest, used to resist projects and policies which have negative impact on climate change. In some cases, the group relies on civil disobedience; for instance, removing portraits of Emmanuel Macron from the walls of town halls across France in order to draw attention to what the group sees as the president's failure of climate leadership. The action began in February 2019 and involved 276 activists by April 2019 (Sauer, 2019).

The response of the French authorities was immediate. By April 2019 with 20 people prosecuted, 22 detained and 16 police searches carried out in order to stop the takedown of presidential portraits. What is even more surprising, however, is that the group's non-violent protest was almost immediately classified as an act of domestic terrorism by the French police. Consequently, the Bureau de la Lutte Anti-terroriste (Blat), the central office of counter-terrorism activity in France, started investigating the ANVCOP21 members and group operations.

Sauer (2019) indicated that the hard response of the French government has a wider context both in France and in the EU. In February 2019, high commissioner of human rights Michelle Bachelet recommended the UN to investigate France for excessive use of force against the *gilets jaunes* ("yellow vests") protesters. In December that same year, the commissioner put forward a statement of support for climate activists (Bachelet, 2019). However, the French government has been expanding its discretion in using

[4]This is the translation [by AS] of a statement taken from the organization's website, url:https://anv-cop21.org/le-mouvement/ (Accessed July 6, 2021).

anti-terrorism measures and surveillance for a while, despite the calls for limitations put forward by political experts and legal scholars.

Back in 2016, journalists and analysts called for prevention of arbitrary policing by adopting prior judicial controls over anti-terrorism measures (United Nations, 2016). The state of emergency in France (in force from November 13, 2015 to November 1, 2017) allowed only for an *ex post* judicial review and provided time needed to pass the new, harsher counter-terrorism legislation. Together with November 2015 law on surveillance of international electronic communications, which increased the state's capability for collecting, analyzing and retaining communications content and metadata without authorization or judicial review, the new counter-terrorism measures created a bottleneck for citizens' political activity, which was difficult to pass.

It is an open question how, if at all, under the current application of French counter-terrorism laws and policing measures, political activity of the citizens, especially in the form of protest or non-violent disobedience is feasible. In the light of unproportional use of force and suppression of even the most benign forms of protest, how can the political activity typical of the democratic state with the rule of law continue in France? The UN called for France to not extend the state of emergency beyond February 26, 2016, but the call was unsuccessful. The UN experts, including David Kaye, Special Rapporteur on freedom of opinion and expression and Maina Kiai, Special Rapporteur on the rights to freedom of peaceful assembly and of association, and others, spoke against the house arrests of the French climate activists which were made possible by the state of emergency in 2015 and 2016. They also warned the French government against abusing the capabilities stemming from the state of emergency (United Nations, 2016):

> While exceptional measures may be required under exceptional circumstances, this does not relieve the authorities from demonstrating that these are applied solely for the purposes for which they were prescribed, and are directly related to the specific objective that inspired them.

In January 2021, a new wave of mass protests arose in France over a strengthening on security laws, including a bill which makes it a criminal offense to film and publicize images of police during operation, thus also making it impossible to share and publicly scrutinize images proving acts of police brutality (Agence France-Presse, 2022). From a purely technical perspective, the methods of surveillance currently in operation and being used against the citizens in France are well documented in cases of climate activists. In a crowd-funded, groundbreaking documentary on privacy and surveillance

entitled "Nothing to Hide",[5] two Berlin-based journalists, Mihaela Gladovic and Marc Meillassoux included testimonies of French and German activists, showing that both targeted and mass surveillance have become a standard in the state's approach to activism – though, as I will show later, the German right to notification made the German case much less harmful than the one in France. Joël Domenjoud was one of the 26 COP21 activists put under house arrest under the state of emergency law in France. Notably, Domenjoud was also a part of the legal team of COP21, actively working on supporting the activists' work within the organization's non-violent agenda (Peillon, 2016). The level of surveillance employed against Domenjoud prevented him from contributing to the work of the COP21 legal team. Since all communications, including all electronic and mobile communications, from and to Domenjoud were monitored, it was impossible for the team to coordinate and act without police supervision. The near complete surveillance of communications of this particular activist not only neutralized his impact within the organization and against the state, but also prevented him from, *e.g.* safely using email and other electronic channels to contact his friends and family, and limited his use of electronic devices in general. This in itself constituted a form of repression, since the fact of being under observation was clear to him from a certain point in time, and no countermeasures were available to him. Physical surveillance was employed as well, with the police following Domenjoud whenever he went. Whether this measure was meant as actual surveillance or simply as an intimidation strategy is open. However, Domenjoud's surveillance was most likely initiated based on his association with COP21 and as such did not stem from *mass* government operations.

The situation was different in case of Andrej Holm, German sociologist working on the topic of gentrification in Berlin. I include a brief description of his case here, so as to give comparison with the COP21 case in France, where no right of notification exists, nor are there any requirements to justify surveillance operations. Holm was put under surveillance by the German intelligence police agency (Bundeskriminalamt, or BKA) based on the keywords in his internet searches, which included "gentrification", "reproduction", and "Maxist-Leninist". Based on seven keywords, all common words for a researcher of his specialization, Holm was placed under full-fledged online surveillance in 2006 and suspected of being a terrorist in a militant group. Together with Holm, a network of other people was likewise surveilled, including his friends and colleagues. Among them was an activist and political scientist Anne Roth. And since in Germany such cases of surveillance can be well-documented by the citizens thanks to the right

[5]The full version of the documentary is available online in open access, url: https://vimeo.com/nothingtohide (Accessed May 10, 2021).

to notification, the parties involved are able to seek legal recourse *ex post* and raise the issue within the public debate. On the other hand, because Holm's case was one of untargeted mass surveillance (based on a purely algorithmic evaluation of mass records of online searches), it can also be seen as more serious, politically speaking, than the case of Joël Domenjoud and the rest of COP 21 activists.

However, in the French surveillance landscape (described in section 2.1.2), no right of notification is available. Given the flow of technologies within the EU, it is safe to assume that mass surveillance measures very similar to those in Germany are being used against activists, scholars and other citizens in France as well. Therefore, any citizen undertaking an activity or research in areas or topics which may be classified as problematic to the French state, should, as a matter of fact, expect to be placed under surveillance similar or exceeding that used against Holm, Roth, and others in Germany.

3.2.2 The emergence of collective rights

Wolfers (1952, p. 481) observed that both terms, *national security* and *national (or public) interest* are ambiguous in that they are likely to mean different things depending in the context. Some particular events, such as the 9/11 attacks bring about systematic transformations in national security. For instance, Zelikow (2003) gave an account of the national security transformation planned by the Bush administration after World Trade Center attacks. His description of the direction of the transformation included clear colonial and hegemonic ambitions, referred to as the "unique responsibilities [of the USA] as the greatest power in this pluralistic world" (Zelikow, 2003, p. 19). Hence, the precisification of the national security as performed by the state administration may also be, and, in fact, often is ideology-driven at least to a certain extent.

New elements may be included in the scope of national security agendas as particular problems emerge as a threat to public interest or national interest. For instance, Levy (1995, p. 36) argued that global environmental degradation was a threat to the USA, while defining three forms of connection between the environment and security, existential, physical and political.[6] Nevertheless, it is safe to say that non-violent activism, climate or otherwise, as well as general political involvement of the citizens *cannot* be

[6]The existential link relies on the relationship between certain aspects of the global environment and the US national values, which, are so strong that they give rise to security interests. The proponents of this view are, among others, Jessica Tuchman Mathews and Norman Myer (Levy, 1995, p. 36). The physical link means that the global environmental degradation has consequences which may arise as physical threats to US security. Finally, the political link is indirect and includes issues such as the appearance of environmental refugees, resource wars, *etc.*. Surprisingly, Levy considered the political link between the environmental degradation and national interest as "the weakest substantive threat to US security".

included among the security threats in a democratic state. In other words, a state which aspires to be called democratic must formulate its security agenda in a way which makes normal political activity, including protests and civil disobedience, possible and feasible.

Given Levy's assumptions, it is clear that in the case studies discussed in sections 3.2.1 and 3.2.1 the measures taken against activists and citizens do not fit into the notion of national security, at least not in conjunction with the principles of a democratic state. That is, state surveillance, including mass surveillance, often has little to do with the national or public interest. What is more important here, however, is that neither of the presented case studies concerned a clash between strictly personal privacy and national or public interest. Rather, privacy of individuals is treated as a collection of pressure points which allow the state to diminish and neutralize a *collective* agenda of a group of citizens. Political privacy of the collective can be eliminated by targeting the individuals who engage in it. When mass surveillance is available, a simple network analysis allows the state to identify those individuals whose neutralization will be the most cost-effective. For instance, the French state decided to force disengagement from the members of the legal team of COP21 through home arrests, as well as physical and communications surveillance.

For this reason, I argue that political privacy must be considered as spurring a collective right, in addition to individual rights. In the recent years there has been a surge in collective rights programs, including in the debates on cultural appropriation and slavery reparations. Although there are stark differences between the problem of privacy and those of cultural appropriation or slavery and its consequences, note that the emergence of the idea of a collective right is relatively recent. As a result, the way in which the collective rights programs are formulated will be similar, often relying on similar theoretical infrastructure, even if the nature of the rights varies from case to case.

Certain rights are more likely than others to be considered as applying to a collective. For instance, the right of freedom of association by definition involves multiple individuals and thus cannot be granted to each citizen separately, but denied when groups or collectives are involved. Guttman (1984, p. 122) observed that while various contributions developing the right to freedom of association contain both an individualistic aspect and a collective aspect, the former received more attention. In relation to privacy, Guttman also referred to NAACP *v.* Alabama, where the relationship between privacy of association and the freedom to associate was established. Namely, the Court decided that membership disclosure violates freedom of association. In this case one could say that political privacy protects the right of political association. In turn, the right to privacy and the right of political association protect the right to vote, which is also uniquely

political (*cf.* Guttman for detailed argumentation).

In the legal system of the USA, privacy as protected by the 4th Amendment was thought to touch upon individual and collective interests at least as far back as the 1970s, notably within works of Dworkin (1973) and later Doernberg (1983). However, in these and other contemporary legal analyses, the collective aspect of the right to privacy was seen as opposing individual freedom. That is, the collective need for *limiting* the scope of privacy was in the center of attention, while the benefits of privacy protection to the collective interest were mostly ignored. This line of reasoning is consistent with a view which persisted in later scholarship, where the desired scope of privacy protection was defined as whatever remained of private interest once it was reconciled with collective interest, the latter being interpreted as countering privacy.

As a result, the very origin of the development of collective rights as a concept was rather complicated. Sanders (1991, p. 368) pointed out that the notion of *group rights* or *collective rights* was initially often used by non-democratic states to justify human rights violations, including, in case of South Africa, apartheid. Following similar logic to that of Dworkin (1973) and Doernberg (1983), non-democratic leaders conjured up collective interests which would justify violations of individual rights on a case by case basis. Sanders (1991, p. 368) also observed that the rights of minorities, construed as group rights from the start, were seen as a threat to the integrity and power of the nation-states. This perspective can still be found in today's nation-states, including the ones described in section 3.2.1. Public security, especially national security, is often presented by the state as requiring far-reaching violations of group and collective interests and rights, especially when the violation may be disguised as directed against individuals instead of groups and collectives.

Fortunately, more constructive approached to group and collective rights emerged in parallel, including one where the rights of Indigenous peoples are considered collective rights (Clinton, 1990). And although collective rights were mostly considered as applying to minorities and colonized peoples (Dinstein, 1976), soon they developed into *human* rights, which could, at least in principle, be applied or extended onto humanity in general. In the political context, the idea of collective human rights was still debated in the context of political science. Freeman (1995, p. 27) for instance reiterated the argument summarized by Clinton (1990) that minority rights (here equated with group rights) are exceptional, as they limit the sovereignty of the nation-state.

By the time of the political debate of the 1990s, the idea that human rights actually are (and ought to be) transnational in nature was widely spread. In a book by Felice (1996), Falk argued that collective human rights allow for a "conceptual recasting of

the human rights discourse", which "is a coherent and helpful way to make difficult civilizational passage from modernity to a type of postmodernity that is reconstructive, not deconstructive" (Felice, 1996, p. xiii). And although the project of third generation human rights met with initial resistance (Kooijmans, 1990), the underlying notion of *solidarity rights* was sufficiently rooted in international human rights jurisprudence to allow for including certain third generation rights in subsequent declarations of the UN. This included, *e.g.*, the 1986 UN declaration on the right to development (Kiwanuka, 1988; Sengupta, 2001). Following a similar intuition, Clancy (2010) proposed to add the collective aspect to the 4th Amendment right, effectively construing a partial collective right to privacy. In this dissertation, I propose that we consider political privacy to be a collective human right – in addition to being an individual right – and add it to the catalog of third generation human rights, alongside the rights to development, peace, and healthy environment.

Cultural appropriation *v.* collective rights of the Indigenous peoples

Collective interest, as well as the rights which protect it, can have a lasting positive impact on societies, and one which is by nature *intergenerational*. Grzybczyk (2021) proposed changing the approach to many of those rights which so far have been perceived as uniquely applying to individuals. This includes various intellectual property rights, including ownership of all products of a specific culture which constitute part of the culture's heritage. The notion of *cultural appropriation* was coined to name the specific type of theft, which takes place when a person or a business agent who cannot legitimately represent the culture in question, derives or uses the products of the culture, usually for profit (either financial or indirect, rooted in projecting values or aesthetic specific to the appropriated culture). Cultural appropriation is most dangerous in situations when an entity in position of power appropriates the culture of a colonized or otherwise repressed group.

Similarly as with the right to privacy, a violation of *cultural assets* may take place *via* illegitimate use of intellectual property of an individual, *e.g.* the work of a specific artist. Such a violation also creates a dent in a more general cultural ownership, which normally benefits the collective of people who legitimately share in the culture. Benefits of cultural ownership may be found in the capacity to create a distinct group identity, develop this identity in accordance with the shifting group values and objectives, and also in the ability to profit financially and socially from the shared identity and the cultural products originating from it. Grzybczyk (2021, p. 20) observed that lack of

protections for group rights surrounding cultural ownership resulted in fading away of various folk traditions and products. Similarly, unrestricted chipping away at individual privacy in situations where political behaviors and attitudes depend on it will take a toll on the future development of democratic institutions and good practices. In this sense, political privacy can be seen as a measure of protecting the social and political heritage of the collective.

Collective rights and collective damage: slavery reparations in the US

Another important intuition concerning privacy as a collective right comes from observing the debate on collective damage incurred on the African American population in the US. Arguing from a moral and legal standpoint, Thompson (2002) laid ground for a theory of reparations where the group which benefits from the heritage of slavery has a moral responsibility to make up for the setbacks which the past damage has caused in the descendants of the enslaved.

Leaving aside numerous questions and controversies present in this particular debate, one may take from it a crucial notion that doing damage to a group or a collective should, in addition to individual reparations, also include group reparations. In order for this to happen, an appropriate organ or institution must be put in place, capable of receiving and redistributing the group reparations for the damages incurred on the collective. I argue that this should be case with political privacy as well, even if specific implementation of this rule may prove difficult.

In the case of the US reparation program, group reparatory measures may include putting in place more equitable education and work opportunities for the descendants, increasing welfare subsidies in order to make up for the wealth gap between the descendants of the slaves and slave owners, as well as ensuring that basic services such as access to healthcare, law enforcement, or transportation are equally available to both groups. This reparatory distribution of wealth and services may happen *via* the federal or state budget because the state is not the offending party, assuming that the legal and political tools of oppression have been mere instruments, but not agents of the damage to the African American community. In the case of privacy, the offending party is often the government, which means that an independent body or network of bodies would be needed to decide on the fair redistribution of reparations for political violations, including violations of political privacy.

3.2.3 Summary

In this chapter, I discussed the right to privacy in selected liberal approaches, together with their criticism. I contrasted them with some of the non-liberal approaches to privacy, especially the arguments which reject the right to privacy together with other universal human rights. This non-exhaustive philosophical overview was meant to lay the groundwork for a presentation of cases where the right to privacy emerged as a collective human right, in addition to being a right an individual right.

As the discussed case studies show, political privacy does not depend on accepting liberal political philosophy, or even embracing the limits of strictly personal privacy. In other words, even those of us who are willing to spy and be spied on by our neighbors, should put effort into protecting political privacy as long as they want to live in a state which is minimally democratic, that is, allows for safe use of critical political tools of the voters and citizens without the risk that their actions, words, and relationships are going to be used as a leverage against them.

Chapter 4

Political privacy, surveillance capitalism, and public security

In this chapter, I discuss how political privacy relates to global economics and public security. I introduce the notion of *surveillance capitalism* as defined by Shoshana Zuboff (Zuboff, 2019). Although the definition of surveillance capitalism which emerges from Zuboff's work is rather versatile, including characterizations based on human rights and social order, her analysis focused on economic and not strictly political elements of privacy and the right to privacy. However, since the importance and relevance of Zuboff's findings is indisputable – there exists a strong feedback between politics and economics – then it is necessary to give account of the main tenets of the theory of surveillance capital before attempting further examination of political attitudes towards privacy and psychology of privacy, and their relation to public and national security.

One of the most important observations stemming from Zuboff's theory of surveillance capital is that surveillance capitalism gives rise to a new type of power (including, but not limited to, political power), that is, *instrumentarian power* (or instrumentarianism). Instrumentarian power relies on the ability to predict and systematize human behavior and allows those who wield it to shape human behavior in line with their own goals and preferences. Although shaping and influencing human behavior, including the behavior of masses is not a new phenomenon, the creation of processes and tools used to truly *know* behavioral patterns, that is, being able to explain and predict human behavior with near perfect certainty and on a global scale, is entirely new and recent. Here also lies the reason why privacy, including political privacy, is not so much dependent on technological advancement, but rather – on the development of the new economic, social and political paradigm that is surveillance capitalism. Comparing surveillance

capitalism to earlier forms of capitalism, one can say that surveillance and surveillance capitalism are not inherent to participating in any technology, similarly as the ability to manufacture objects out of raw material is not inherently rooted in capitalist economy. The raw materials (in earlier economy this being wood, water, ore, or other resources, in surveillance capitalism – users, that is, real people and their behavioral patterns) and the tools and technologies applied to them could just as well be used outside the economic paradigms of capitalism and surveillance capitalism. And just as the abuses of capitalist economy are not due to tools such as wood cutters or automated production lines, the abuse of our privacy is not due to technologies being available, but due to the logic which underlies surveillance capital.

4.1 The emergence of surveillance capitalism

4.1.1 First and second modernity

The overarching theme of the story of surveillance capital is that of "second modernity". The first mass consumers in history participated in what is known as "first modernity", a brief industrial period of history (ending roughly in the 1960s) where human life became *individualized*, in the sense that great numbers of people were able to break away from the norms, rules and meanings enforced by tradition, lineage, and other social and historical conditions. This separation meant that human life became *open ended*, a process to be actively shaped or discovered, and not a certainty to be enacted, as in pre-modern times. Zuboff remarked that although the deficiencies of the social or economic environment makes open-ended future unlikely for many people, even the most disempowered of them cannot experience their fate as the only possible story (Zuboff, 2019, p. 33). At the same time, the emergence of *individualization* has nothing to do with the neoliberal ideology of *individualism* or the psychological concept of *individuation*[1]. Individualization relevant here is a long-term consequence of modernization and does not depend on any philosophical or psychological prerequisites.

In comparison to the "first modernity", the challenges faced by the inhabitants of the "second modernity" are even more complex. On the one hand, "second modernity" people experience the right to choose their own lives, but, on the other hand, this right is also not something one can resign from – it becomes a necessity. Ready availability

[1]Zuboff (2019, p. 33) understood *individualism* as the ideology which shifts all or most responsibility for success or failure onto a highly idealized individual, existing in social and familial vacuum. Psychological *individuation* is defined as a lifelong process of self-development.

of life-improving phenomena such as public healthcare, cheap consumer goods, intellectually demanding work, and so on, makes the "second modernity" the stage where humanity may shift away from collective solutions in favor of the exploration of an individual "self". However, Zuboff pointed out that because of the collision between the consciousness created by the second stage of contemporary modernization and the economic violence stemming from decades of neoliberal governance, the "second modernity" does not offer a trouble-free everyday reality for its citizens. Rather, economic conditions tend to limit the possibility of reaching one's own existential and social and political potential, even when the goal seems well within our cognitive and physical capacity. This so called economic "neoliberal habitat" became a breeding ground for anti-democratic policies and solutions, one of which includes a push back towards imposing the absolute authority of market forces in the lives of the citizens (Zuboff, 2019, p. 39):

> In the "crisis of democracy" zeitgeist, the neoliberal vision and its reversion to market metrics was deeply attractive to politicians and policy makers, both as the means to evade political ownership of tough economic choices and because it promised to impose a new kind of order where disorder was feared. The absolute authority of market forces would be enshrined as the ultimate source of imperative control, displacing democratic contest and deliberation with an ideology of atomized individuals sentenced to perpetual competition for scarce resources. The disciplines of competitive markets promised to quiet unruly individuals and even transform them back into subjects too preoccupied with survival to complain.

To make matters worse, lack of economic stability brought about by the rise of absolute market freedom of raw capitalism, discourages social participation. As Piketty (2013) argued, capitalism without strong limitations by democratic institutions is *anti-social* and has caused many regions to revert to the preindustrial, "feudal" hierarchies due to the sharp rise in economic and social inequalities. A compelling case study of economic and social inequality caused by market-based order was presented by You Yenn (2018), who focused on the social and economic conditions in Singapore.

Another element of the neoliberal habitat of surveillance capital was the acceptance of the dogma of "shareholder value maximization", that is, an idea that the sole *objective* purpose of the firm is to bring profit to its shareholders. In particular, no bounds on social, political or environmental impact were imposed on firms and their operations. In this sense, the abominations of surveillance capitalism stem from the same source as the large-scale ecological disasters caused by corporate exploitation of the natural

environment. A crucial observation here is that, despite what most marketing campaigns try to convince the consumers that social, environmental and political responsibility is not a solid component of the logic of business operations of modern firms.

In these conditions, it is understandable how the forces behind "real" capital seized the digital resources. It is also natural that citizens of the "second modernity" slowly started to consider the digital sphere their primary social and political playing field, as most online activities did not, at least in the early stages of Internet development involve any large investments or economic power, contrary to the conditions in extra-digital reality. Soon, citizens using mass digital services were turned into the raw material of the new market paradigm, that is, surveillance capitalism. In 2004 Google launched targeted ads based on markers found in users' Gmail correspondence. In 2007, Facebook followed with Beacon, a tracking counterpart of the software used by Google, but targeted at its own users. Zuboff (2019, p. 49) makes clear that users were at no point considered a party in this market process. Rather, advertisers were seen as clients of the firms which used surveillance in order to extract the most value our of their raw material – the users. This exploitation mechanism successfully mimicked the neoliberal social ideology by imposing unreadable documents called "privacy policies" on users who accepted them automatically, inadvertently agreeing to a "contract" the shape of which they have no change of influencing. Finally, the surveillance capitalist firms turned towards presenting the exploitation and violation of users as a necessary evil, a cost of "free" online services which they provided.

4.1.2 Neoliberal economy and the "policy vacuum"

The pressures from the societies of the second modernity, especially concerning equal rights, political participation of marginalized groups, and austerity measures, added to the confusion and chaos in which the political decision-makers of the mid-1970s found themselves. Facing the period of economic stagnation and crisis in the USA and UK, the politicians of the era sought for a remedy to the "policy vacuum" which hindered further social and economic development in both countries. The neoliberal economists of the time saw this impasse as an opportunity for realizing their radical free-market economic theories. The political ideology which accompanied the free-market agenda soon spread from Europe to the Anglo-American world. From the policy-maker perspective, neoliberal free-market economy offered an easy solution out of the "policy vacuum" problem. Instead of creating policies for regulating the emerging markets and social conflicts, the free-market theories suggested that most processes in economy, social and political life

are somewhat self-regulating. This meant that the lack of policies was something to be accepted, or even embraced, rather than remedied.

Zuboff links the emergence of the surveillance capitalism's foundations to the work of three economists in particular. First, Friedrich Hayek, who received the Nobel Memorial Prize in Economic Sciences in 1974. The essence of capitalism à la Hayek required that inequality of wealth and rights was accepted a positive element of unrestrained market forces working their way towards the progress of society. Hayek also laid the ground for the soon to come theory of the firm, which secured the privileged position of contemporary surveillance capitalist firms in their relation to society and public authority. Specifically, the firm was seen as a distinguished agent in the economic system, one which, in optimal economic reality, could operate without any limitations other than those of the market itself. In Hayek's view, the markets "extended order" was superior even to legitimate political authority of the state, which ultimately meant complete submission, individual and collective, to the invisible forces of the market.

Next, Michael Jensen and William Meckling completed Hayek's work by starting the *shareholder value movement* in 1976. In their theory of the firm, they proposed to do away with the pro-social mission of firms altogether. The manager was seen as a parasitic agent, subsisting on the resources of ownership, hindering the growth of shareholder wealth. The market metrics, that is, the indicators of the assumed "extended order" were supposed to help owners limit the cost of management by using an incentive system based on share price of the corporation.

This way of thinking spread towards politics, as the approaching crisis of democracy called for solutions to the new problems, requiring a new type of social and political order. The imperative authority of the market allowed the politicians to postpone making high-stake decisions and silence the growing discontent of the second modernity citizens.

The political evils of the post-socialist era were replaced by new enemies, this time enemies of the free market: state regulation, welfare and other collective policies, individual protections and principle-driven democratic processes. Economic progress was designated as the ultimate goal of societies, where competition was interpreted as a valid alternative to social justice.

4.1.3 Civil unrest as a signal of neoliberalism's success

Zuboff pointed out that the success of neoliberal economy has become apparent by early 2010s. The term *success* has a specific meaning here. Neoliberalism did what its logic

was designed to do: advance those market agents who turned out the most powerful, and demote those who could not match up to the power of the rich. The largest transfer of income to the top in human history took place, causing the living conditions of the majority of the global population to decline, despite the explosive digital and economic growth.

One of the results of neoliberal policies in the USA and the UK was the wave of protests and other acts of civil disobedience, often rooted in the wealth inequalities. Post-transformation life as a regular citizen has become *unbearable* for so many that the durability of growth came under threat.[2] The political systems embedded in free-market economy also became unstable, which brings to light another motivation for state usage of surveillance tools, that is, curbing the risks of protests and revolutions caused by growing social discontent at state management. As I argue throughout this dissertation, political privacy is a natural antidote for instrumentarian power, including instrumentarian power derived from surveillance.

4.1.4 Surveillance capital as the new type of economic power

The needs of people inhabiting the contemporary "third modernity" radically differ from those of their predecessors. Combined with the economic-political fertile ground, those needs enabled a mutation of the capitalist economy, which resulted in "a new breed of economic power" (Zuboff, 2019, p. 52).

New ways of justifying corporate privacy and consent violations became possible thanks to careful framing and redefining the notions such as client, corporation, and service. Before the third modernity, the idea of a corporation violating their clients' privacy as part of their service was outright rejected. Often the very motivation for developing the legal and political concept of privacy was to prevent companies and public institutions from such violations. However, in the new digital economy, the corporations started to label themselves as "service providers" – a move which obscured the old client-company relationship. As service providers, companies were no longer accountable to those who used their services. Clients were replaced by *users*, people who peruse the services while having no control over their conditions. A powerful distraction was born in the form of postulated trade-off between accepting the corporate violations and access to their services. The argument based on this alleged trade off, though invalid both pragmatically and legally, became known as the "get over it" argument, taking its name from the infamous quote by Scott McNealy (see section 3.1.1). By this token,

[2]For a detailed study of the wealth transformations in neoliberal capitalist systems, see Piketty (2013).

the service provided by the corporation was "free", meaning that no payment was expected of the users – as long as they agreed to any and all conditions put forward by the "provider", including violations of their privacy.

One of the bargaining cards in the hands of corporations was that their services were not specified, but rather added up to general access to information, connection with others and market inclusion. In this sense, though users could make do without a particular service, they could no longer forego all of them. The violations allowed the companies to collect raw data and turn it into surveillance capital, selling it to their new "clients" – other corporations and political agents who could make use of the massive collections of data or access and exposure to large groups of "users".

4.2 The psychology of privacy and surveillance

In everyday discussions concerning privacy, as well as in privacy education, arguments based on the perception of privacy are often in the center of attention. Those perceptions and opinions about what should be private and when our privacy is being violated typically originate either from individuals' psychology, or from culture in which they live. In this section, I briefly list the psychological factors which contribute to the everyday perception of privacy, as well as some of the arguments and opinions which they bring to the fore. Notably, these tendencies and biases made possible the use – both by surveillance capitalists and by state surveillance entities – of what Zuboff dubbed *behavioral surplus*, understood as the value which our activity and relationships produce under surveillance.

4.2.1 Psychological incentives behind the behavioral surplus

As Zuboff pointed out, our activities and relationships, and especially the behaviors which are the building blocks for these spheres of our lives, may be turned into *value* when treated as *raw material* for surveillance capitalist production. Since these behaviors are often monitored and recorded digitally, the outcome of this process takes the form of a collection of data: information displayed in a standardized and consistent format, available for further structuring, interpretation, and use.

For instance, a phone conversation between a man and his produces a set of metadata, including the information on when the call started and how long it lasted, where both have been at the time, *etc*. The metadata can be amended by a recording of their voices, eligible for content and emotion analysis later on. A single phone conversation may be

amended by a number of other conversations, not just on the phone, but also ones made in person, through geospatial monitoring of their whereabouts and using their smart devices to make a recording of audio or video. All the data collected in the process of surveillance of the two, may be used and re-used in multiple contexts, and for a multitude of purposes, including sales, advertising, insurance rate calculation, criminal monitoring and prevention, mass data analysis, flow tracking (that is, estimating how many people visit or pass through a given point on the map at each moment), risk estimation, social monitoring, *etc.* If any of the two become distinguished points of interest in the social network, their relationships and other activity, as well as that of their friends and family, will be subject to more attentive, near real time analysis. In particular, the specific elements of the relationship may be leveraged against the father or the daughter in order to force a decision or a confession.

Such scenarios are in fact commonplace in mass surveillance endeavors such as the American NSA's programs. The whistleblower Edward Snowden (Snowden, 2019, chapt. 25) gave an account of one such monitoring which gave the NSA insight into parental bond with a child, where the father was singled out for monitoring because he sent out a job application to an Iranian university:

> The grounds for suspicion were often poorly documented, if they were documented at all, and the connections could be incredibly tenuous — "believed to be potentially associated with" and then the name of some international organization that could be anything from a telecommunications standards body to UNICEF to something you might actually agree is menacing.
>
> Selections from the man's communications had been sieved out of the stream of Internet traffic and assembled into folders — here was the fatal copy of the résumé sent to the suspect university; here were his texts; here was his Web browser history; here was the last week or so of his correspondence both sent and received, tagged to IP addresses. Here were the coordinates of a "geo-fence" the analyst had placed around him to track whether he strayed too far from home, or perhaps traveled to the university for his interview. Then there were his pictures, and a video. He was sitting in front of his computer, as I was sitting in front of mine. Except that in his lap he had a toddler, a boy in a diaper. The father was trying to read something, but the kid kept shifting around, smacking the keys and giggling. The computer's internal mic picked up his giggling and there I was, listening to it on my headphones.

In cases like these, the violation of privacy is multifold. Not only the academic's professional and leisure activity in his home was surveilled, but also his relationship

with his son and wife. By gaining access to a single gateway – the man's computer – the surveillors can also force open the doors to all spheres of activity (including relationships) which are enacted in front of or using the computer or a mobile phone. The idea of this kind of access being even possible, let alone being in actual operation, came as a shock to the international community when Snowden first revealed the American surveillance programs and methods in June 2013.

However, the undoing of the surveillance systems which were already in place proved prohibitively difficult for many, both inside and outside the government. Some of the legal struggles which followed the Snowden revelations were described in section 2.2, but what remains is the following question: if we already know that our mobile and electronic devices are being used to violate the privacy of our relationships and activities, why won't we stop using them? If the social networking platforms used by surveillance capitalists are turining us into raw material, impacting our financial, political and personal decisions in ways beyond our control and best interest, why do we maintain our presence on them? These mass decisions have no political or legal explanation. In order to understand them, one needs to track how the surveillance capitalist companies lobbied for accepting privacy violations early on in their projects, and used psychological biases of their users to their advantage.

4.2.2 Eliminating decisions

One of such biases in human psychology which surveillance capital makes regular use of originates from the decision and attention fatigue, phenomena typical of how human brains function. Social media platforms and other service providers, such as Apple, Instagram, and Facebook, have been successful in making easy the decisions which align with their business agenda and, conversely, making going against them almost impossible for the users.

The events and exchanges which require an action or an expression of consent from the legal point of view, do not necessarily translate into actual decisions which users make in the process of "signing contracts" with a surveillance capitalist firm. As Rustad and Koenig (2014, pp. 1431-1432) observed, the Terms of Use (ToU) of services such as Instagram are structured and executed in a way where accepting them requires virtually no actions for active users and a single mouse click for new ones, but are difficult and resource-costly to repeal or revoke. Moreover, the ToU can only be changed by the platform or the service provider, but not the user, which means that users can only access the offered services at the price of near total uncertainty about how the data regarding

their activity will be used. This includes being unable to decide who will have access to the data, for how long, or whether the data will be given away or sold to a third party, who also may make unrestricted use of it. Even if the specific ToU offer restrictions in using the data at a particular point in time, they can be unilaterally changed by the firm later on, with no tenable path of appeal for the affected users.

There are at least two strategies which surveillance capitalists rely on to stabilize this unilateral bond. First strategy is to normalize the delegation of decision making, for instance, through making their ToU inaccessible, lengthy, and incomprehensible. Users trying to access the platform's services need several hours at best to become familiar with the content of the ToU, possibility being unable to understand them in full without consulting a lawyer, but at the same time they are a single click away from "accepting" the ToU, thus allowing the service provider to make the decision for them. Later on, any change in the ToU requires significant legal effort, such as the class action lawsuit filed against Instagram in 2012 and 2013 (*cf.* Rodriguez *v.* Instagram, Funes *v.* Instagram). Overall, this contractual setup is designed to discourage individual involvement and replace it with apathy and submission to the service provider's financial goals. This kind of conditioning for passivity has by now become second nature to most individuals who engage in online and electronic services as users.

The second strategy, which I will call *no opt-out* (NOO), used in which context is to present the delegation-for-service exchange as something normal, standard, or otherwise unavoidable for an individual. Advertising campaigns for online platforms often rely on human need of belonging, exemplified by the following marketing slogan by Facebook from 2013: "Your friends are waiting inside your phone. Set them free with Facebook Home."[3]

In the context of surveillance-based platforms, simple, intuitive prompts are presented as arguments for the overall fairness the delegation-for-service exchange. Users are led to believe that either everyone else has agreed to the exchange already, so disagreement would lead to isolation from the group, or that there exist no viable alternatives to the service based on surveillance. The latter prompt is closely related to a more general narrative of surveillance capitalists, where technological advancement is defined as logically equivalent to submission not limited to privacy issues. In this area as well, human adversity to change and isolation, as well as their susceptibility to intuitive slogans backed by power of access and connection, work against individuals who might otherwise protest or boycott the abusive ToU and other forced conditions of the services

[3] A tweet on the official Meta account, url: https://twitter.com/meta/status/320916102689472512 (Accessed March 9, 2022).

they use.

This problem is not limited to the decisions concerning becoming a user of the particular service. Social media platforms adapt their marketing and advertising strategies to the social proximity between their users (Song et al., 2014, p. 765). They may also obtain reliable personality evaluations for their users (Golbeck et al., 2011) and later use these evaluations to influence users' behaviors, including political and voting choices (Riezebos et al., 2011). Case studies for the 2014 Scottish referendum and the 2013 General Election in Pakistan were produced by Munir (2018) and Butt and Awang (2017) respectively. The infamous case of Cambridge Analytica engagement in political matters of the US, as well as other countries, were covered by, among others, Wylie (2019) and Isaak and Hanna (2018).

4.2.3 Panopticon *v.* decision-making

Another psychological aspect of perceptions of privacy in the context of surveillance is how human behavior changes under observation. Both pro- and anti-surveillance arguments acknowledge this aspect of observation. As historical cases indicate, workers are easier to control and organize under surveillance, maximizing labor effectiveness. Surveillance is also beneficial for the employer in other ways than through increasing productivity: workers under surveillance may have a harder time establishing personal relationships and creating labor unions, as I will show in section 4.3.3. Regular citizens are less likely to commit minor offenses, such as jaywalking, but also less likely to organize a political opposition or a successful protest (see section 2.1.2). Consequently, a plea for privacy protection is often met with a question about the workers' or citizens' purpose: why do you need privacy? What is it that you are trying to hide?

The pro-surveillance (or anti-privacy) slogan known as *nothing to hide argument* (NtH) is perhaps better characterized as an *incentive* to share information than as an actual argument in the public privacy debate. Marwick and Hargittai (2019) also showed that NtH can also be viewed as a mental coping mechanism among the individuals who display resignation towards privacy violation in the online context. This attitude is closely related to NOO (no opt-out) strategy used by surveillance capital companies from early on, aimed at conditioning individuals who partake in their services to passivity and thus turning people who would normally see themselves as clients into users. The mindset related to the status of a user causes individuals to perceive little to no control over their ability to make decisions related to privacy protection. For those who believe that privacy protection is not possible (or, in other words, information sharing

is not optional, but mandatory), NtH often becomes a consolation and a mechanism to rationalize the inflexible reality of participating in online platforms (Marwick and Hargittai, 2019, p. 1697-1698). Yet another use of NtH was identified by Murumaa-Mengel and others, who conducted a study on privacy perceptions in Estonia in 2014. Estonian residents were characterized in the study as enthusiastic about new technologies, but at the same time skeptical of surveillance, due to the Soviet past of the country. The results of the study suggest that among Estonian residents, NtH was often used as a risk mitigator, a coping strategy in complex informational privacy situations. When individuals were unable to fully comprehend the risks behind perusing online services, especially with respect to privacy risks and confusing practices of the service providers (Murumaa-Mengel et al., 2015, p. 196).

Since the NtH strategy was first put forward, to later be reinforced by the social and political implications of the American "war on terror", many have refuted its legitimacy. Cofone (2019) explored the economic legitimacy of NtH in the context of information disclosure, showing that individuals who have nothing to hide from the perspective of the decision-maker, still have a lot to lose if information disclosure becomes a part of the economic model. This analysis adds to the normative justification of privacy, based on two case studies, involving the use of genetic information in the context of health care, and the value of silence in the context of tax privacy. Solove (2007, 2011a) argued repeatedly that NtH offers an apparent trade-off between privacy and security, but that the trade-off is *false*. Solove (2011b) observed that NtH is often presented as an argument in contexts which involve a very narrow segment of privacy protection, limiting the prognoses of the damage which specific security-oriented solution may cause in the legal and political system:

> In many cases, privacy issues never get balanced against conflicting interests, because courts, legislators, and others fail to recognize that privacy is implicated. People don't acknowledge certain problems, because those problems don't fit into a particular one-size-fits-all conception of privacy.

According to Solove, one of the reasons why this harmful lapse in impact estimation is possible, confusing our understanding of the trade-off between privacy and security, is that a more general concept of privacy is missing from the academic and public discourse – the problem which this dissertation is aimed at eliminating (*cf.* chapter 1).

An important consequence of the popularization of NtH was the conception of a narrative where seeking privacy is seen as implicating criminal intent or criminality. Although, similarly to NtH, the idea of privacy as criminality does not offer a legitimate

anti-privacy *argument*, it became a strong tendency in policy-making, to the extent that certain privacy-enhancing solutions are seen as criminal or cyber threats. Such was the case with the EU cyber security agenda and solutions such as the Tor network or end-to-end encryption.

4.2.4 The paradox of end-to-end encryption in Europe

Koomen (2021) observed that secure encryption[4], including end-to-end encryption (E2EE), has played a paradoxical role in the debate on data protection in Europe.

End-to-end encryption (E2EE) is a method used in digital and mobile communication, where only the communicating users are able to decipher the messages. Although various methods of E2EE offer different levels of protection, successful deciphering (known as eavesdropping) or modification of E2E-encrypted messages is considered effectively impossible from the probabilistic point of view. And so, in principle, E2EE prevents potential eavesdroppers from obtaining the decryption keys necessary to decipher the messages between communicating users. This includes malicious state and public bodies and service providers, such as Internet and communication services, and others.

Users protected by E2EE ensure that only the sender and the recipient may access and modify the information exchanged in the conversation. Because no third party can access the data, companies which provide E2EE cannot provide so called *backdoor* to the conversation, or hand over the messages of their users to the authorities. This fact was interpreted as an obstacle to law enforcement in the EU, and declarations to weaken or eliminate E2EE in Europe have been undertaken by cyber security institutions.

In July 2020, two related strategies were launched by the European Commission, an update of the EU's Security Union Strategy and a plan to combat child sexual abuse (Koomen, 2021). Parallel proposal of the two was not a coincidence. In both strategies, E2EE was framed as a method used by criminals, including child abuse perpetrators, to mask their identity. This way of presenting E2EE focuses on the perspective of the law enforcement, or public safety, alleging that the elimination of E2EE would be beneficial to public safety. This caused some of the central EU bodies to envision E2EE primarily as aiding criminal activity. For instance, thee European Commissioner for Home Affairs

[4]Encryption *sensu largo* is the process of encoding information by converting the original representation of the information, called *plaintext*, into an alternative form, called *ciphertext*, according to a given method. A *safe* encryption method is such that only authorized parties are able to decipher the ciphertext back to plaintext, thus being able to read the original message. If the message is intercepted by a third party, but the message was encrypted using a safe method, then, at least in principle, the interceptor should be unable to access the information in the original, meaningful format.

Ylva Johansson said that the *problem of encryption* requires developing a *technical solution*, implying that the EU law enforcement should be entitled to a backdoor to every digital or mobile conversation (Johansson, 2020).

However, two important aspects of E2EE are missing from the mainstream EU debate. One of them was mentioned by the Information Commissioner's Office (ICO), a UK-based watchdog authority. Namely, in the context of child-related criminality, E2EE not only protects the abusers from the law enforcement, but also protects children from the abusers. The ICO argued that the debate over E2EE in the UK and the EU was too unbalanced, causing a "misinformed opposition" to E2EE, which ultimately endangers children even further. According to the ICO, E2EE promotes online safety of children, while abusers can be identified using other methods, less damaging to public security and open society.

In 2022, the UK's Information Commissioner's Office – the government body responsible for enforcing online data standards – also stated that opposition to E2EE was misinformed and the debate dangerously unbalanced, with too little focus on benefits, since E2EE "helped keep children safe online" and law enforcement access to stored data on servers was "not the only way" to find abusers. The English campaign called "No Place to Hide" launched in 2022 cost over £500k, targeting the plan to introduce E2EE in Facebook from 2023 onwards. The campaign was met with opposition from the media and the public. For instance, Corfield said that the campaign intended to "make it easy for police workers and other public-sector snoopers to read the public's online conversations without having to get prior permission or defeat privacy protections" (Corfield, 2022).

Similarly, Stephen Bonner, the executive director for innovation and technology of the ICO, argued that E2EE helped keep children safe online by not allowing the abusers to send them harmful content or access their pictures or location. Moreover, Bonner said that "the discussion on end-to-end encryption use is too unbalanced to make a wise and informed choice. There is too much focus on the costs without also weighing up the significant benefits" (BBC, 2022).

Another important, yet often undervalued aspect of E2EE is that it is an essential component of open societies and markets and the statistics of use for privacy-oriented tools confirm that E2EE is overwhelmingly protecting legitimate, non-criminal activity. This fact is visible from the usage metrics of privacy-enhancing tools such as the Tor network, the leading anonymous communication tool launched in 2003.

The Tor network is used by millions of users every day to access thee internet with relative anonymity, meaning that, if used correctly, Tor can be used to conceal the activ-

ity on websites, but not their addresses, meaning that a third party can learn that the user is accessing a specific website, but not much more that this. In particular, the content of communications and messages, visiting specific sections of the site, *etc.*, are usually private. Because of the negative publicity which Tor was receiving, also because of the law enforcement campaigns such as the recent "No Place to Hide" in the UK, the creators of the network started developing methods to safely collect usage statistics about the network, that is, to establish who and how uses the network without endangering the privacy of the users (Kenneally and Dittrich, 2012).

One of the most comprehensive privacy-preserving measurement studies of the Tor network by (Mani et al., 2018, p. 188), confirmed the analysis of the Tor Foundation in that Tor is used predominantly for web browsing. Moreover, the users of Tor tend to visit the same websites as non-anonymous users, including platforms such as Facebook, Google, *etc.* However, the study suggested that the Tor Metrics Portal[5] is underestimating the number of unique Tor connections, that is, the number of people making regular use of the network. According to Mani *et al.*, the clients of the network were distributed over 200 countries and generated approximately 1.2 billion anonymous circuits every day during the measurement period in 2018.

The usage statistics show that Tor is often used as a way to protect one's activity on "regular" platforms, accessible also for non-Tor users. A crucial consequence of this fact is that the connection between Tor and illegal activities conducted using the darknet is less significant that initially thought. However, the connection between deep web searches, that is, accessing websites which are not indexed by Google and other popular search engines, and criminal activity became so ingrained in public perception of darknet and freenet tools that the very phrase "dark web" has become a synonym for criminal concealment in the popular discourse. Popular culture and misinformed media portrayals led the public to associate the dark web with the exchange of drugs, firearms, murder for hire, and child pornography, despite the fact that the overwhelming majority of such activities is likely conducted using non-dark web tools. Meanwhile, a good majority of criminal activity takes place outside of the "dark" part of the Internet. A good example would be the use of Facebook in Myanmar, where the military organized and incited the genocide of Rohingya *via* publicly available posts in 2016 and 2017 (Mozur, 2018).

[5]The Tor Metrics Portal is an analytical project launched by the Tor Foundation and supported by the National Science Foundation. Its aim is to safely collect, analyze, and provide visualizations of statistics from the public Tor network and from Tor Project infrastructure. url: https://metrics.torproject.org/ (Acceessed March 1, 2022.)

4.2.5 Framing the Other

Another aspect of political decision-making, where the impact of privacy on public security is downplayed, often consciously, by the public authorities, is migration. In this context, the migrants are often presented as a threat, either to the culturally-backed way of life in the "defending" country, or to its economy. Such was the case with non-white Muslim migrants in France described in section 2.1.2. This psychological effect, known as the siege mentality, is easily developed in public perception and contributes to an increase in anti-European and anti-Islamic sentiment, hostility towards migrants and rise in subjective perception of insecurity (Cox, 1990; Bar-Tal and Antebi, 1992; Šram, 2015).

In Samonek (2019), I argued that privacy violations in the process of controlling migration have negative impact on individual liberties of the citizens, as well as the rule of law and the accountability in public governance. In particular, I argued that the violations of privacy of foreigners and migrants are often justified as exceptions, alas within a never-ending "state of emergency", either formal or purely suggested, centered around various forms of exaggeration and misinformation in the public media. These "emergencies" are building blocks of the siege mentality, aimed at sustaining and growing hostility towards distinguished categories of the public. This process of *othering* encompasses not only the migrants, but also a number of internal "enemies", such as the climate protesters, political opposition, welfare beneficiaries and the unemployed, and many others. In such narratives, privacy protection is equated with an attempt to infiltrate or attack "the public", thus allowing for an overblown, inappropriate notion of interventions required for public security.

Aside from endangering specific targeted groups of people, the process of othering contributes to the destruction of social solidarity needed to oppose the state authority. This allows the government to gradually win control over the governed population (Bauman and Lyon, 2013). As I wrote in my 2019 paper, by pointing to the common enemy of the nation, the governments are able to single out any individual as a potential threat and neutralize their political or economic influence. The mechanism of social division supports this process by providing new features which serve as foundations for evaluating a given individual as a threat to the security, the traditions or customs, the national heritage or the financial well-being of the state. Such features include in particular gender, sexual orientation, foreign origin or ethnicity, living in poverty, *etc.*

One such system was the Polish governmental program called *Empatia*, an assistance tool aimed at the unemployed citizens seeking social support. Niklas et al. (2015)

argued that *Empatia* was in fact used as a profiling tool, aimed at raising the statistics of welfare institutions' effectiveness, and not at helping the individuals seeking assistance and benefits from these institutions. And as I pointed out in my 2019 paper, the declared purpose of the assistance tool was to assess the chances of a person registered in the labor office at the job market and customize the office's assistance to fit their individual needs. Each person among the registered unemployed was categorized as either an A, a B or a C, depending on the total points for the answers in a questionnaire given to them at the moment of registration. The first category included those who were likely to find a new position without the assistance of a labor office but used it to browse through the recent post openings. B-category included people who were employable, but less likely to find a job offer on current listings of open post available to a labor office. The third category, C, included those deemed "permanently away from the job market", the unemployable.

Falling into the third category proved relatively easy for most applicants, as it was not at all based on the criteria of availability, skill, education or qualification. For example, a woman over 30 with an ill person under her care would qualify as a C. The labor office would not use its resources to help a person who was a C but would rather direct all efforts towards those who are easier to help, mostly those in A-category. Such procedure was indeed very effective from the statistical standpoint, but failed to help those whose well-being lay in the heart of social services, that is those who cannot deal with a problem without assistance. An argument for following up on the categorization and cutting off those in categories of B and C from certain (or sometimes even all) opportunities available to the A-rated was similar to other emergency-based arguments. After all, people with lower chances of finding a stable working position may be seem as a "threat" to national budget. The process of imposing limitations on social service in this case is similar to the process of restricting rights of the foreigners. Based on a premise that a given characteristic turns individuals into a designated threat to the national agenda, they are denied access either to the territory, or to a service which otherwise would be obtainable without restrictions.

Using surveillance as a means of population control has long historical roots. In fact, the origin of census can be traced to the Babylonians in 3800 b.c.e., when the number of inhabitants in each household was recorded together with information on the goods available to them – the quantities of butter, honey, milk, wool and edible vegetables. Even in modern times, census was used in a similar vein. For instance, Aly et al. (2004) showed how the census was used by the Nazi government in 1939 to identify citizens who were either Jewish or so called "Jewish half-breeds", that is, person of Jewish and

non-Jewish origin, recording the information of religion and descent of all parents and grandparents. The information was immediately passed on to the police and allowed for more targeted discriminatory practices and later, a more effective genocide (see section 5.2.3).

Even in contemporary EU most member states require foreign residents to register with the local authority for long-period stays. For instance, foreigners in Belgium are obliged to register with the Aliens Registration Department of the local council within 8 days from the day when they obtain an address. The process of registration requires the following:

- a personal visit to the Aliens Registration Department, submitting all personal information, including marriage certificate, diplomas, addresses in the home country and in Belgium, ID and passport copies, proofs for sources if income and similar documents for all family members;
- a non-scheduled visit of the police officer, who will inspect the house or apartment of the foreigner, take note of the living arrangements and contracts; this step requires that the foreigner is present at the address indicated at the time of the non-scheduled visit, which effectively requires taking time off work, as the visits usually happen during working hours; the police can visit and inspect any room and place in the house and ask for further documents and explanations;
- another personal visit to the Aliens Registration Department, submitting certificate from the employer, medical and birth certificates for the foreigner and their family members, and, in some cases, the certificate of good conduct pertaining to the prior five years issued by the national police of the former country or countries of residence.[6]

Countries which the European standards for freedom of movement do not obtain, often employ more comprehensive methods for surveillance of foreigners' flow and activity. For instance, in China the registration at the local police station closest to their accommodation is mandatory for any foreigner, including tourists, within 24 hours of arrival in the country (Smith, 2020).

Aside from institutional factors for privacy loss, both the foreigners and native residents of countries all over the world are impacted by the factors related to culture, meaning either the local culture relative to their local community and tradition, or culture shaped by the global forces of capital and political power. In the subsequent section,

[6]Information from the official website of Office des Etrangers, url: https://dofi.ibz.be/fr (Accessed February 20, 2022).

I analyze some of the most prevalent cultural aspects of oversight and privacy, and give examples illustrating each of them.

4.3 Cultural aspects of privacy and oversight

Lyon (2018, p. 4) observed that a form of *surveillance culture* has already rooted itself in most modern societies, making certain practices of surveillance capital, the state and the society a part of our everyday, accepted reality. McGrath (2004) argued that in certain areas of culture, such as art, performance, and popular culture (one could easily add other areas of social life to this list, such as marketing and personal brand development), individuals often have much to gain from oversight. This point, however, requires that we focus on oversight in the sense of personal privacy, that is, a relationship between an individual and the society, and not political privacy, which guards individuals and groups against the state. Because of this fact, a number of phenomena which contribute to surveillance culture are not relevant to political privacy. Rather, they concern personal conditions which individuals would like to see met in the process of their participation in social life. Although these elements of surveillance culture impact, among others, psychological attitudes and personal comfort of individuals, as well as their subjective feeling of inclusion in social and political life, they do not concern the vehicles of democratization and political empowerment in a direct or easily measurable way. Hence, in this section I focus only on those element of culture which concern privacy and surveillance, and which are immediately relevant to political privacy.

First, I will briefly describe the rise of *sousveillance* and reverse surveillance, where the objects of state or corporate surveillance conduct oversight of their watchman or themselves. I will discuss the efficiency of sousveillance, its use by the police and preventative recording (or *alibi sousveillance*), and specific principles of emerging sousveillance cultures. I will show that what McGrath referred to in 2004 as "surveillance" has later been conceptualized as sousveillance. Next, I will talk about surveillance spaces, that is, physical spaces where the environment and processes have been designed with privacy loss in mind. I will give examples of public spaces, where transparency and surveillance are indicative of the lack of public trust. Separately, I will present examples of surveillance spaces and practices used by mass employers, starting from the shoe factory and employee facilities owned by The Bata Company, a shoe-making firm founded in 1894 in the Czech part of Austro-Hungary and run by Tomáš Baťa up to the beginning of WWII. This early attempt of employee surveillance informed contemporary workplace surveillance, including electronic surveillance of employee's activity in their

homes during so called "home office", a period between 2020 and 2022 when many companies transitioned towards labor outside of their headquarters due to the Covid-19 pandemic.

4.3.1 Sousveillance

Fernback (2013) argues that sousveillance, understood as close observation, recording and scrutiny of the institution conducting surveillance, is the result of resistance to surveillance environments created by surveillance capitalists, such as Facebook or Google, and the state. Another perspective on sousveillance is to see it as a process where, while participating in the activity, individuals record and document their participation using small wearable or portable personal technologies. Huey et al. (2006, p. 150) claim that the term "sousveillance" is due to Steve Mann, who used it in 2004 to refer to "the use of surveillance technologies and tactics by the lower classes for the purposes of increasing equality through making public the hidden workings of powerful institutions and groups". Later on, the term was used to describe analogous use of technology to monitor the activity of the law enforcement, public institutions, *etc.* In their paper, Huey, Walby and Doyle describe the US-based initiative called Cop Watch, aimed at promoting democratic accountability of a state institutions, especially in their relation to marginalized citizens. Cop Watch, similarly to other community-driven sousveillance initiatives, allowed the citizens to actively engage in the politics of surveillance though resisting institutional forms of power through their own surveillance activities.

However, sousveillance does not equal counter-surveillance. Mann et al. (2015) famously argued that "surveillance is a half-truth without sousveillance", thus sousveillance may be used together with surveillance to create a more comprehensive mode of observation. Thus, citizen engaging in sousveillance are unable to reciprocate surveillance perfectly, because the information they collect may also be used by the watchman to boost the impact of surveillance.

Sousveillance *sensu largo* involves citizens' recording, thus observing the events from the first person perspective, but no specific political or social agenda is necessary. Inverse surveillance is a form of sousveillance aimed either as a couter-surveillance measure or a form of opposition against surveillance or its supporters. For instance, citizens participating in a protest or a rally may conduct sousveillance of the law enforcement during the event. Inverse sousveillance may focus on surveillance systems, proponents and enacters of surveillance, or authority figures and organizations.

Mann, Nolan and Berman track the origin of scientific interest in sousveillance to

the social conflict surrounding personal monitoring technologies such as the Eye Tap, eyeglasses with an integrated electric seeing aid. Institutions and business owners who routinely perform surveillance of their customers and visitors strongly objected to people who used Eye Tap system, based on the claim that the technology subjects them to inverse surveillance. Moreover, a number of experiments revealed that the greater the appearance that the sousveiller has personal control over the device, the less acceptable the act of sousveillance becomes (Mann et al., 2003, p. 341). In other words, those who conduct surveillance tend to oppose sousveillance in the form of inverse surveillance, especially when the person involved in it displays any degree of agency or control over the process.

Sousveillance of a state by its citizens has been successfully used to address social and political problems such as election fraud, for example, in Ghanaian general elections in 2008 (Pryce, 2008; Tettey, 2017). Inverse surveillance and personal sousveillance were also used as a means of *alibi sousveillance*, that is, self-monitoring and recording aimed at generating an alibi as evidence to defend against allegations of wrongdoing. Thompson (2007) documented the case of Hasan Elahi, an academic who was placed on the US terrorist watch list without probable cause or justification. Elahi was affiliated with the University of Maryland and was detained in 2002 when traveling from the Netherlands to Detroit. The FBI suspected Elahi of collecting explosive materials in a storage unit in Florida, but the allegation turned out to be false. As an academic, Elahi was subject to suspicion due to his frequent travels, including approximately 100.000 kilometers (or 70.000 miles) each year to conferences and art-related events. Thus, expecting the escalation in preventative measures on the side of the US government, he decided to maintain full transparency towards the FBI, as well as the general public. Since 2002, Elahi notifies the FBI agents about each trip by phone. He also uses his cell phone as a tracking device and documents his movements and transactions by publicly posting debit card logs and other transactions.

Alibi sousveillance is also being used by the law enforcement, especially the police, to maintain a record of the interactions of the officer with civilians and criminals. In a series of experiments, Mohler et al. (2022) show that videos of police-citizen interactions on social media impact public perceptions of legitimacy and procedural justice. The study suggests that online videos of police-citizen interactions contribute substantially to increasing distrust in the police when they document negative interactions. However, policing agencies may use the same form of documentation to improve the civilians' perceptions of legitimacy and procedural justice. Thus, sousveillance can also be used to the advantage of the law enforcement agencies both through increasing the account-

ability of the officers *via* monitoring and recording of their activity, and improving the public image of the agencies when the positive interactions are recorded and made publicly available.

Browne (2015) argues that sousveillance cultures, though not associated with the term *sousveillance* have a long history in American emancipation movements, including Black citizens' emancipatory struggle. She links contemporary surveillance technologies and practices to the ideologies rooted in race theories and the resulting tendency to police and control the bodies of Black Americans. Browne also showed that the adaption of various technologies to increase the chances of escape or survival could be seen as a form of sousveillance, which she calls "dark sousveillance".

4.3.2 Surveillance spaces

One of the first surveillance spaces, and arguably the most famous architectural design prioritising surveillance, is Jeremy Bentham's project of the Panopticon prison (from Greek *panoptes*, or all-seeing). Bentham developed the Panopticon in letters while visting his brother, Samuel Bentham, in Krichev in Eastern Europe in 1785 and 1786 (Burns and Sprigge, 2017). The inspiration for the prison design was based on the ideas on the observation of workers conducted by Samuel. Jennings (2012, Chapter 91 "Panopticon 1791–92") gives the following description of the Panopticon based on the original characterization by Bentham (1791):

> The Building circular – an iron cage, glazed – a glass lantern about the size of Ranelagh – The Prisoners in their Cells, occupying the Circumference – The Officers, the Centre. By Blinds, and other contrivances, the Inspectors concealed from the observation of the Prisoners: hence the sentiment of a sort of invisible omnipresence. – The whole circuit reviewable with little, or, if necessary, without any, change of place.

The Panopticon would be associated with the system of multi-level control, where the prisoners would be surveilled by the gaoler or a manager, and the highest prison authority would be accountable to the general public and external public officials. The design of the Panopticon was soon applied in England. The construction of the National Penitentiary in Millbank was initiated in 1812 and was finished in 1821.

The National Penitentiary in Millbank was a response of the British government to the persistent problems of the prison system in London, especially the Newgate Prison. The idea behind the prison surveillance was that the prisoners knew they can be observed, but did not know when they were watched. Hence, they would need to behave

as if under observation at all times, prompting them to follow required script of behavior. Bantham thought that the Panopticon design should be used not only in prisons, but also in schools, hospitals, asylums, and, most importantly, factories. The Millbank prison was expected to be the first institution to effectively use the Panopticon system to *extract labor out of prisoners*. The Millbank project failed at bringing wealth to the British government, and soon stirred controversy due to, among others, the fact that it caused mental illness among prisoners (Kelly, 2017, Chapter 8). Despite its failure, the Panopticon design was reused and reapplied in many prisons in England and around the world, including the K-wing near Lancaster Castle prison, a semi-rotunda with a central tower for the supervisor, and the Pentonville prison in London (Simon, 2016, p. 43).

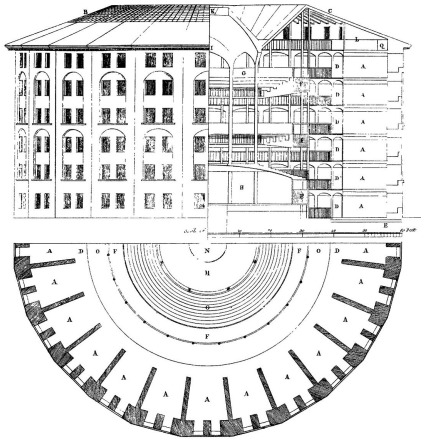


Figure 4.1: Plan of Jeremy Bentham's panopticon prison, drawn by Willey Reveley in 1791 (1843, originally 1791). Source: The works of Jeremy Bentham vol. IV, 172-3.

The Panopticon design was also used in Cuba, where between 1926 and 1931 the national government built four prisons, which were connected to a massive central structure through a system of tunnels. The structure of interconnected prisons was called *Presidio Modelo* ("A model prison") and built on Isla de Pinos (today called Isla de la Juventud). The central part of the design was to serve as community center, while each of the four prisons had 93 cells separated into 5 floors. Cells had no doors, as per Bentham's original project, and the inmates could in principle walk freely around the facility and spend their time learning trade or reading. However, the project soon became unmanageable due to overcrowding and the humanitarian conditions in the facility declined significantly. By 1953, the four panoptical circulars were home to ca six thousand prisoners (Wallace and Melton, 2008, p. 259).

A collection of studies edited by Newell et al. (2018) presents a variety of perspectives on how surveillance is solidified in public spaces and, in turn, what changes public spaces are undergoing as a results of surveillance. Shoemaker and Schmidt argue that the trends in designing spaces used for higher education essentially led to the creation of "ivory surveillance towers", the effect of which contradicts the intention behind universities as they evolved in the twentieth century. Moreover, they claim that "the panoptic power of the institution and neoliberal paradigms of accountability are generating changes in access and behaviors within this sphere[higher education – AS], and that these changes echo longer historical traditions of control on campuses" (Newell et al., 2018, p. 34). Newell, de Conda and Thomasen analyzed surveillance of public spaces in North America, including Canada, the US and Mexico. They concluded that despite differences in legal regulations of privacy in public spaces in the three countries, the regulatory trends behind them display a level of similarity. First, little to no protection is offered to aid the privacy for activities and information that are (sometimes by necessity) either exposed to public view or performed in publicly accessible space. The tests of expectation of privacy in all three cases are formulated in such a way as to eliminate privacy of activity in all spaces other than those which are explicitly designated as controlled by the individual. In Canada and the US, the courts tend to waive the expectation of privacy in public spaces of individuals (and most private actors, *e.g.* corporate) against the interest of public authority. In Mexico, protections of privacy in public spaces are upheld largely nominally (Newell et al., 2018, p. 237). Boanada-Fuchs presented similar findings with regards to the evolution of public spaces in São Paulo. He observed that the ongoing hybridization of public space is indicative of the need to combine the public feeling of shared urban space with the need to maintain privacy of certain activities and relationships. The influence of the US on the development of public spaces in South America resulted in assigning new forms of "centrality" to work and leisure spaces such as shopping centers, business parks and entertainment centers. This new notion of centrality was in fact suburban, that is, it allowed an escape from the perceived periphery without the need to travel towards metropolitan spaces. Leisure and work became more central once performed in spaces which were open, more communal, and more public, as opposed to the private and family life which was mostly enacted within the tight spaces of enclosed districts and walled gardens (Newell et al., 2018, p. 54).

Klauser (2016, pp. 78-79) shows that surveillance in public spaces has generally retained its tendency to create spherical shapes, which Bentham proposed for his Panopticon prison back in the 1780s. Intentional use of transparency and separatedness in

urban planning often signals authority and control, which are also indicative of lack of trust of public authority towards its own citizens.

4.3.3 Employment surveillance

Given the time of its emergence, one of the most developed systems of control used in the workplace was designed for the Bata Shoes factory in the 1930s. The headquarters of the company in Zlín (in today's Czech Republic) was known as Building No. 21, or Baťa's Skyscraper, and was one of the first high-rise buildings to be constructed in Europe. Building No. 21 was built in 1936-1938 incorporating the ideas of Jan Antonín Baťa, who followed Tomáš Baťa as the company president. Within the building, the mobile office of the president was a technical rarity at the global scale. Installed in an elevator, the office moved at the approximate speed of 0.75 meters per second, which would allow the president to have oversight over the operations of offices on all floors in Building No. 21.

Although Baťa never got to actually use the office, as its construction was completed after Baťa's exile during WWII, its potential for monitoring and using oversight as motivation technique for his workers at all levels in the firm is representative of the philosophy of Baťa on how surveillance conditions effectiveness.

The Baťa family took inspiration from Henry Ford in designing their own conveyor belt production lines. Relying on the assumption that an average worker is not intelligent and self-sufficient enough to be trusted with responsible and timely production, the production lines in both Ford's and Baťas' factories split the manufacturing process into simplest tasks, which could be completed by anyone, without prior training and work experience (Burita and Chvátal, 2016, p. 186). Baťa's conveyor belt also relied on collective oversight and the practice of shaming the slow workers into better work efficiency:

> The father sets up new production lines so that "each human unit is automatically driven to the greatest productivity." If any single worker cannot keep pace in the production line, the conveyor belt stops and a red bulb lights up on the wall. Thanks to this signaling system, the entire unit can see not only that they must stop work, but also who is to blame. (Szczygieł, 2014, chapt. 1)

Similar psychological techniques, initiated by Tomáš Baťa and continued by his brother, were aimed at changing the behavioral and emotional patterns of their workers. Tomáš Baťa famously said: "In my work I do not only think about building factories, but people. What I do involves building the human being" (Szczygieł, 2014, chapt.

1). Aside from using specific architectural designs in the workplace, Bat'a engaged the pro-surveillance designs and practices in worker's homes and leisure facilities in the industrial garden city of Zlín, a worker town which housed *ca* 45,000 inhabitants. When the production moved overseas, to UK, Manila, and other countries, the blueprint of the Zlín garden city was recycled. Burrows interviewed some of the people who remember living in the Bat'a worker town in Essex:

> Some elements of the Bata way might seem intrusive by today's standards. "People knew if their garden was overgrown they would be pulled into the office and asked politely to sort it out," says former employee Graham Sutcliffe. "It made them respect the town a bit more." (Burrows, 2016)

The Zlín practices of controlling and managing the private affairs of the factory employees for the sake of their loyalty to the company extended far beyond home and garden maintenance:

> The social department has its spies who inform on lovers. As soon as they notice a new relationship, they report the couple. The company recommends that they get married and have children. The manager of the personnel department, Dr. Gerbec, says: "Children are the leashes we hold their daddies by." (Szczygieł, 2014, chapt. 1)

In commissioning the design of the homes for his factory workers, which were known as *batovky*, Jan Antonín Bat'a subscribed to a view that a family-oriented house separated from other workers and their families will encourage productivity and draw the attention of the worker away from thing such as labor unions and debating worker's rights.

> At the same time it is thought that a worker who is deprived of communal accommodation, such as barracks shared with other families, will turn his back on collective demands and syndicalism. (Szczygieł, 2014, chapt. 1)

However, the houses also discouraged workers from spending time inside the family unit. Jiřina Pokorná, wife of one of the workers, mentioned that the size of the batovky kitchens and their purposefully dysfunctional layout was aimed at making sure that "life didn't happen at home" (*ibidem*). Instead, workers were encouraged to spend their free time in factory-controlled areas, often "catching up" on delayed work, effectively providing the company with unpaid labor. The houses were built with purposefully thin walls and long, unwelcoming spaces, to move conversations and leisure outside, where

they can be observed and, if needed, relayed to the company by designated social monitors.

In a study conducted between 2017 and 2019 in a large (up to 3000 workers) Amazon fulfillment center located in Italy, Delfanti (2021, p. 40) shows that the practices and methods of control started in pre-war Zlín have been developed further, including the reconceptualization of labor in 1960s Italy, called *operaismo* (workerism). These new ways to embed labor in capitalist business models, as well as digital forms of surveillance and data extraction help contemporary business giants such as Amazon structure labor in a way that pushes the workers to collaborate with data collection. Ajunwa et al. (2017, p. 742) give account of the development of workers' surveillance in the US and argue that the erosion of limitations of surveillance has quickened in the recent decades. Companies such as UPS and Amazon use algorithms and tracking to monitor their workers behavior up to a fraction of a second and have adjusted their process to the optimal, though often unattainable ideal route of movement. One of the most controversial practices of boosting productivity at the cost of basic needs of the workers in the recent years has been the monitoring of time spent in the toilet during work hours and the invention of a tilted, pain-inducing toilet bowl for workplace use (Olen, 2019). Delfanti (2021, p. 520) argued that the efficiency-oriented processes, as well as the "datafication" and capture of workers' knowledge, are used to strictly control the labor process for maximum profit.

So far, little to no legal protections are available at the state-level to either the US workers or the workers elsewhere. In the EU, the challenge to protect the workers' rights from workplace surveillance have yet to be comprehensively addressed. Todolí-Signes (2021, p. 65) argued that under current legal framework of protections, employees undergoing publicly accessible performance evaluations are subject to even more intense and wider degree of monitoring than traditional workers. When worker protections do exist, they tend to center around limitations on the control of *data*, such as e-mail and computer use monitoring (Rustad and Paulsson, 2004).

4.4 Political privacy and public security

One of the most pressing themes in the debate on privacy is its relationship with public and national security. In the remainder of this chapter, I will focus on addressing three problems which contribute to our understanding of the trade-off between privacy and security. First, in section 4.4.1, I will discuss how evoking public fear conditions the acceptance of privacy violations in the name of security or safety. In section 4.4.2, I

address the question whether mass surveillance prevents terrorism or helps minimize it. Finally, in section 4.4.3, I argue that political privacy is in fact necessary for national and public security.

4.4.1 The psychology of fear and surveillance

Gold and Revill (2003) conducted a study of how surveillance impacts the urban landscape, analyzing security measures applied by the local authorities in suburban areas, such as Ealing Broadway in West London. They drew attention to two aspects of the emergent "landscape of fear", by which they understand an area changed by the growing perception of danger. First, the propensity to accept and even require increased security measures in a given area depends on the subjective level of fear, often related either to an event like a terrorist attack, as well as on the increase in measures in other areas. In other words, the public tends to expect that the measures applied in their neighborhood will be no less than what they see elsewhere. This tendency to level-up security measures as a response to public pressure will be also relevant to the discussion of cost-effectiveness of airport security, which I will present further below. The second aspect of the "landscape of fear", which Gold and Revill describe is that often the primary function of security measures such as steel posts embedded in the pavement, the anti-climb paint on the gates of schools, or the CCTV cameras in exposed places is to alleviate fear even when these measures do not contribute much to actual increase in security. Steel posts may indeed deter ram raiders, but first and foremost, they signal to the people walking on the pavement that the area is protected against cars. However, note that a steel post does not *stop* the ram rider, but merely adds some damage their vehicle. As for the deterrence, it is at best debatable whether an attacker attempting to ram into the crowd or detonate a bomb will be successfully discouraged by a CCTV camera or a steel post in the pavement. Gold and Revill argue that such measures in urban areas had "as much to do with perceived security as real threat" (Gold and Revill, 2003, p. 27).

In certain cases, one may argue that, in comparison to actual risks involved, the perceived security dominates the considerations. Airport security is a good example, which Stewart and Mueller (2014) analyzed as far back as 2014, using risk and cost-benefit methods to evaluate the cost-effectiveness of counter-terrorism security measures at airports. They compared data from the Global Terrorism Database for the period 1998-2011 and found that 20 attacks on airports in the US and Europe killed the total of 64 people. In the same period, 31 successful attacks on aircraft were conducted despite airport security measures. Combined attacks on aviation, including airports, aircraft

and others, accounted for less than 0.5 percent of all terrorist attacks. Overall, threats to aviation infrastructure were rather low compared to non-aviation areas. Fatality risks from terrorist attacks to airports are 100–1000 times less than acceptable risks elsewhere, which means that the threat is extremely low, and not due to the security check either.

> Although there may be special reasons to protect airplanes, however, it is not at all clear that there are any special reasons to protect airports. Elias (2009) states that these areas have "unique vulnerabilities because it is unsecured". However, compared with many other places of congregation, people are more dispersed in airports,and therefore a terrorist attack is likely to kill far fewer than if, for example, a crowded stadium is targeted. (Stewart and Mueller, 2014, p. 19)

Hence, Stewart and Mueller argue that the probability of an attack would have to be much higher than the observed rates of attack to justify protective measures. In fact, they identified the most cost-effective measure as adding curbside blast deflection and shatterproof glass to airport infrastructure (Stewart and Mueller, 2014, p. 27). Despite these findings, no significant change in airport security measures has occurred since 2014. One explanation for this is that the security check offers a form of a spectacle, to use the terms of Gold and Revill, a way to curb the irrational emotional responses of the passengers who may still view airports as relatively unsafe, despite ample statistical evidence to the contrary.

Of course, the aforementioned observations concerning the psychology of fear in relation to surveillance do not exhaust the range of factors which contribute to acceptance and adoption of advanced security measures. Living in militarized societies, areas of social or military conflict, experiencing changes in the everyday environment, including one's financial and social situation, all impact one's views on surveillance, often in ways which do not relate to privacy directly, but rather treat privacy as a luxury among the basic psychological needs in a situation where even more basic ones are difficult to meet. Shalhūb-Kīfūrkiyān (2015) conducted a case study of Israeli-Palestinian relations in the context of settler colonialist policies, where security and surveillance have a distinctly anti-Palestinian character. The politics of fear of the Palestinians gives rise to a kind of "security theology", a mindset promoted by the Zionist politicians whereupon historical facts and justice-based arguments are overridden by the notion of "sacredness" of the colonial elimination of the perceived enemy. The issue of criminality of the forced displacement, dispossession and massacres of the Palestinian population is re-framed as necessary sacrifice, which the Zionist need to make for the sake of "sacred" security, supporting the quest of colonial erasure of racial "opponent" (Shalhūb-Kīfūrkiyān,

2015, p. 16). In cases involving security and surveillance such as this one, it could be more productive to speak not of the *psychology* of fear and surveillance, but of fear and surveillance *culture*, given how advanced security-based thinking is among the general population and political leaders. Such cases, if described with appropriate depth and detail, would provide sufficient research material for a number of dissertations, and thus are left outside the scope of the present work.

4.4.2 Mass surveillance, counter-terrorism and state surveillance

Knowing that certain popular security measures, such as airport security checks, are not cost-effective in preventing the terrorist attacks on airport infrastructure, the next question in the context of privacy, and especially political privacy, is – but what about mass surveillance? Does mass surveillance contribute to increased security? Does it prevent or alleviate the fallout of terrorist attacks?

Houston (2017, p. 3), following a definition used by Privacy International, defined mass surveillance as "the subjection of a population or significant component of a group to indiscriminate monitoring", also noting that "any system that generates and collects data on individuals without attempting to limit the dataset to well-defined targeted individuals is a form of mass surveillance." Houston analyzed the effectiveness of PRISM, an American mass surveillance program initiated after the 9/11 attacks in stopping terrorist attacks in the US. The results show that mass surveillance is overwhelmingly ineffective in preventing acts of terrorism. While traditional surveillance methods, in use prior to 9/11, succeed in roughly 70 percent of cases, mass surveillance tools allow for success rate up to 20 percent. This disparity in success rate persisted despite significant intelligence community resources being redirected towards PRISM, the operating costs of which is roughly $100M USA annually. Without this diversion in funding, it is likely that traditional surveillance method would allow for an even higher success rate. Houston argued that both the funds and the technology developed for the purposes of mass surveillance must be put to a different use – that the resources used up by programs such as PRISM must be directed back to traditional surveillance methods that are proven to work; and that the technology used in mass surveillance programs should be used only in a restructured role, as aid to traditional surveillance, for instance for collecting data only from designated areas of the Internet, such as extremist chat rooms and knowledge bases.

Maras (2010) approached mass surveillance from another angle, asking whether measures such as biometric IDs, licenses and passports, PNR (Passenger Name Record)

data transfers, Secure Flight program, and US-VISIT program make it harder for terrorists to insert operatives in the US territory. Maras' results show that mass surveillance measures do not prevent the terrorists from entering the US, and also that their entry is by far not the major security issue, as most terrorist are home-grown, or domestic, and no type of border control can prevent a terrorist who is already in the US. Maras argued that "it makes little sense to use mass surveillance measures against terrorists – especially home-grown terrorists" (Maras, 2010, p. 35). Among the successful counter-terrorist measures used in the US, Maras mentioned pre-9/11 methods, which Houston referred to as traditional, such as using undercover agents, informants, and agent provocateurs.

At the start of the mass surveillance programs in the US following the 9/11 and the beginning of the "war on terror", the efficacy of mass surveillance was not known. From the perspective of over 20 years of US government spending and usage of these programs and associated methods, however, it is clear that, whatever function mass surveillance plays in the US national system, it is *not* a counter-terrorist measure. For one, it is because other, traditional surveillance methods are far more effective in preventing acts of terrorism. Another aspect revealing the inadequacy of the mass surveillance programs is that they are often designed against those who try to enter the US territory, despite most terrorism beging home-grown as Maras pointed out, or against foreigners or ethnic, or religious outsiders in general, for instance, in case of France described in section 2.1.2. The latter strategy goes in parallel to a myth-building strive of the national governments, desribed in detail by Lubin (2017, p. 502), to signal to their citizens that "the governments only spy on foreigners".

4.4.3 Political privacy is necessary for internal and external security

Mass surveillance, aside from being demonstrably ineffective in combating terrorism, has another, perhaps more dangerous, drawback. The risk here stems primarily from the fact that the attacks relying on mass collection of data rarely are seen in connection to mass surveillance tools and technologies, despite a strong link between them. I would like to point out two elements, which add to the spectrum of political threats related to mass surveillance.

First is the idea that government usage of mass collected data is ineffective, as shown in section 4.4.2, thus increases the overall risk to the society, compared to a situation when traditional surveillance methods are used exclusively. The very creation of government databases and access points to mass collections of citizen's poses additional

risk of exploitation by hostile third parties, a risk that is unnecessary given the low efficacy of mass surveillance. As I argued in my 2020 paper about the potential for joint European cyber security programs, preventative measures are the only effective way to deal with cyber threats.

Based on my paper, I propose to differentiate between a cyber threat and a cyber attack in order to explain their relative relevance to national cyber security and cyber defense strategies. A cyber threat is understood as the possibility of a malicious attempt to damage or disrupt a computer network or system, or the possibility to access files and infiltrate or steal data, even in the absence of an attempt of damage or disruption. That is, the very possibility to put the network of a system in jeopardy constitutes a cyber threat. The latter may potentially put the entire system of institutions relying on a secure channel of communication or database out of operation, simply by making the communication or data unreliable.

An important aspect of the proposed definition is that it identifies a cyber threat as a *possibility* as opposed to an *actual* attack. An attack is merely one instance of a particular cyber threat, taking form of concrete actions against the security of information or the integrity of a network or a system. Cyber *attacks*, as opposed to cyber *threats*, are often of second-rate importance to high-level defense policies, because there are not many known techniques available to deal with cyber attacks, other than through prevention. In most scenarios knowledge about the attack is only gathered *ex post*. Thus, most types of cyber attacks cannot be stopped or mitigated. The overwhelming impact of such attacks is visible in incidents like the Panama Papers case from 2016, where a simple unpatched software vulnerability was exploited, or the Proton Mail Ransom case, where powerful distributed denial-of-service (DDoS) attacks were conducted, using resources available to very few actors, such as nation states or global business giants. Once the possibility of an attack emerges and the door to exploitation of some vulnerability is forced open, there is close to nothing that a state or a federation of agencies can do to avoid the consequences (Samonek, 2020, pp. 45-46). Hence, the focus of the national or supranational cyber defence plan must always fall on prevention. Avoiding the mass collection of data is by far one of the most fool-proof preventative strategies that a government can use. After all, the data base that is had never been built, cannot the stolen, broken into or otherwise exploited.

The second point is that mass collection of data such as performed, *e.g.*, in PRISM is not direct. Instead, it relies on private firms, such as Microsoft, Yahoo, or Meta (Facebook), to collect and often pre-process data. The vulnerability here was imminent from the beginning of post-9/11 surveillance programs, in that private companies were never

operating in secrecy comparable to that of government agencies. Two immediate threats arise here. First, that the very fact of data collection taking place in the services of these companies was public knowledge. Second, the existence of surveillance-based technologies such as centralized social network or email trawling algorithms created what I call *mass entry points* to users' informational space. Hostile parties no longer even need to bother performing resource-costly cyber attacks on government databases. They can target the citizens *en masse* through the mass channels of communication made available to anyone who pays the service fee. The fact that the national government accept the existence of such mass points of access and centralized mass channels of communication is in itself a threat to national security, as was demonstrated during the US presidential election of 2016 (Madrigal, 2017; Pybus, 2019). Acceptance of centralized private services on the side of national governments is even more surprising given that safer alternatives, such as decentralized social networks (fediverses), are already in operation. Moreover, end-to-end encryption guarantees safe communication among the members of the government and citizens alike, providing a safe way out of services such as Google Mail. In chapter 5, I will elaborate on the notion of decentralized digital services and discuss their potential for securing political privacy.

4.5 Summary

In this chapter I analyzed the relationship between privacy, and especially political privacy, and the emergence of surveillance capitalism – a new type of economic power, which Zuboff (2019) called instrumentarian power. I briefly summarized Zuboff's own findings concerning the origins of surveillance capital in section 4.1. I also pointed out some of the psychological aspects of the discourse about privacy and surveillance. In sections 4.2.1 and 4.2.2, I described psychological incentives for passive acceptance of data collection practices. In section 4.2.3, I indicated that human behavior changes under observation – and that this fact contributed to the narrative behind the "Nothing to hide" slogan, whereupon seeking privacy is equated with criminal intent or criminality.

Assumed criminality played a significant role on the European debate on E2EE, which I presented in section 4.2.4. It also impacted the situation of targeted social and political groups, who suffered additional surveillance measures employed in the process of systematic othering (section 4.2.5).

Next, in section 4.3, I focused on certain cultural elements of surveillance, including the emergence of sousveillance, or undersight, where the citizens are observing the actions of their authorities (section 4.3.1), the design and philosophy behind surveillance

spaces (section 4.3.2), and early forms of employment surveillance (section 4.3.3).

Finally, in section 4.4, I discussed those aspects of mass surveillance and public security, which are most relevant to political privacy. I argued that there exists a connection between the public need to alleviate fear and the pressure to introduce certain surveillance measures even when they do not result in increased security (section 4.4.1). Using studies of efficacy of particular mass surveillance and security programs, I showed that mass surveillance is not an effective way to fight terrorism. Moveover, in section 4.4.3, I argued that political privacy should be considered a value protected by the public or national security programs.

Chapter 5

Political privacy and democracy

In this chapter I bring together the observations made throughout this dissertation to shed more light on the relationship between political privacy and democracy. First, in section 5.1.1, I clarify certain fundamental concepts, including the core components of democracy which I take into consideration, and how they align with the zones of political activity which I used to define political privacy in chapter 1. Then I discuss in more detail certain areas of democractic governance, including the freedom of speech and freedom of media (section 5.1.2), the electoral freedom (section 5.1.3), and the freedom of assembly and the right to protest (section 5.1.4). In section 5.2, I focus on limits to surveillance necessary within nation-states and federations aspiring to democratic governance, as well as globally, for the sake of peace and sustainable political development. I point out some pressing problems related to political privacy in the context of international politics, such as the habitual use of surveillance as an aid in committing genocide. Finally, in section 5.3, I make concrete policy recommendations concerning the future development of privacy laws and practices within the EU.

5.1 Democratic institutions protected by political privacy

In section 1.4 I have proposed the following characterization of the three thresholds of political privacy protection. First, a person, group or a collective has (or maintains) critical political privacy when they can authorize or deny access to the critical zones of political activity, that is those zones of political activity which are necessary for their minimum active involvement in the political system of a given country. Next, a person, group or a collective has (or maintains) baseline political privacy when they can authorize or deny access to the basic zones of political activity, that is those zones of

political activity which are necessary for and which sustain their active involvement in the political system of a given country, with possible exceptions. Finally, a person, group or a collective has (or maintains) full political privacy when they can authorize or deny access to all standard zones of political activity, that is those zones of political activity which sustain and encourage their active involvement in the political system of a democratic state.

Level of privacy protection	**Protected (guaranteed) zones of activity**	**Example of a zone of activity**	**Democratic principles necessary at a given level**
Critical political privacy	Critical	forming familial and collegial relationships where unsupervised methods of communications exist	limited application of the electoral principle and/or other principles
Baseline political privacy	Basic	participating in the presidential elections	the electoral principle the majoritarian principle the consensual principle
Full political privacy	Standard	starting, participating in and openly supporting a social organization	the liberal principle the participatory principle the deliberative principle he egalitarian principle

Table 5.1: Levels of privacy protection together with corresponding zones of activity and democratic principles.

Hence, the level of political privacy allowed in a given state can be described relative to the zones of political activity which are effectively protected in a given state. In order to be able to say whether a state has reached a given threshold of protection of political privacy, we must first agree on which zones of political activity are critical, baseline and standard. Both my earlier characterization in chapter 1, as well as my proposal for interpreting them given in the present chapter, are assuming a perspective of democratic principles. Consequently, although both the thresholds described earlier and their interpretation are up for debate, especially in the context of specific applications, where more coarse- or fine-grained analyses are needed, a necessary prerequisite for entering the discussion on what specific zones of activity should involve is a belief that a democratic state, despite all its shortcomings and inadequacies, is the optimal form of political organization within a modern state, relative to existing alternatives. That is, to debate the implementation of the theory of privacy which I developed, one must accept that a democracy is in principle superior to an autocracy, a dictatorship, *etc.* As

for the division into three types of zones of political activity, as well as the arguments which I am about to make concerning their content, one can argue that both should be formulated slightly differently, depending on the context in which they are used.

5.1.1 Zones of political activity

In my characterization of the critical, basic and standard zones of political activity, I take as a point of reference the seven principles of democracy used to conceptualize the notion of democracy in measurement projects such as the Varieties of Democracy (V-Dem). The seven principles by V-Dem are based on, though not identical to, the democratic principles in Dahl's theory of polyarchy (Teorell et al., 2019; Dahl, 2008). Thus, the term "critical" is in fact interpreted as meaning "critical from a democratic standpoint", as opposed to perspectives centered around other forms of political organization (*e.g.* a totalitarian standpoint), as well as fields which allow for systematic evaluations of states altogether (*e.g.* an economic standpoint). Similarly, the term "basic" and "standard" can be read as "basic for a democratic system" and "standard for a democratic system". At the same time, note that "critical from a democratic standpoint" does not mean the same as "critical for a democratic system". This choice of wording is deliberate and regards the idea behind the condition for critical political privacy protection being available in non-democratic states.

What are the *critical* zones of political activity? I proposed to understand them as the zones which are necessary for making possible the minimum active involvement of citizens in the political system of their state. This does not mean that the system is democratic, but rather that citizens are seen as an active component of governance in a country, where the government itself is not necessarily democratic and responsible to its people. For instance, from the democratic perspective, there exist a qualitative difference between the systems in China and North Korea in the extent to which citizens can be involved in local and national decision-making. Similarly, there exist qualitative differences between their approach and use of state surveillance. Even in a situation where China, or another non-democratic state, does not aspire to the full catalog of democratic principles, it may indeed aim at maintaining critical political privacy if the citizens are expected to be engaged in decision-making, for instance, at the local level. Conversely, the lack of critical political privacy is a situation when, as a result of surveillance, an individual, a group or a collective becomes almost completely subjugated to the representatives of public authority. In this sense, China itself may not meet the criteria for critical political privacy, but it is much closer to reaching them than, *e.g.*, North Korea.

Intuitively, minimum active involvement of citizens could mean that (1) citizens are allowed certain liberties against the local representatives of the central government, (2) may have real influence on the choice of representatives of local and national authority, even when elections are not held, (3) may successfully appeal to the judiciary in cases involving the decisions made by public authorities, even when the court cannot enforce the ruling on the public authority. Thus, the term "minimum active involvement" means the situation where citizens are allowed to hold real power over certain domains or problems, where they can lobby and take collective action in certain cases, but it does not necessarily signify a situation where the right to protest, congregate and vote is generally respected by the state. Some of the critical zones of political activity are:

(A1) forming familial and collegial relationships where unsupervised methods of communication exist (even if they are not used),
(A2) spending time alone, including developing ways of critical reflection, which may turn out to be subversive from the perspective of the government or public authority,
(A3) challenging the decision of a public employee, including a government employee, either individually or collectively,
(A4) appealing to the public authority in cases of abuse of power within the public sector,
(A5) appealing to the judiciary in cases of conflict with private or public entities.

Essentially, although critical political privacy does not guarantee the same level of individual or collective freedom as could be expected for citizens of a semi-democratic state, it is supposed to mark a difference between privacy violations which possibly render the state non-democratic, and violations which result in near complete subjugation of the citizens. It could be argued that the CCP in China allows different scope of political privacy to the Han Chinese, *i.e.*, the citizens who belong to the dominant ethnic group in China, and to other ethnicities. For instance, the repression of Uighurs discussed in section 2.5 relied on both electronic and physical surveillance, which included forcing the Uighur families to allow communist party officials to stay in their homes, often sharing the same bed (Towadi et al., 2021, p. 63). This policy is in direct violation of a critical zone of political activity, here (A1), where Uighur citizens are not allowed to have a normal family life, which preconditions the bare minimum of social and state involvement. In section 5.2.3 I return to the case of Uighur community while discussing the use of surveillance as a tool in genocide. Here, the remark I made earlier about the zones "critical from a democratic standpoint" may explain why I argue that the in-person

surveillance of Uighur families is a negative phenomenon. Although it may be seen as a positive development from the perspective of effective internal politics according to the CCP guidelines, ethnicity-based targeted surveillance violates, *e.g.*, what from a democratic standpoint constitutes the consensual principle of democracy, which I discuss in more detail below.

Baseline political privacy is the threshold where the considerations about the principles of democracy enter the picture. As I indicated at the beginning of this chapter, for the purposes of this dissertation I rely on the conceptualization of the term "democracy" used by the V-Dem democracy measurement project comprising in seven general principles that are subsequently operationalized in terms of chosen indices according to the V-Dem methodology (Coppedge et al., 2021, p. 4). In case of baseline political privacy, I propose to require that the *basic* zones of political activity be defined as the zones of political activity which are necessary for and which sustain the active involvement of the citizens in the political system of a given country. Intuitively, this means that the formal and institutional elements of a democratic system are already in place, though some of them may be faulty or lacking the material or human component needed to render the state fully democratic.

For instance, the electoral principle of democracy constitutes a core value of making the decision-makers responsive to the citizens by means of elections, carried out at regular, predetermined intervals. Coppedge and others argue that once the state drops the electoral principle, it can no longer be called democratic, regardless of its stance on other principles from the list. There may exist material differences between the citizens, which interfere with their access to votes in the election, as was documented, *e.g.*, in India, where citizens have been compelled to yield their voting rights to the representative of the political party which claimed dominance over a given area. The election fraud in India was in fact so significant that biometric confirmation of vote legitimacy was proposed in some analyses of the election process (Yadav and Singh, 2013; Vidyasree et al., 2016). In this case, the faulty election process does not automatically render India a non-democracy. However, voter fraud and corruption in voter authentication violate the egalitarian principle of democracy, which states that all citizens and groups should enjoy equal *de jure* and *de facto* capabilities to participate, including participation in the election. In other words, although the formal and institutional components of democracy are in place, their execution is impaired to a certain extent.

The state which wants to sustain the citizens' active political involvement must respect, at the very minimum, the following principles of democracy: the aforementioned electoral principle, the majoritarian principle, and the consensual principle. The majori-

tarian principle states that a majority of the citizens should be capable to express their political will through policies. To balance it out, the consensual principle requires that a majority should allow for sufficient representation of the interests and perspectives of political minorities. Note that there needs not be any trade-off between the two principles. In China, due to the superiority of the CCP over the will of the people, combined with the repression of ethnic, religious, political and sexual minorities, both principles are violated. Thus, a decrease in consensuality does not mean an increase in majoritarianism, or *vice versa*.

Given these principles, the basic zones of political activity may be identified as, for instance:

(B1) participating in the election process, while having the ability to freely discuss the choice of candidates among family and friends, even if the election process is flawed,

(B2) expressing and enacting one's identity (ethnic, religious, political, gender, *etc.*) without state retribution in the political context, within the frames of the law, even if the process is flawed,

(B3) lobbying for the collective interest of one's group (political, ethnic, *etc.*) without state retribution, within the frames of the law, even if the process is flawed or systematically unsuccessful,

(B4) being able to gather and congregate, including political assemblies conducted without state interference,

(B5) expressing one's political views publicly without retribution and discussing political matters in the press without state retribution (direct or indirect), within the frames of the law, including the right to protest.

The three examples which I describe in sections 5.1.2, 5.1.3 and 5.1.4, all fall into the basic zones of political activity, showing that the current state of political privacy protection is already rather poor, even in relatively privacy-oriented countries, such as the EU member states. At the same time, the proposed thresholds for political privacy are cumulative, which means that every basic zone of political activity is, by definition, also a critical one. Similarly, each standard zone will be considered basic and critical by default.

The last threshold, that of full political privacy, does not represent an ideal situation for which the states will strive asymptotically. Rather, the conditions for "full" political privacy ask for sustaining the zones of activity which are standard from the democratic standpoint. This means that the full list of democratic fundamental principles should be

considered, including, in addition to the previously mentioned, at the very least, the liberal principle, the participatory principle, the deliberative principle, and the egalitarian principle.

The liberal principle of democracy states that individual and minority rights must be protected against both the state and the "tyranny of the majority" (Coppedge et al., 2021, p. 4). Constitutional guarantees of civil liberties, rule of law and the system of checks and balances contribute to the values held through the liberal principle. Respecting the participatory principle means that citizens are free to engage with a multitude of political process, not limited to local or small-scale initiatives. Related to this is the deliberative principle, which says that political decisions must be informed by a process of multi-level dialogue, as opposed to populism, coercion, or manipulation on the side of the decision-makers. Finally, the egalitarian principle requires that the material and immaterial inequalities that inhibit the *de facto* use of formal political rights and liberties be eliminated. This includes significant inequalities in health and health care access, education, or income.

The standard zones of political activity related the principles described above are, for instance:

(C1) starting, participating in and openly supporting a social organization or a non-governmental organization, without state retribution, within the frames of the law,
(C2) running for and serving at public offices, including the positions of power, without state retribution or obstacles from the incumbents,
(C3) participating in the creation of agendas for public institutions and authorities without state retribution,
(C4) keeping sufficient checks on the state institutions at all levels, including citizen's initiatives to monitor public authorities,
(C5) being able to access knowledge and information needed to make informed political decisions.

An exhaustive characterization of the three types of zones of political activity may not be possible, given that the catalog of fundamental rights and freedoms – thus, also the list of democratic principles – remains open by design. Hopefully, the examples and explanations of the definitions of critical, baseline and full political privacy are sufficient to plant a solid intuition about the scope of each of them. In what follows, I will discuss some of the most relevant zones of activity where political privacy is a necessary guarantee of the zone's availability to citizens. First is the freedom of speech and its special case, the freedom of media and censorship. Second, the freedom of

elections, directly related to electoral principle of democracy. And lastly, the freedom of assembly and the right to protest.

5.1.2 Freedom of speech and free media

The interconnections between privacy, freedom of speech and freedom of media so diverse and well-documented that a brief summary is bound to omit some of their important aspects. Here, I limit my considerations to the issues most relevant to mass surveillance, which has been one of my foci in this dissertation. Mass surveillance has major impact on media and social communication, including on the relationship between journalists and their confidential sources, the credibility and safety of journalists and their editors, as well as access to the media in general. Aside from mass surveillance, journalists, editors, and whistleblowers have been subjected to targeted surveillance and repression.

Waters (2018) conducted a qualitative study on the methods which national security journalists use to communicate online to evade potential surveillance by government authorities, specifically through available digital security technologies. Both Waters and McQuail (1987) assume that surveillance is fundamentally connected with media in that, aside from its meaning related to state oversight, surveillance also describes a necessary prerequisite of journalistic work. Journalists, and indirectly also their supportive staff and editors, turn the results of their surveillance, in the form of observation of events and people, into news (Waters, 2018, p. 1296). However, I disagree with Waters on that the state surveillance and journalistic surveillance represent what is essentially the same phenomenon. Observation is not the same as oversight, and, as Waters himself noted, overt oversight typically results in attitude change in the object of observation, leading to subjugation and obedience towards the surveillor. Journalistic work, however, generally does not cause such changes in the mental state of the observed. Moreover, journalistic and media work usually involves targeted, purposeful observation, limited in time and scope. Eventually, objects of observation learn about the surveillance and they are in full power to challenge the appropriateness and truthfulness of the journalist's findings. The relationship between the journalist-observer and an individual is horizontal, equal from the legal point of view. In case of state surveillance, the relationship is hierarchical and ways of defense or appeal almost none. Targeted and purposeful surveillance are only some of the solutions in the state's rich observational toolkit, which includes wide and almost unrestricted use of general purpose surveillance, oversight conducted "just in case" or preemptively.

In my view, the expansion of the definition of surveillance proposed by Waters and McQuail trivializes the phenomenon. By this token, academic research would constitute a form of surveillance as well. Social scientists could be seen as turning surveillance of people and their relationships into analyses of social reality, while physicists could argue that they conduct surveillance of the universe. There is more to surveillance than just observation, and the social framework of panopticism, which Waters himself uses in his study may provide one explanation of what the difference between them is. Namely, surveillance is different from mere observation in that it gives the observer significant leverage, or power over the one being observed. Surveillance allows the observer to dominate and subjugate the observed in ways which simple observation cannot. After all, inmates do not typically conduct surveillance of the prison guards, even when both look one another in the eye.

However, aside from certain definitional problems, Waters' study reveals that mass surveillance changed the ways that journalists work. Some journalists said that mass surveillance required them to develop advanced technical skills in order to continue their field work. The ability to gain and rely on the technology impacted both the journalists' views on mass surveillance and the methods of securing their communication with sources. It also shifted their role towards the topic which they covered, making it more or less "adversarial" depending on their perception of mass government surveillance in the US (Waters, 2018, p. 1302). However, many national security journalists refused to participate in the study, often due to the sensitivity and potential risks associated with the content of the interviews. The refusal and drop out rate were so high that they imposed significant limitations on the study. The explanation of these phenomena given by Waters is informative of the difficulties in approaching topics such as this one, hence worth citing in full:

> A particular difficulty of this study was finding journalists willing to speak on the record about mass surveillance. Many national security journalists, who are likely more aware than the general public of the capabilities of mass surveillance programs, were reluctant to speak about the topic, regardless of any promise of anonymity. During the recruitment process, many potential participants stopped responding during the informed consent process, when they asked to see the interview protocol in advance. If they did respond during the consent process, several potential participants said they would not discuss these topics online, no matter how many precautions were taken, and others refused to discuss these topics with the author, whom they did not know. A common reply to requests for an interview was an outright refusal to discuss the topic on the record, preferring to keep their

methods and opinions to themselves for various reasons. (Waters, 2018, p. 1311)

Another important aspect of mass surveillance in relation to media is a simple matter of access. Bischoff (2022) conducted a rough comparative analysis of the internet freedom for countries around the world in 2022. The methodology behind the analysis was straightforward, each country being evaluated in six categories. The score in each category is assigned up to 2 points, except one, messaging/VoIP apps (Voice over Internet Protocol, or IP telephony), assigned up to 1 point. This is because many countries included in the analysis were banning or restricting certain communication apps but allowing the use of alternatives controlled by the government or the accredited telecoms providers. The six categories were: content—torrents, pornography, news media, social media, VPNs (virtual private networks), and messaging/VoIP apps. Overall, the higher the score, the more censored the country is. The score in each 2-point category is estimated as follows: the country scores 1 point if the service mentioned in the category is restricted but accessible; if the service is banned, the country scored 2 points.

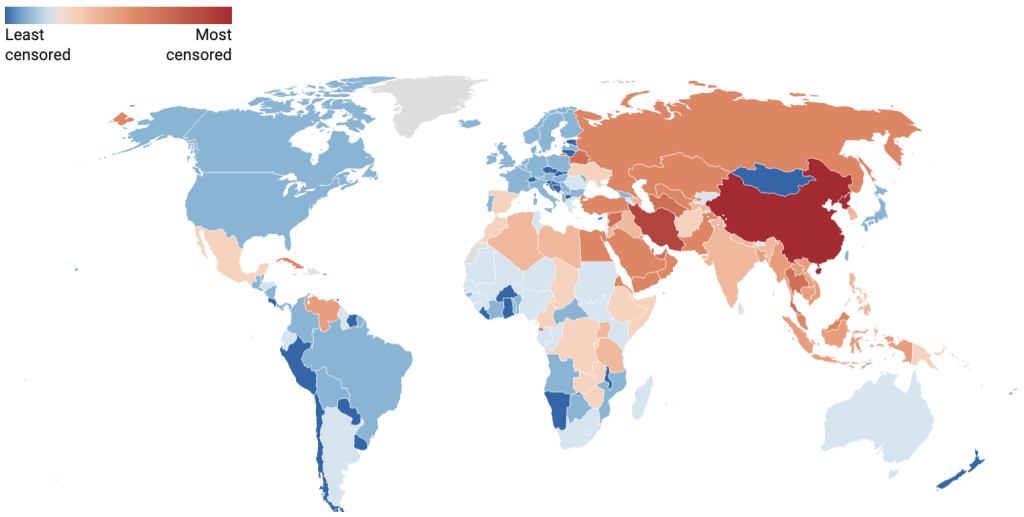


Figure 5.1: The map comparing the censorship levels around the world in 2022, based on the methodology desgined by Bischoff (2022) for Comparitech.

At the top of the list of censors state are North Korea and China (11 out of 11 points), Iran (10 points), Belarus, Qatar, Syria, Thailand, Turkmenistan, and the UAE (all with 8 points). All these countries heavily censor political media, restrict or ban social media and the use of VPN services. In Europe the most censored countries are Belarus (8 points), Ukraine (4), Turkey (7) and Spain (4), with possible addition of Russia (7) through the Kaliningrad Oblast, but Russia is not included in Bishoff's analysis of European censorship. So far, messagging and VoIP apps are not restricted in Europe, but

VPN services are restricted in Turkey and banned in Belarus. Restrictions on social media are present in Belarus, Montenegro, Spain, Turkey, and Ukraine. Political media is restricted in 12 countires, including Belarus and Turkey where the censorship is severe. Online pornography is banned in Belarus and Turkey, and restricted in Ukraine, while torrenting sites are banned or shut down in 18 countries.

In the context of EU regulation, technologies which enable E2EE (end-to-end encryption) and anonymous browsers such as TOR, both of which I discussed in chapter 4 (section 4.2.4), contribute greatly to maintaining and developing ways of protecting the citizens against state censorship. For this reason, I will argue that the European institutions, as well as the member states, need to turn back from their strategy to ban or limit the use of both types of technologies. Rather, they should focus on boosting the availability of anonymization tools in Europe and around the world. More details on the policy solutions which could bring the EU closer to this goal are included in section 5.3.

The Tor network and similar tools have been developed with civil liberties in mind, though solutions to prevent blocking access to the tool itself were added much later, after it turned out that Tor was being blocked during elections in Iran in June 2009 and in China earlier that same year. In case of Iran, it is alleged that around 10 percent of all traffic incoming to one of the major social networking platforms from Iran was coming *via* Tor (with 90 percent coming from proxies in the Amazon cloud) in June 2009 (Dingledine, 2009, p. 47). Despite intense efforts to develop technical solutions to censorship and firewalls, according to Dingledine, the co-founder of the Tor project, no amount of technology can replace legal and political solutions. This is because the power of firewalls and censorship is primarily *social*, not technological. Even when technical obstacles can be solved, actually obtaining solutions to bans and blockades which the states put up will require organizational and mental effort, and is likely to overwhelm the majority of citizens.

Free access to uncensored information about the political situation and the facts about the politicians, which are already within public discovery elsewhere, is a necessary component of making decisions related to voting in the elections, both individually and within collective or public discourse. Citizens who are deprived of free access to information cannot make proper use of their right to participate in the electoral process, thus violating the electoral principle and bringing the state below the minimal threshold for a democracy. The backdoor to messaging/VoIP apps in certain countries allow the state to interfere even within the most critical zones of political privacy, such as communicating with friends and family on themes related to political matters. Take for instance, the case of Aneeqa Ateeq, 26-year-old woman who was sentenced to death

in 2022 (including both a 20-year sentence and hanging) by a court in Rawalpindi for sending "blasphemous caricatures of holy prophets" and making remarks about the holy personages in a private WhatsApp conversation with a friend. Additionally, Pakistan asked Facebook and Twitter to assist in identification of Pakistani citizens suspected of blasphemy for the purposes of prosecution and extradition (Baloch and Ellis-Petersen, 2022). Similarly as in Pakistan, every instance of depriving citizens of control over a given zone of political activity constitutes a decrease in political privacy. Particularly relevant to the EU is the the censorship of political media and blocking or banning the VPN services.

5.1.3 Right to free elections

A problem related to privacy and security, but also to the freedom of elections due to known history of attacks, is the viral spread of fake news in the media, both traditional and social. The idea of fake news as a cyber threat has been proposed by Mare et al. (2019), Caramancion (2020) and Gradoń (2020), but so far did not gain enough traction to attract large-scale solutions within the field of national cyber security. Rather, the issue was ceded to private and non-governmental organizations running "debunking" and verification projects, where each potential threat (piece of news) is inspected on case-by-case basis. After several years of research (Lorek et al., 2015), certain automated credibility checkers[1] were also implemented by social media platforms since 2019 (Brattberg and Maurer, 2018).

In order to understand the root of the problem behind the 2016 US presidential campaign, Kim (2018) analyzed strategies and tactics of the Russian operative proven to have links with the Kremlin, the Internet Research Agency (IRA). Kim studied 3,519 Facebook and Instagram advertisements selected and released by the House Permanent Select Committee on Intelligence (HPSCI), generally reconfirming the earlier findings by the HPSCI concerning both the fact that the IRA showed a clear understanding of

[1] One of such solutions was proposed by myself and my team during the "Hack Belgium" hackathon in 2019. Our project, which took first place in the category "Credible, Engaging Media (Creating new experiences and new sources of trust)", proposed adding a "credibility layer" to links and media shared in news feeds and private conversations on social media platforms such as Facebook, Twitter, and WhatsApp by visualizing the level of reliability of the source in the preview and under a thumbnail of a published link (Samonek et al., 2019). Our analysis of credibility focused on targeting automatically generated content, forged images and videos, and sources related to known fake news generators, prioritizing neutrality, transparency of the evaluation process and user-friendliness, and taking into account the social component of technical problem mentioned by Dingledine (2009). A solution similar to ours was implemented independently by Facebook several weeks after the project was made public, but did not cover using automated checkers in private conversations.

political and election campaign strategies, as well its capacity to leverage data-driven targeting tactics on social networking platforms which they were using. One of the most striking and novel strategies on the side of the IRA was to create a full-blown digital ecosystem, including at least 73 different ad sponsors or groups. This allowed the IRA ecosystem to mimic the organic digital ecosystem, a network of related people and organizations, which an citizens using Facebook or Instagram would encounter in their everyday browsing. The ecosystem displayed deep knowledge of issues relevant to American users, including memes, music and events, aside from news-like pieces and political messages. This robust ecosystem allowed the IRA to perform a wide-scale attack, targeting users across the political spectrum and across multiple different platforms (besides Facebook and Instagram, also Eventbrite, MeetUp, Twitter, YouTube and other Google services).

The second aspect of the 2016 election attack was using the artificial ecosystem to run campaigns focused on the issues which would be maximally divisive in the American society, including race, nationalism and the alt-right movement, immigration, terrorism, guns and gun control, and LGBTQ rights. From among the ads surveyed by Kim almost 67 percent of ads contained a dictionary term (or a keyword) related to race, around 25 percent mentioned terms related to nationalism and the alt-right. The focus categories listed above covered up for around 96 percent of the Russian ads sample, leaving only around 4 percent to other issues, less controversial in the US (Kim, 2018, p. 4). To identify the US-based users receptive to the issues related to the six focus categories, the IRA relied on interest-based targeting in around 73 percent of cases. Interest-based targeting is a feature provided to ad sponsors on Facebook, where the "targets" are identified based on their personal preferences and data, which the company collects, following the mechanism described by Zuboff (2019) (see section 4.1.4). This allowed the IRA to use micro-targeted ad campaigns strategically designed to engage users whom Facebook identified as the the most susceptible to divisive messaging.

In parallel with the divisive campaigns, the IRA ran another campaign, aimed at voter suppression. Kim observed that around 7.6 percent of the surveyed ads contained non-political content. A qualitative analysis of the non-political subsample revealed that these ads were used to identify targets for voter suppression messages later on, especially in case of non-white users. Ads targeting African Americans and other non-white citizens initially promoted themes related to their racial or ethnic identity (which the IRA invested in for the sake of establishing trust) and switched to content discouraging participation in the elections later on, closer to election time.

Finally, through a simplified link analysis Kim was able to detect coordinated net-

works dating back to the pre-2016 election campaigns. The networked organization of the IRA included:

- organizing events where people from opposite positions on the political spectrum were set up to clash, including both demonstrations supporting one or more of the divisive causes and the counter-demonstration,
- using the same ad across ostensibly separate platforms or groups,
- creating what Kim called a "hub of influence", a landing page linked to multiple groups and online accounts, and
- using an intermediary, or a middleman, for certain groups and accounts, where the intermediary was seemingly unrelated to the main group, but served to amplify messages, build up traffic and add credibility to the main group in the evaluation of the platform's algorithms.

All the strategies which Kim described in relation to the 2016 US election campaign attack constitute violations of the political rights of the US citizens. For instance, setting up events designed to cause a clash between the citizens, which are not *bona fide* in support of any of the causes, is in fact a form of cyber attack targeting the the right to protest, aside from the more long-term goal of meddling in the US election, yet another violation of the democratic process and the US citizens' political rights. All the zones of political activity involved in the strategies used by the IRA require a breach of privacy before they can be accessed. The surveillance capitalist business model of Meta (Facebook) made this breach possible, thus endangering the national cyber security of the US.

Disinformation, or fake news, is as a cyber threat that endangers the security of citizen's discourse on political matters, thus threatening public and national security as well. This is why, in section 5.3.3, I argue that policies concerning fake news should be adjusted to the level of damage it involves, focusing on prevention *via* a multitude of cyber defense projects, as well as legislative efforts to decentralize the Internet.

5.1.4 Right to free assembly, protest and counter-instrumentarianism

Political privacy is a natural antidote to what Zuboff called instrumentarian power, both on the side of the governments and surveillance capitalist firms. The right to free assembly and the right to protest stand at the core of the conflict between the citizens and state power, as the rise in citizen discontent went hand in hand with the political and financial instability caused by effectively unregulated free-market economy.

As I mentioned before (see 4.1.3), civil unrest rooted in wealth inequalities which blew up around the 2010s is closely connected with the maturity of the neoliberal economic systems around the world. At the same time, surveillance tools were developed in part with the intention of mitigating the pressure caused by the protests. The reasoning behind using surveillance to curb civil unrest may seem benign at first, but upon closer inspection it seems that the very logic behind it is flawed.

Protests are a form of disrupting the normal operation of the state or its infrastructure. Thus, the state may interpret them as a threat to national security, since terrorism *sensu largo* aims at similar goals. It is through this goal identification that the state comes to associate protests with disruption and likens them to terrorist acts. However, such understanding of terrorism is much too broad, encompassing almost all successful resistance to state actions on the side of the citizens and non-citizens alike. Note that the very idea behind the right to protest was to empower the citizens to exert pressure on their governments, in the exact way which the modern governments came to see as a threat to state security.

The connection between the right to protest, the right to free assembly and political privacy was already made clear in chapter 2, where I analyzed the case of climate protesters in France, whose actions had been interpreted as threatening the stability and security of the state, and prosecuted extra-judicially under anti-terrorism laws (see section 2.1.2). One of the most important takeaways from this case study was that surveillance has a negative impact on political mobilization and political activism. Protecting political privacy at both state and European level may help reverse this state of affairs, thus boosting further development of civil societies in the EU.

5.2 Limits to surveillance

Königs (2022) argued that limitations on surveillance must be imposed on governments in democratic states, considering three scenarios. First is a loss of citizens' privacy due to mass collection of data by the governments, and the second – privacy loss due to accessing the collected data. I explored in depth in previous chapters (see in particular, section 1.3.4). The third possibility, which also features in studies by Raynes-Goldie (2010) and Marwick and Hargittai (2019), is that the collected data may be used for objectionable purposes. According to Königs, even within established democracies the expansion of surveillance leads to situations, where laws of doubtful legitimacy are enforced *via* surveillance and disproportionate punishment for the citizens who violate these laws. The list of illegitimate laws often includes the very laws which put surveil-

lance tools and practices in place:

> [T]he problem of defective legitimacy affects not only laws that are enforced with the help of government surveillance but also government surveillance as a policy itself. If existing democratic procedures do not meet the requirements necessary for democratic legitimation, the actual decision-making processes that lead to the introduction of surveillance programs may fail to ensure their legitimacy. Indeed, given the secretive nature of many surveillance operations and the importance of transparency for political legitimacy, the problem may be particularly acute for surveillance policies. (Königs, 2022, p.16)

Maintaining boundaries on how surveillance, especially mass surveillance, is used on their citizens is in the best interest of democracies, at least if they want to remain democracies. Meanwhile, surveillance technologies have become an important component of international technological arms race, especially with regards to the US and China (Chang, 2020). What actionable steps can democracies undertake to eliminate *external* surveillance? I propose that mass surveillance tools be treated with similar caution to how weapons be treated in international politics. That is, states should impose international standards on limiting surveillance, especially mass surveillance, and maintain a system of mutual control on the level of compliance with these standards.

I postulate that in case of the EU this means imposing uniform limitations on both government and corporate surveillance, which should be seen as a part of the joint cyber security effort among the member states. At the same time, programs which have the potential to yield open source privacy protection solutions should be designed and funded, while existing privacy-oriented solutions should be unanimously protected (see section 5.3.4).

5.2.1 Institutional *v.* social privacy

Raynes-Goldie (2010) and Marwick and Hargittai (2019) proposed to differentiate between institutional and social privacy. These term bear certain similarity to political and personal privacy in that both institutional privacy and political privacy involve institutions and mechanisms of public (state) authority, while social and personal privacy are limited to our peers. However, institutional and social privacy relate not to the concept of privacy as it, but to the *perceptions* concerning privacy. They are psychological, not political phenomena. To say that political privacy is different from personal privacy means that there exist zones of activity which are relevant to how an individual, a group or a collective share in state decision-making and how they engage in the politics of

their country. Personal privacy encompasses those zones of activity which lack political relevance, regardless of whether they involve a single individual, a family, a group of friends, or a political collective or government institution. As I have shown in section 5.1.1, forming familial and collegial relationships in which unsupervised methods of communications are available, even if they are not used, is a critical zone of political activity. Governments such as the CCP in China have a documented history of targeting these zones of activity for uniquely political reasons, including genocide (see section 5.2.3).

This being said, efforts to limit surveillance in accordance with the objectives of a democratic state may take advantage of the psychological tendency to separate social and institutional privacy. Raynes-Goldie discussed various strategies which the young netizens[2] relied on to manage their social privacy online, limiting other people's access to information about their personal affairs. Raynes-Goldie conducted an ethnographic study of young (predominantly 20-29 year old) Facebook users and described the methods which they use to re-purpose the platform's design to protect their own social privacy and also to violate the privacy of other users. Some of the participants in the study engaged in subversive practices aimed at mitigating privacy concerns, including aliasing, obscuring profile information and regular "wall cleaning". The first two are in direct violation of the platform's terms of service, while the practice of "cleaning" the record on regular basis contradicts the mission of Facebook to make users share "more rather than less", while being their "true" selves – the latter being a condition which the platform interprets as having one's real name and other personal information (day of birth, location, *etc.*) permanently attributed to one's online activity and also other people's online activity (Raynes-Goldie, 2010). In order to enforce the merging of all identities and activities, Facebook uses a range of technical solutions which make it harder for individuals to keep various areas of their life separate. Friends and strangers can tag users in posts and pictures, making any activity visible to the user's entire social circle, allowing for public discovery of all areas of their life without prior consent. Moreover, "cleaning" the wall is also discouraged, requiring each tag, image and post to be deleted manually. This form of "cleaning", deleting items from permanent record, requires time and energy, and if not performed regularly, may not be feasible for an average user. The

[2]The term *netizen* is used to describe the person using the internet in a context where being called a "user" usually relates to specific online service or platform, and where being a "user" entails being bound by the specific terms of service or user agreement, while being a "netizen" is free from such connotations. Achmad (2021, p. 1567) linked the emergence of netizens to social changes induced by the globalization of Internet and digital technologies, where a variety of technologies and tools are used to create a public arena for expression and communication.

participants in Raynes-Goldie's study who engaged in "cleaning" their walls usually did so on weekly basis.

However, Raynes-Goldie observed that institutional privacy seems to predate social networking platforms like Facebook, and comes closer to what was originally meant when the term "privacy" was being used by both theorists and regular citizens (see section 1.2). Marwick and Hargittai (2019) were interested in which incentives and disincentives netizens take under consideration when debating whether to share information with institutional actors online. Many focus group participants expressed distrust towards governmental and corporate institutions, mentioning skepticism and fear of discrimination among the causes for their concern. They observed that the willingness to disclose information significantly depended on the context in which information was provided, the recipient and the specific content of the information. The willingness to protect institutional privacy, which Raynes-Goldie understood as limiting or denying the access to information of firms and governments, was in fact quite universal and did not depend on one's strategies regarding social privacy.

5.2.2 Metaveillance, or who watches the watcher

Social "veillance", being seen by peers, which Raynes-Goldie researched in young netizens, is sometimes referred to as *coveillance*. Thus, under fine-grained definitions of various forms of observation, lateral and mutual observation among citizens or institutions at a comparable level of influence does necessarily need to entail surveillance. Sousveillance and metaveillance may contribute to balancing the surveillance activity, although, as I explained in section 4.3.1 sourveillance does not necessarily entail countersurveillance. On the contrary, sousveillance may be used to amplify the impact of surveillance. Thus, critical reflection on the limits and consequences of surveillance is better realized within metaveillance, the observation of observation, or the "veillance of veillance" (Mann, 2016, p. 1409). Certain technologies, such as drone swarming could be used to perform surveillance and security audits, autonomous-vehicle sensory verification, and automotive sensing, all early forms of metaveillance (Mann et al., 2019).

The popular rise in bottom-up counter-surveillance activity around the world shows that citizens still expect and value transparency on the side of police and other governmental bodies. Brucato (2015, p. 39) said that one of the challenges for modern governmental self-disclosure is ubiquitous surveillance, that is, wide and unrestricted use of surveillance technologies, where all possible information is collected, searched, and analyzed. Similarly to Königs (2022), Brucato argues that procedures and solutions

which are invented to repair the damage done to democratic values may be endangered, as the public authority takes steps to adapt to them. In his analysis of police brutality and the "cop watching" movement in the US, Brucato shows that the American police has grown into the new type of transparency, one induced by citizen sousveillance, people documenting the wrongdoing of police officers. Even though transparency is assumed to bring in at least a possibility of accountability, thus contributing to citizen empowerment, the actual outcomes of documenting police violence are not as significant as could be expected (Brucato, 2015, p. 50). Such initial analyses of the impact of sousveillance suggest that effective oversight of public authorities will require much more than bottom-up initiatives. "Cop watching" projects may give the citizens a feeling of control, but they fell short of curbing actual police violence. It is likely that proper metaveillance will not develop from citizen action alone, either. Rather, successful metaveillance requires a system of well-established independent institutions to monitor and restrict the use of surveillance in each state, as well as globally.

At the state level, a good start has been the German right to notification, discussed in section 2.1.4, together with the requirement to create a catalog of minimum safeguards, including specifying the nature, scope and duration of the possible oversight measures, the grounds for ordering them, the authorities competent to permit, carry out and supervise the use of these measures, and making available appropriate countermeasures to raise the level of public scrutiny and minimize the risk of abuse of the system of surveillance. Collegial supervisory bodies such as those created in Germany for the sake for metaveillance should become standard in every democracy, and should be made mandatory for all surveillance activity on the side of the government, as well as surveillance capitalist firms.

In relation to the case of genocide described in section 5.2.3, I propose that the international equivalents of state metaveillance control are put in place. From the strategic point of view, there exist procedural similarities between prosecuting excessive surveillance and prosecuting genocide. The countries where the governments are guilty of killing their own citizens are generally disincentivized to pursue prosecution, while any external interventions require significant diplomatic effort in order to not violate state sovereignty. The situation with surveillance is similar in this regard, which could make certain procedures used by the International Court of Justice (ICJ) effective in providing international solutions to abuses of oversight. As I argue in the following section, an additional reason to establish international control of the use of state surveillance is that surveillance often goes hand in hand with violence towards the citizens.

5.2.3 Surveillance in genocide and the need for global solutions

In a versatile historical study of genocide and its prosecution, Gebert (2022) shows that the idea to pursue protection from the violence inflicted on the citizens by their own state is much more recent than one might expect. The struggle for creating the international genocide convention started well after the second world war and was due to the efforts of Raphael (Rafał) Lemkin, a Polish lawyer whose family perished in the Holocaust and who attempted to propose a convention on genocide to Adolf Hitler during a conference in Madrid in 1933, but was prevented from doing so by the Polish Ministry of Foreign Affairs for the fear of offending Hitler (Gebert, 2022, p. 25). Lemkin survived the war and kept lobbying for the multilateral treaty which would criminalize genocide and obligate signatory states to enforce its prohibition. Only in 1948 did his plans come closer to becoming reality, when the United Nations General Assembly adopted (unanimously) the Convention on the Prevention and Punishment of the Crime of Genocide (CPPCG), also known as the Genocide Convention on December 9. The Convention entered force in January 1951. As of April 2022, 152 states have ratified or acceded to the treaty, including Mauritius (July 8, 2019). The Genocide Convention was the first legal instrument to challenge genocide. Before its adoption, genocide of their own citizens was seen as the prerogative of the states, a necessary attribute of their sovereignty. Irvin-Erickson (2016, p. 231) observed that even after its adoption, the Genocide Convention was "essentially stillborn", as no international tribunal capable of enforcing the treaty existed at the time. Genocide as a crime of intentional destruction of a people in whole or in part, where a people is understood as an ethnic, national, racial, or religious group, is still difficult to prosecute effectively, but the legislative efforts of Lemkin himself as well as his followers over they years resulted in relative progress.

However, so far both the lemkinian idea of "vandalism", or "cultural genocide", (Lemkin, 1947; Klamberg, 2018), as well as the problem of using state control to make acts of genocide possible are not widely discussed, let alone put into the law. For example, the use of surveillance in service of violence towards citizens was documented in case of Democratic Kampuchea, where surveillance techniques, biopolitical documentation, and preemptive policing strategies led to widespread "purges" during the rule of the Khmer Rouge (Tyner, 2018, p. xv). Esparza et al. (2009) conducted case studies of regimes of Argentina, Chile, Guatemala, Peru, and Uruguay, showing that during the Cold War period the US intelligence provided training needed to carry out surveillance campaigns in these states, aimed at identifying the "internal enemy", groups who were later subjected to genocidal violence. For instance, in case of 21 massacres conducted by

the Guatemalan government between June 1981 and December 1982, the targeted communities were subjected to surveillance, including multiple in-person visits by soldiers (Esparza et al., 2009, p. 93).

Perhaps the most versatile use of surveillance in genocidal violence nowadays is to be observed in China, where multiple communities are victim of genocidal violence, often assisted by ubiquitous surveillance technologies. One such community is the Uighurs of Xinjiang, whose current situation I explained in section 2.5. Another is the Tibetans, whose culture and population are systematically erased by the CCP, despite concentrated efforts to raise international attention by both the Tibetan government in exile and the Tibetan citizens who perform acts of self-immolation as a form of protest on regular basis (Barnett, 2012; Woeser, 2016; Demick, 2020). Although the citizens of Hong Kong and Taiwan so far escape the large-scale political violence inflicted by the CCP, Hong Kongers are massively leaving their home country due to the backlash following the pro-democratic protests and the Umbrella Movement, choosing indefinite emigration to escape the CCP prosecution (Chan, 2014; Leung, 2022). At the same time, Taiwan, who maintained a significant level of independence from the CCP and is currently governed by the majority Democratic Progressive Party (DPP) with the support of president Tsai Ing-wen, is preparing for military clash with China, expecting the Chinese invasion to mimic the recent Russian aggression in Ukraine (Davidson, 2022).

Clarke (2021, p. 9) described the elements of surveillance which accompanied the settler colonialist policies, political violence and cultural genocide in Xinjiang, which he referred to as the site of the "largest mass repression of an ethnic and/or religious minority in the world today". The pervasive use of surveillance is aligned with extrajudicial detentions in concentration camps (which the CCP calls "re-education" centers) and the systematic erasure of Uighur ethnic and religious identity. In the eyes of the CCP, cultural, ethnic or religious diversity is automatically demonstrative of subversiveness, threatening the cultural and ethnic dominance of the Han Chinese in the colonized region. In order to deal with the "internal enemy", the CCP established invasive measures of control and "transformation", both inside and outside the concentration camps (Clarke, 2021, p. 10):

> Outside of the detention centers more than 10 million Turkic Muslim minorities in the region exist in a "carceral state" where they are subjected to a dense network of hi-tech surveillance systems (including key elements of China's "social credit" system), checkpoints, and interpersonal monitoring which severely limit all forms of personal freedom.

In case of Xinjiang, no plans have been made to restrict the *means* of cultural geno-

cide, and even the international pressure concerning the already accomplished acts of cultural or strictly understood genocide are not particularly effective in preventing further violence. Note, however, that without surveillance tools and technologies, this level of targeting and erasure of Uighur cultural heritage could not be reached. Although blocking and banning the use of already developed surveillance tools to commit violence such as that in Xinjiang would be a complex international political feat, its potential to prevent totalitarian agenda from destroying communities and peoples is so significant that it may be well worth the effort.

5.3 Policy recommendations for the future of EU

In the final part on this chapter, I bring together the arguments presented throughout the dissertation to propose several changes in the EU approach to the problem of privacy and security. My proposal includes both legal and political instruments, which contribute to European cyber security and democratic stability. In section 5.3.1, I advocate for a multi-level understanding of privacy in the catalog of fundamental human rights. Both personal and political privacy should be seen as individual rights on the one side, and collective human rights on the other, with political privacy being emergent on various instances of personal privacy, especially when considering those zones of political activity which are critical from a democratic standpoint (see section 5.1.1). In section 5.3.2, I present three guiding principles, which could empower the effort to create a joint cyber security and cyber defense strategies in the EU. Section 5.3.3 draws on these principles to present disinformation campaigns as a threat to national security, which could be mitigated through joint defense programs.

Finally, in section 5.3.4, I present four sample solutions which further the protection of political privacy in the European model (see chapter 2 for a detailed explanation of what the three main models currently in use are). The solutions involve prioritizing open source tools, in accordance with the principle that what is open source, cannot be stolen. I also propose mandatory decentralization of digital services, in the same manner as anti-cartel and anti-monopoly regulations are enforced. With regards to end-to-end encryption (E2EE, also see section 4.2.4), I propose that the projects which make E2E encrypted communications possible be given special protection and funding in the EU, in order to make them safe and widely available even outside Europe. Lastly, I propose that research based on data exploration and analysis be performed in accordance with the best ethical standards and practices.

5.3.1 Personal and political privacy as fundamental human rights

As I have shown in section 2.1, the right to privacy is well-established in the EU, as it is counted among the fundamental human rights, protected under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). It is clear, however, that under current formulation in the ECHR, the right to privacy is interpreted as an individual right, but not a collective right. In section 3.2 of chapter 3, I argued that the right to privacy, especially political privacy, possesses an irreducible collective component, in that privacy is often the point of friction between the collective citizen agendas and the state, where the individual rights are merely a vehicle through which collective plans and postulates are lobbied for and, in case of government backlash, destroyed.

Hence, I propose that both political privacy and personal privacy in scope in which it contributes to the protection of political privacy, be protected as individual and collective human rights. The current form of Article 8 of the ECHR only protects personal privacy as an individual right, thus providing protection of only one out of four indispensable components of the right to privacy. In addition to extensions of the right to privacy in European law, I propose that actionable mechanisms of protection and appeal are put in place, such as the German right to notification, the possibility to challenge the decision to be put under surveillance, and other solutions which I presented throughout this dissertation.

5.3.2 Joint cyber defense strategies in the EU

I argued that issues such as state and corporate surveillance, and various cyber threats to civil society and the democratic processes, should be countered within a systematic program of a multilateral framework. In case of the EU, I proposed in Samonek (2020) that the strategies of cyber defense and cyber security programs be pursued jointly, though not necessarily through central management of the European institutions. I proposed three principles for a joint hybrid cyber security strategy, which I briefly summarize in what follows.

The first principle, known as the principle of efficiency in European cooperation, states that sharing the costs of building a resilient cyber security system is beneficial, assuming that a perceivably fair distribution of commitments is agreed upon. Second, the principle of non-aggression between the member states, which lies at the heart of the European project, requires an extension onto the new realms of warfare, including cyber warfare. In case of cyber attacks, identity attribution is a frequent problem. The attackers

may abuse third party resources to perform an attack, thus obscuring the source and leveraging the parties' ignorance against the system or network of interest. Unless the EU members commit their resources to building a joint defense strategy and facilitating the practice of sharing the information relevant to fending off the threats, it may become possible for one member state to be at war with another, and inadvertently so, though an unwitting contribution of resources.

Lastly, the principle of priority of the European Single Market (ESM) states that equal participation should be seen as an objective by the member states without being taken for granted. The member states should negotiate their respective contributions to cyber security systems and tools instead of relying on the EU regulations which guarantee a certain level of ESM access. The principle of ESM priority is of particular relevance to regulating privacy, as the companies like Apple or Facebook tend to negotiate their policies and business decisions almost exclusively with the EU representatives, while rarely attempting to address the institutions of the member states. Additionally, the European courts and EU data protection units have at their disposal appropriate tools for changing the privacy policies, user agreements, invalidating patents and solutions which threaten to harm the EU citizens and democratic stability. The national data protection authorities and other national security agencies are often unable to address large-scale negotiations and crises. This set up makes possible a positive reception of the European assistance with cyber security problems related to the private market, which overwhelm the national cyber defense systems.

My proposal to unify cyber defense strategies in the EU does not automatically imply supporting the current European legislation, enforcing the 2016 Cybersecurity Directive, or the operation of the EU Cybersecurity Agency (formerly ENISA, the European Union Agency for Network and Information Security) in its current capacity. Rather, I advocate for a bottom-up approach to joining and uniformization of European cyber defense. This method of coordination requires that the European cyber security agencies, including EU Cybersecurity Agency, focus their efforts of addressing the trust deficit among the member states through facilitating the environment for safe information exchange, instead of communicating with the member states through the medium of regulations and prescribing security standards. The European defense and cyber security authorities may benefit from embracing the inherent political character of international trust-building and taking the role of an active mediator, as opposed to presenting themselves as apolitical agents focused on purely technical aspects of European cyber security.

A particular threat to cyber security, which requires coordinated effort of the EU institutions and the member states is the propagation of disinformation (or fake news),

especially in relation to political processes and political attitudes formation.

5.3.3 Fake news as national security threat

Disinformation, also called fake news, is a special type of of misinformation. The latter term describes the spread of false information, with or without malicious intent, or without any intent at all. Disinformation is defined as deliberate misinformation: intentional spreading of false information.

Caramancion considers various aspects of technologies and human factors contributing to the spread of fake news, observing that "as a precursor, it has to be first recognized and postulated as a laying ground that disinformation should be categorized as a cyberthreat." (Caramancion, 2020, p. 440). In this dissertation my focus was only on digital disinformation, that is, spreading false information through the cyberspace. Both disinformation itself, as well as its primary set of motivations, are not new. Both have existed well before the emergence of computers and digital technologies. Traditional (non-digital) disinformation was, and still remains, pervasive in entertainment, politics and other areas of public life. Outside of politics, disinformation was documented to cause irreversible damages to financial assets of private firms, negatively affecting the stock value of the company's shares, its brand and social reputation. In relation to election processes, a case where a disinformation campaign significantly affected the presidential elections was described in section 5.1.3.

Aside from the immediate negative consequences to a specific target, fake news affects netizens' ability to engage and process information found online in the long-term as well, decreasing their ability to participate in the public dialogue and stay informed about issues which are relevant to their political and social situation (Wang and Lu, 2007; De Keersmaecker and Roets, 2017; Lee et al., 2020).

Because fake news is still seen primarily as a threat affecting social networks, digital media and other privately-owned information sources, and not political systems, it is usually private businesses and non-governmental organizations who are left with the task of combating it. This approach is a dangerous one because of the principle behind it and the consequences to the freedom of speech. The very idea that private operations should be responsible for dealing with disinformation, affecting the political life of the country both short- and long-term, is misguided. National cyber defense programs and strategies typically include protection of infrastructure, data and networks critical to the functioning of the state and society. Fake news spread directly targets the country's functioning, regardless of whether the channel of spread is privately-owned or not.

Another reason to deal with disinformation at a systemic level, rather than leaving the solution up to individual companies, is the decrease in freedom of speech and freedom of communication induced by the companies' protective policies.

Figure 5.2: The map of surveyed value repertoires in relation to value orientations: self *v.* other and citizen *v.* consumer by Trillò et al. (2021, p. 890).

Trillò et al. (2021) conducted a combined qualitative–quantitative content analysis of 20 popular value-related Instagram hashtags, sampling top 100 posts for each of them (running three rounds of 4 days each between February and April 2020), and revealed that distinct visual footprints are associated with 19 of them, typically showing an orientation towards the self and a strong emphasis on consumption. The focus on value-related terms, such as happiness, freedom, progress, knowledge, tradition, respect, sustainability, equality, compassion, and so on, was motivated by the question of how values are represented visually and propagated through the platform. The consistency between the expected value repertoire and the execution of value-related content in posts was the most unexpected result of the study. In 19 out of 20 cases, the hashtag possessed a distinct visual footprint, meaning that the statistical analysis revealed at least one distinguishing attribute for each of the 19 values. This makes the further results of the study particularly informative about the character of value's visual representation. The majority of value-related terms are associated with representations aligned with "showing-culture" (as opposed to "telling"), meaning that they prioritize icons as the preferred sign type and use images of cultural artifacts or relations between human subjects as their central theme (Trillò et al., 2021, p. 888). The orientation of the set of values onto the spectrum of self *v.* other and the spectrum of citizen *v.* consumer

revealed a striking bend towards self-oriented consumerism, as shown in figure 5.2.

These recent findings show a pervasive bias of Instagram content propagation towards marketable good and services in the representation of social and political values. Paradoxically, the value representations on Instagram are specifically directed *away* from citizenship. Trillò et al. considered two possible explanations for this anti-political bias. First, they asked whether the self- and consumerism-oriented direction originated from the users of the platform. Perhaps people simply use Instagram to engage with consumer goods and individual promoters of these good, and not to build communities or discuss politically relevant topics? If this preference was pervasive enough in most users, it could demonstrate itself even in the representation of value-related terms. However, a second possibility emerges as much more likely. Namely, the algorithms guiding content promotion and propagation are designed to give more visibility to consumption-related content and limit the visibility of political content. This mode of operation has been widely documented for account discussing matters related to femininity (Are, 2021; Faust, 2017), marginalized communities (Middlebrook, 2020), and others. The censorship of political or otherwise non-marketable information on Instagram often takes the form of a so called *shadowban*, a form of covert algorithmic censorship of the user's account without their knowledge or consent. Methods involved in performing a shadowban include restricting the visibility of the account to other users, rendering specific user hashtags undiscoverable, filtering out user's posts from the news feeds of others, or rendering the users handle (account name) invisible in the search results. The fact that a shadowban is covert means that the user cannot be sure that the ban is in place before its punishing effects are realized in the form of massively decreased interactions with other users. No ways to appeal the bans, including shadowbans, on Instagram exist. Techniques such as shadowbanning together with other, similar content promotion policies make Instagram a platform hostile towards political debate and citizen-oriented information. In relation to their study, Trillò et al. concluded what follows.

> This analysis suggests that the narrower meaning of value-related terms is not random, but follows a consumption-based paradigm in which things have to be marketable and monetizable in order to achieve enough visibility to enter the mainstream of Instagram's archive. A different way to look at this is to say that the commercial logic of Instagram's mainstream turns values into positively charged signifiers and puts them to work to increase the market appeal of specific goods and services (Trillò et al., 2021, p. 893).

The specific rationale behind information dispersal on Instagram makes it a platform, where political news, both fake or not, is not likely to gain visibility. Other platforms

deal with disinformation in different ways, often using algorithms specific to their infrastructure. However, many of these methods have been linked with censorship, often giving merit to abusers and misinformers over *bona fide* users (Are, 2020; Picardo et al., 2020; Bamman et al., 2012; Hintz, 2015).

In my opinion, the documented history of failure in combating disinformation, while preserving freedom of speech on social media platforms shows that individual companies are not competent to deal with cyber threats, which have impact on the political life of the communities to which they cater their services. Hence my proposal to designate disinformation a threat to national and European cyber security, and start taking seriously the need for safe systematic solutions.

5.3.4 Prioritizing existing beneficial solutions

Another proposal concerning cyber security and privacy policies is to prioritize the use and manufacturing of technological and technical solutions, which are beneficial to privacy, democratic stability and security in the EU.

Included in this list are various types of open source solutions in the EU, including cyber security tools. One aspect of open source software speaking in favor of its wider use is a simple fact that what is open source cannot be stolen. Public availability of open source code is a given, thus surprise takeover become much less likely. Open source code is often attack-tested immediately after release, making possible quick adjustments and fixes, thus eliminating vulnerabilities which would damage the infrastructure protected with proprietary, or "secret" code.

Another benefit of maximizing the use of open source software is the cost. According to Alsharif and Khelifi (2019, p.117), organizations and private companies would rather spend millions on proprietary security products and services, often making them the largest cost of the company's operations, before searching the market for open source alternatives. They argue that an active approach towards the challenges and misconceptions of today's open source software can help in mitigating these costs.

At the policy level, this could mean new batch of funding for projects which tackle the challenges of open source and produce new open source solutions needed in the European security market. Commitment to open source would also be a step towards building a joint European cyber defense (see section 5.3.2), without the need to force any of the EU members to share their solutions on a case-by-case basis.

Also on the list of solutions which are uniquely beneficial to both privacy and security are decentralized social media networks and services. Among them fediverses,

that is, collections of federated (interconnected) servers that are used for web publishing and file hosting, occupy a special position. Providing alternatives to widely used social media platforms such as Facebook, Instagram, or Twitter, fediverses such as Mastodon offer a distributed, decentralized and more customizable environment for citizen interaction (La Cava et al., 2021). On top of that, fediverses make disinformation campaigns such as that described in section 5.1.3 less threatening, because no central database of user data is available for ad customization and targeting.

The origins of fediverses and related open source software are connected to a mission avoid the censorship and control of centralized corporate social media platforms, while giving the users full capacity to communicate with their networks. The creators of fediverses have proven that technological progress, including social media technologies, is not inherently dependent on the abuse of privacy and data. They challenged the alleged neutrality of the software, showing that the widely marketed platforms are in fact not universal, neither are they necessary for social and political participation. Mansoux and Abbing (2020) discuss these and other benefits of developing and using fediverses, including the elimination of free labor and mass surveillance.

Future European policies should support the development of fediverses and other Internet decentralization tools. Moreover, decentralization of all services operating in the EU should be mandatory. Mass data collection and processing are not necessary for running social media services, as well as many other solutions which rely on surveillance capital at the moment. As Zuboff has argued (see section 4.1), surveillance capital is essentially dependent on data-predatory business model, not technologies. The EU should force the companies which operate within the logic of surveillance capital to search for new, safer and non-abusive business models. The technologies needed to make this happen are already in place, and many of them are freely available due to open source policies of their proponents. Decentralization should be pursued without consideration to financial losses to the corporation using a predatory business model, in the same manner as anti-cartel and anti-monopoly regulations are enforced. After all, if at any point in the history of European legislation the sacrifice of citizens' privacy was considered as an option to mitigate security threats, we have all the more reason to see the profits of a small number of companies as a reasonable trade-off for making possible a secure political future of European democracies.

Likewise, the protection of end-to-end encyption (E2EE) must become a default in European cyber defense agenda. This concerns also other anonymization tools, some of which I discussed in section 4.2.4. This means that effort must be made to inform technological non-experts, including legislators, about the character of E2EE, TOR, and

other privacy-protection tools. So far, even though effective ways of relaying this knowledge have been developed by, for instance, (Bai et al., 2020), Dechand et al. (2019, p. 401) have shown that both citizens and legislators do not know that secure and attack-proof methods of protecting their privacy exist and have developed inherent distrust to the communication technologies as a result.

The final point is ethical data exploration for the sake of knowledge building and research. Projects such as the aforementioned study of Tor usage by Mani et al. (2018) are using guidelines based on the Menlo Report (Kenneally and Dittrich, 2012). Four criteria for ethical network research laid out in the Menlo Report are:

(1.) the principle of respect for persons, realized *via* a rigid application of privacy protection practices and tools, refraining from collecting information which may identify specific persons, such as the IP addresses, and using differentially private techniques;
(2.) the principle of beneficience, meaning that the benefit of research is weighed against potential risk of harm to persons, public interest and security on a case-by-case basis;
(3.) the principle of justice, which in case of Mani and others' study meant that no specific group of users are chosen as the sample;
(4.) the principle of respect for law and public interest, attainable through maintaining transparency in research methods, including using open source software for data analysis and submitting the research plan to independent review bodies.

For research purposes, specialized review bodies which are able to develop and force compliance with the ethical data analysis standards should be created. There is also no reason why corporate use of data would need to stray from the ethical guidelines, to which the Menlo Report is just an initial step.

5.4 Summary

In this chapter, I focused on the relationship between political privacy and democracy, coming back to my initial proposal to consider three thresholds of privacy protection from a democratic standpoint. In section 5.1.1, I made a proposal on how to interpret the definitions from chapter 1 and relate them to democratic principles, taking as my reference point the seven principles used to conceptualize the notion of democracy in V-Dem measurement projects, an advanced, data-driven democracy measurement research project.

I proposed to differentiate between critical, baseline and standard zones of political activity, which in turn contribute to the definition of three level of political privacy protection. My interpretation of these terms is relative to the standards of democracies, even when the definition of a particular level of privacy protection is not sufficient for a democratic state. The choice to ignore the economic benefits, as well as the advantages of particular formulations of the notion of political privacy to, *e.g.*, totalitarian governments, is deliberate. The proposed thresholds for political privacy are cumulative, so that every basic zone of political activity is, by definition, also a critical zone, and each standard zone is also both basic and critical.

I understand critical zones of political activity as the zones which are necessary for making possible the minimum active involvement of citizens in the political system of their state, or treating citizens as an active component of governance in a country, even when the government itself is not necessarily democratic and responsible to its people. The minimum active involvement of citizens means that the citizens enjoy certain liberties against the local representatives of the central government, may influence the choice of representatives of local and national authority, even when elections are not held, or can successfully appeal to the judiciary in cases involving the decisions made by public authorities, even when the court cannot enforce the ruling on the public authority. This means that the citizens can lobby and take collective action in certain cases, but do not necessarily have an actionable right to protest, congregate or choose their political representatives at a state level.

Baseline political privacy is the threshold where the democratic principles start to matter. The basic zones of political activity are those which are necessary for and which sustain the active involvement of the citizens in the political system of a given country, often meaning that the formal and institutional elements of a democratic system are already in place, though some of them may be faulty or lacking the material or human component needed to render the state fully democratic. The following principles of democracy must be respected for the state to conform with the criteria for baseline privacy: the aforementioned electoral principle, the majoritarian principle, and the consensual principle (see section 5.1.1 for a description of the principles).

The final threshold, the protection of standard political privacy, does not represent an ideal, unattainable situation, but the conditions for sustaining the zones of activity, which are standard from the democratic standpoint. This means that the full list of democratic fundamental principles should be considered, adding to the previously mentioned, the liberal principle, the participatory principle, the deliberative principle, and the egalitarian principle.

In sections 5.1.2, 5.1.3 and 5.1.4, I discussed some of the most basic zones of political activity, which had been documented to have a strong connection to political privacy. The fact that all these zones are qualified as basic and not standard suggests that the current baseline of political privacy protection is rather low, even in relatively privacy-oriented countries of the EU. In discussing attacks on the security of the presidential elections, I highlighted several strategies which the Russia-funded operative known as the IRA used to influence the voters on platforms such as Facebook and Instagram. These strategies included the creation of a digital ecosystem, networked across multiple platforms, running a series of campaigns focusing on issues which are divisive in the American society, election interference and voter suppression, as well as the coordinated effort to mobilize and demobilize specific groups of voters.

In section 5.2 I discussed the limits to surveillance, bringing up some of the most pressing problems related to political privacy globally, such as the habitual use of surveillance as an aid in committing genocide and furthering settler colonialism in contemporary world. Finally, in section 5.3, I presented a list of policy recommendations concerning the future development of privacy laws and practices in Europe.

Conclusions

We need to change our way of thinking about privacy. This concerns both citizens and governments, as the increase in undemocratic surveillance measures is often caused by public pressure for more "security"; a state of affairs which, as discussed in section 4.4.1 often has little to do with actual drop in accidents and attacks, and more do to with public perception of situations and spaces.

In case of privacy and surveillance, we must keep in mind that nothing is given forever. It is natural to readjust our definitions and interpretations of fundamental concepts, as long as these processes are aimed to solidifying democratic principles. It was my intention in this dissertation to show that the state need not necessarily be seen as adversarial to privacy or democracy in general. At the same time, state and public authorities should not be so eager to take up the role of the adversary in order to protect themselves from their citizens.

The studies and examples which I analyzed show that state constant vigilance is counterproductive. The most obvious example of this fact is that the US "war on terror" unleashed by the administration of George W. Bush in September 2001 is almost unequivocally considered a failure (Kurtz-Phelan, 2021). But if we are to limit security measures, especially the mass surveillance, how far should we go? What is the necessary boundary for democratic governments in limiting their citizen's privacy, as well as the privacy of the foreigners?

In order to address these questions, I developed a new theory of privacy and used it to speak about political privacy. In chapter 1, I specified the conditions, which a theory of privacy needs to satisfy in order to be applicable to contemporary political problems. I discussed these conditions in detail in section 1.1, explaining that the conceptual framework supporting a political theory of privacy should satisfy the following:

(a.) be independent of terms strictly related to the current state of technology;

(b.) be centered not around the means of privacy protection, but around the ultimate value to which privacy is instrumental, that is, human life, dignity, and activity;

(c.) support a theory which is cross-disciplinary and uniform throughout contexts and cultures;

(d.) allow for differentiating between individual and social (communal) discovery of person's life and the discovery conducted by the state; and that

(e.) the resulting theory must allow for abstracting away from those social, political and economic convictions which are not fundamental to the concept of privacy.

As it turned out, none of the existing theories of privacy allowed for obtaining a framework which would fulfill these desiderata. I analyzed some of the most prominent theories of privacy in section 1.2.

In section 1.2.1, I showed that the first theory of privacy to be introduced in the American legal discourse, where privacy was interpreted as nonintrusion, was prompted by the public discontent regarding the unrestricted use of latest information technology at the time – photography. Based on the "right to be let alone" proposed by Cooley (1906, p. 29), consisting in the right to complete immunity against the effects of physical violence, including emotional and psychological damage, Warren and Brandeis came up with their own addition to this classification of rights – a protection against non-physical invasions into the private life of an individual. Although the definition quickly proved inadequate in characterizing privacy (Moor, 1991, p. 71), it was successful in combining normative arguments with the basic tenets of human psychology and the need for shelter from scrutiny.

The theory of privacy as freedom to act in personal matters (see section 1.2.2) was a result of judicial deliberations in the ruling concerning the Griswold *v.* Connecticut case in 1965. Although the theory was designed to support the constitutional reproductive rights, and not to give a comprehensive account of privacy as such, it helped the problem of privacy garner attention and respect both within law and among the US citizens.

Privacy as control of information is the first theory proposed after the supremacy of information in modern communication was established. Many presently used theories of privacy have as their foundational concept the notion of information. Moor (1991, p. 74) argued that this turn is due to the rise of information technologies, perceived as being capable of invading the privacy of individuals in a manner, which is unprecedented in the history of technology – a justification of "unprecedented" technological intrusion having at that point become a tradition in theorizing about privacy. The control of information account of privacy was proposed, among others, by Fried (1984), Beardsley (2017) and Westin (1967). As Moor (1991, p. 75) observed, information is wrongly conflated with the subject of privacy protection. However, information cannot be defined as the central

value of privacy because there are frequent situations in which control of information is lost, but privacy has not been breached or invaded. I discussed and analyzed examples of such situations in section 1.2.3 and 1.2.4.

The theories of restricted access, discussed in section 1.2.5, are among the most common modern theories of privacy. They are usually classified though specifying *what* it is that we are restricting access to, that is the range of states of affairs to which privacy is attributed. For instance, we may choose to restrict access to: (i.) information and persons themselves (Allen, 1998; Gavison, 1980; Powers, 1996), or (ii.) situations (Moor, 1991). Both types of theories, despite their shortcomings, which I pointed out in section 1.2.5, offer accurate insights into the social perception of privacy. I derive from these insights in proposing a novel gateway theory of privacy in section 1.3.

In the gateway theory of privacy a person has the benefit of privacy with respect to a specific zone of activity when she can authorize or deny access to it. I define a zone of activity as the domain of affiliated behaviors the consequences of which are restricted to the boundaries of this domain. In other words, a person will be said to have privacy with respect to a given zone of activity if she controls all its gateways, or points of access, which make observation of this zone possible.

Zones of activity, although comprising of various instances of behaviors, are not reducible to them. Similarly to the notion of a situation, a zone of activity can gain communal recognition or not. Despite these parallels with Moor's situations, zones of activity are not spatiotemporally burdened, nor can they be paraphrased as *just whatever a person does*. As a matter of fact, people can display behaviors which have no affiliation with other behaviors and do not belong to any known zone of activity. Moreover, zones of activity, although their catalog is open, are often conventional and it is by convention that their recognition as protected or unprotected is decided upon. Certain zones of activity are goal- or value-oriented, other stem from biological or territorial necessity. I listed examples of what can be a zone of activity in section 1.3.1 and also later in section 5.1.1.

Having developed the gateway theory of privacy, I apply it to contemporary debate concerning privacy and mass surveillance, as described in section 1.3.3. My hope is that an update in the concept of privacy will add relevance to the theoretical foundations of privacy debates, including that between the NSA and various privacy protection advocates.

But in my characterizations of the latest controversies surrounding privacy I do not defend or support any of these groups of interest. Rather, I acknowledge that the representatives of both may have legitimate interest in pursuing their respective strategies,

even when their goals and actions are not aligned with the best interest of the citizens, public security or democratic principles. I present the gateway theory of privacy as a middle ground, where all stakeholders are able to formulate their claims and concerns using the same conceptual basis (see section 1.3.6).

Next, I proposed the notion of political privacy in section 1.4. Since in the gateway theory privacy means being in control of the gateways to specific zones of activity, I propose to interpret political privacy as control of the gateways to zones of *political* activity.

At the same time, I specified, as a matter of initial proposal, three threshold of privacy protection. First, a person, group or a collective has (or maintains) *critical political privacy* when they can authorize or deny access to the critical zones of political activity, that is those zones of political activity which are necessary for their minimum active involvement in the political system of a given country.

Analogously, a person, group or a collective has (or maintains) *baseline political privacy* when they can authorize or deny access to the basic zones of political activity, that is those zones of political activity which are necessary for and which sustain their active involvement in the political system of a given country, with possible exceptions.

Finally, a person, group or a collective has (or maintains) *full political privacy* when they can authorize or deny access to all standard zones of political activity, that is those zones of political activity which sustain and encourage their active involvement in the political system of a democratic state.

Later in chapter 5, I gave examples of each type of zone of political activity (see section 5.1.1) and at the same time crossed them with the seven principles of democracy underlying the V-Dem democracy measurement project. I embedded political privacy into five key concepts in political philosophy: an individual, society, property, authority and the state (Rau et al., 2018, pp. 20-26). I argued that political privacy is directly linked to society as a whole, while personal privacy concerns primarily an individual and property. This orientation becomes clear when the fundamental notion on which privacy is built shifts from superficial vehicles, such as information or situation, onto more basic building blocks, such as zones of (political) activity, rooted in social relationships and social structures. At the same time, I noted the fact that one can only conduct surveillance of groups and collectives *via* surveillance of individuals. For this reason, privacy as an individual right will always require protection in the context of political activity.

In chapter 2 I argued that the relationship between privacy as a political, ethical and philosophical concept and *the right to privacy* (together with appropriate *privacy laws*), that is, privacy as a legal institution, is strictly hierarchical, and that the latter always

comes after political and ethical considerations. However, in order to be able to inspect the models of privacy regulation which are in use around the world, which I do *via* comparative model building, relevant laws must be brought up. I consider three cases of the right to privacy as it functions in the legal systems of the EU (with France and Germany as indication of internal trends), the USA and the China.

My analysis revealed striking differences between the case countries, ranging from the goals and strategic bases for implementing privacy solutions, to the role which theories of privacy play in the domestic and foreign policies of the analyzed countries. While the theories of privacy developed in the EU and the US predominantly aim at informing the policy and statutory law, Chinese scholarship mostly focused on explaining the already implemented policies and legitimize them in light of the social-political values, which are constituted from the top-down. Surprisingly, there exist point of convergence between the methods and the practice of surveillance between the US and China, much more so than between the US/China and the EU. Since 2013, the EU gradually implemented a strong protection model, one which is currently the most democratically promising from among the three paradigmatic models of privacy regulation. In comparison, the US model is that of *minimal protection*. Although the US government is unable to stop or challenge the public scrutiny of their surveillance programs after the Snowden revelations (see section 2.3), as well as ignore the conflict between mass surveillance and the US Constitution, it has displayed an overall positive approach towards mass surveillance throughout all presidential administrations since George W. Bush, including surveillance by the public or semi-public sector, and surveillance capital private firms.

The government of China overtly rejects political privacy, including in their laws what I called the Big Brother principle (see section 2.5) and removing political privacy from the scope of privacy protections in their recent regulations. Ubiquitous surveillance in China is not technologically unique, but its scope and official character make China an informative case in a comparative study.

In chapter 3 I argued that the privacy has a collective political component, aside from being an individual right. First, in section 3.1.1, I considered the position of privacy in liberal political philosophy. On one hand, certain liberal philosophers see privacy as a hindrance on the exchange of information in a free society (Posner, 1977; Sandel, 1998, p. 233). On the other hand, privacy was seen as one of the facilitating conditions for informed choice even by the critics of unlimited privacy protection (Allen, 1987; Seidman, 1986; Etzioni, 1999). Second, in section 3.1.2, I briefly discussed the role of privacy in non-liberal political philosophy, including a criticism of the liberal humanism

of human rights and how it failed to address the needs of the Indian society by Kapur (2014), as well as proposals for alternative philosophies of privacy and human rights by Ren (2018) and Chan (2015).

I showed that although privacy, and political privacy in particular, is not inherently dependent on liberal political philosophy, it does promote collective interests of the citizens, in alignment with the principles of liberal democracy, even when the citizens do not entertain all democratic freedoms in their county. In section 3.2.1, I analyze the case study of the Weiquan movement and the ethnic cleansing through surveillance in China (see also 5.2.3). I also examine the case of climate activists of ANVCOP21, who were treated as domestic terrorists in France, despite an openly non-violent character of their activity. Finally, in section 3.2 I show that collective rights are needed to protect collective interest and prevent collective damage, including the erasure of peoples and their cultural heritage.

In chapter 4 I discussed political privacy in the context of global economy, with special attention to surveillance capital, as well as the relationship between surveillance, privacy, and public security. Zuboff (2019) has shown that surveillance capitalism gives rise to a new type of power (including, but not limited to, political power), called instrumentarian power, or instrumentarianism. Instrumentarian power relies on the ability to know and systematize human behavior and allows those who wield it to shape human behavior in line with their own goals and preferences. I explored the origins of surveillance-based instrumentarianism throughout the first, second and third modernity in section 4.1. Next, in section 4.1.4, I argued that the emergence of surveillance capital, which spurred the development of ubiquitous surveillance technologies was the result of policy vacuum in an economic ecosystem of neoliberal free market.

I also described the conceptual changes which happened as a result of surveillance-oriented market shift. Customers of surveillance capitalist firms became *users* of their services, provided for free to all who agree to become the raw material for data extraction, analysis and behavior-informed targeting. Concerning the psychological aspects of privacy, I discussed certain perceptions which are often at the center of privacy education and public discourse. In section 4.2.1, I mentioned psychological incentives guiding the extraction of behavioral surplus. I argued that one of the key components of a surveillance-oriented business model is an elimination of decision-making, or agency (see section 4.2.3). I explained the fallacies of certain anti-privacy arguments, such as the "nothing to hide" argument, popular among the firms which collect user data on massive scale.

In section 4.2.4, the paradox of end-to-end encryption (E2EE) in European security

and privacy protection agendas is described alongside the basic facts concerning the use of privacy protection tools, such as the E2EE and the Tor network. In section 4.2.5 I placed surveillance in the context of "othering", alienating groups of citizens who are seen as a problem to the ideological or financial agenda of the government.

I explained how sousveillance is different from counter-surveillance in section 4.3.1. As Mann et al. (2015) argued before me, citizens engaging in sousveillance are unable to reciprocate surveillance perfectly, since the information they collect may also be used by their watchman to augment surveillance.

Section 4.3.2 contains considerations about the nature of *surveillance spaces*, such as the original concept of a Panopticon prison by Jeremy Bentham and many more facilities which were inspired by it. I also discussed the long tradition of employment surveillance, dating back at least to the Bata Shoes factory in the 1930s (section 4.3.3).

Also in chapter 4, I discussed mass surveillance, counter-terrorism and state surveillance, as defined in section and 4.4.2. I reviewed studies conducted by Maras (2010) and Houston (2017), who showed that the efficacy of mass surveillance was often much lower than that of traditional investigative methods. In section 4.4.3, I argued that political privacy is often necessary for internal and external security of a democratic state.

In the final chapter 5 I brought together the gateway theory of privacy and the democratic principles as proposed by Teorell et al. (2019). I described and gave examples of the critical, basic and standard zones of political activity, which condition, respectively, critical, baseline, and full privacy of the citizens.

Then, I discussed examples of democratic institutions which are protected by the right to privacy, including the right to speech and free media, the right to free elections, the right to free assembly and protest. In section 5.2 I argued that limits to surveillance are needed not only at the level of national governments, but also globally, using the case of Chinese genocide of Uighurs and Tibetans to illustrate how mass surveillance is instrumental in the control and erasure of peoples.

Lastly, I called for changes in privacy and surveillance policies within the EU. I proposed that the catalog of human rights be amended to include political privacy and personal privacy, both as individual, as well as collective rights (see section 5.3.1). I proposed that cyber defense strategies of EU members be united into a coherent, joint agenda, using soft methods based on voluntary contributions and trust-building initiatives.

Fake news, or disinformation, should be included in the list of threats to democracies, both in the EU and around the world. In section 5.3.4, I proposed that the existing privacy- and democracy-promoting solutions be given more attention from the decision-

makers, including support and funding of open source, free and widely available privacy protection tools. Finally, the principles of web decentralization and ethical data research should become mandatory in the EU.

Open problems

As I indicated throughout this dissertation, many interesting problems related to privacy and surveillance were left outside the scope of my considerations. Among them is the problem of applying the gateway theory of privacy in non-political contexts, including intercultural and intergenerational variance. It would be instructive to see how the notion of privacy as control over gateways leading to specific zones of activity plays out in different cultures, and how other critical concepts – such as, for example, family, employment, parenthood – influence which zones of activity are recognized as worthy of protection. How would the cultures of privacy protection interact with surveillance cultures in specific countries?

In case of European law and policy-making, it remains to be seen how the EU institutions impact the national privacy and surveillance politics of its member states. The reverse question is also open – how do EU members contribute to the shared understanding of privacy, including political privacy, and surveillance? And how to unify privacy protection regulations within the EU? Yet another set of open problems is what would be the optimal way of implementing the policy recommendations made in section 5.3. How do we prevent surveillance-assisted human rights abuses and genocide? How can the European model of privacy regulation be developed to reach full privacy protection?

The introduction of *political privacy* changes the debate about privacy and surveillance, especially mass surveillance. In this context, a question about alternatives to mass surveillance also emerges. Decentralization of the Internet is bound to restructure the entire digital market – how do we make the most effective transition from the current state of the market towards safer, more politically mindful business models? By answering these questions, we will create a better digital future for modern democracies.

Bibliography

Achmad, W. (2021). Citizen and Netizen Society: The Meaning of Social Change From a Technology Point of View. *Jurnal Mantik 5*(3), 1564–1570.

Agence France-Presse (2022). Tens of Thousands Protest Against New French Security Bill. *The Guardian*, January 30, 2021. https://www.theguardian.com/world/2021/jan/30/tens-of-thousands-of-people-across-france-protest-against-new-security-bill (Accessed May 30, 2021).

Agre, P. E. and M. Rotenberg (1998). *Technology and Privacy: The New Landscape*. MIT Press: Boston.

Ajunwa, I., K. Crawford, and J. Schultz (2017). Limitless Worker Surveillance. *California Law Review 105*, 735–776.

Akhgar, B., G. B. Saathoff, H. R. Arabnia, R. Hill, A. Staniforth, and P. S. Bayerl (2015). *Application of Big Data for National Security: a Practitioner's Guide to Emerging Technologies*. Butterworth-Heinemann: Oxford.

Al Ameen, M., J. Liu, and K. Kwak (2012). Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. *Journal of Medical Systems 36*(1), 93–101.

Allen, A. L. (1987). Taking Liberties: Privacy, Private Choice, and Social Contract Theory. *University of Cincinnati Law Review 56*, 461–492.

Allen, A. L. (1998). Coercing Privacy. *William and Mary Law Review 40*, 723–758.

Allen, A. L. (2012). An Ethical Duty to Protect One's Own Information Privacy. *Alabama Law Review 64*, 845–866.

Allen, A. L. (2013). Our Privacy Rights and Responsibilities: Replies to Critics. *Newsletter of the American Philosophical Association: Philosophy and Law 13*(1), 19–27.

Alsharif, I. and A. Khelifi (2019). Exploring the Opportunities and Challenges of Open Source Software and Its Economic Impact on the Cybersecurity Market. In A. Al-Masri and K. Curran (Eds.), *Smart Technologies and Innovation for a Sustainable Future: Proceedings of the 1st American University in the Emirates International Research Conference, Dubai, UAE 2017*, pp. 115–127. Springer: Cham.

Altman, I., A. Vinsel, and B. B. Brown (1981). Dialectic Conceptions in Social Psychology: An Application to Social Penetration and Privacy Regulation. In *Advances in Experimental Social Psychology*, Volume 14, pp. 107–160. Academic Press: San Diego.

Aly, G., K. H. Roth, E. Black, and A. Oksiloff (2004). *The Nazi Census: Identification and Control in the Third Reich*. Temple University Press: Philadelphia.

Amnesty International (2021). Why Edward Snowden Should Be Pardoned. *AI Actions for Individuals*, October 19, 2020. https://www.amnesty.org.uk/edward-snowden-nsa-whistleblower-pardon (Accessed May 30, 2021).

Appari, A. and M. E. Johnson (2010). Information Security and Privacy in Healthcare: Current State of Research. *International Journal of Internet and Enterprise Management 6*(4), 279–314.

Are, C. (2020). How Instagram's Algorithm Is Censoring Women and Vulnerable Users But Helping Online Abusers. *Feminist Media Studies 20*(5), 741–744.

Are, C. (2021). The Shadowban Cycle: an Autoethnography of Pole Dancing, Nudity and Censorship on Instagram. *Feminist Media Studies*, 1–18.

Avancha, S., A. Baxi, and D. Kotz (2012). Privacy in Mobile Technology for Personal Healthcare. *ACM Computing Surveys (CSUR) 45*(1), 3–20.

Bachelet, M. (2019). Note to Correspondents: Statement by UN High Commissioner for Human Rights Michelle Bachelet on Human Rights Day. *United Nations Statements*, December 10, 2019. https://www.un.org/sg/en/content/sg/note-correspondents/2019-12-09/note-correspondents-statement-un-high-commissioner-for-human-rights-michelle-bachelet-human-rights-day-scroll-down-for-french (Accessed May 30, 2021).

Bäck, E. and K. Wikblad (1998). Privacy in Hospital. *Journal of Advanced Nursing 27*(5), 940–945.

Baezner, M. and P. Robin (2018). Trend Analysis: Cyber Sovereignty. Center for Security Studies (CSS), ETH Zürich.

Bai, W., M. Pearson, P. G. Kelley, and M. Mazurek (2020). Improving Non-experts' Understanding of End-to-end Encryption: An Exploratory Study. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 210–219. IEEE.

Baloch, S. M. and H. Ellis-Petersen (2022). Woman Sentenced to Death in Pakistan Over "Bblasphemous" WhatsApp Activity. *The Guardian*, January 19, 2022. https://www.theguardian.com/world/2022/jan/19/pakistan-woman-aneeqa-ateeq-sentenced-to-death-blasphemous-whatsapp-messages (Accessed March 4, 2022).

Bamman, D., B. O'Connor, and N. Smith (2012). Censorship and Deletion Practices in Chinese Social Media. *First Monday 17*(3).

Bar-Tal, D. and D. Antebi (1992). Beliefs About Negative Intentions of the World: A Study of the Israeli Siege Mentality. *Political Psychology*, 633–645.

Barbopoulos, A. and J. M. Clark (2003). Practising Psychology in Rural Settings: Issues and Guidelines. *Canadian Psychology (Psychologie canadienne) 44*(4), 410–420.

Barnard-Wills, D. (2013). Security, Privacy and Surveillance in European Policy Documents. *International Data Privacy Law 3*(3), 170–180.

Barnett, R. (2012). Political Self-immolation in Tibet: Causes and Influences. *Revue d'Etudes Tibétaines 25*(12), 41–64.

Bartczak, M. (2013). The Right to Privacy in the Legal System of United States of America. *Toruńskie Studia Międzynarodowe 1*(6), 5–12.

Baude, W. and J. Y. Stern (2015). The Positive Law Model of the Fourth Amendment. *Harvard Law Review 129*, 1821–1889.

Bauman, Z., D. Bigo, P. Esteves, E. Guild, V. Jabri, D. Lyon, and R. B. Walker (2014). After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology 8*(2), 121–144.

Bauman, Z. and D. Lyon (2013). *Liquid Surveillance: A Conversation*. Polity Press: Cambridge.

BBC (2022). Encryption: UK Data Watchdog Criticises Government Campaign. *The BBC Technology News*, January 21, 2022. https://www.bbc.com/news/technology-60072191 (Accessed April 16, 2022).

BBC News (2001). Transcript: Bin Laden Video Excerpts. *BBC News Archive*, December 27, 2001. http://news.bbc.co.uk/2/hi/middle_east/1729882.stm (Accessed May 30, 2021).

Beardsley, E. L. (2017). Privacy: Autonomy and Selective Disclosure. In J. R. Pennock and J. W. Chapman (Eds.), *Privacy and Personality*, pp. 56–70. Transaction Publishers: New Jersey.

Benndorf, V. and H.-T. Normann (2018). The Willingness to Sell Personal Data. *The Scandinavian Journal of Economics 120*(4), 1260–1278.

Bentham, J. (1791). *Panopticon: or, The Inspection-house. Containing the Idea of a New Principle of Construction Applicable to Any Sort of Establishment, in Which Persons of Any Description Are to Be Kept Under Inspection, etc.* Thomas Byrne: Dublin.

Berscheid, E. (1977). Privacy: A Hidden Variable in Experimental Social Psychology. *Journal of Social Issues 33*(3), 85–101.

Bersoff, D. N. (2008). *Ethical Conflicts in Psychology*. American Psychological Association: Washington.

Berthold, S. and R. Böhme (2010). Valuating Privacy With Option Pricing Theory. In *Economics of Information Security and Privacy*, pp. 187–209. Springer: Dodrecht.

Binicewicz, A. (2021). *O prywatności w świecie nowych technologii: asymetria przejrzystości*. Universitas: Kraków.

Bischoff, P. (2022). Internet Censorship 2022: A Global Map of Internet Restrictions. *Comparitech*, May 12, 2022. https://www.comparitech.com/blog/vpn-privacy/internet-censorship-map/#Methodology (Accessed April 16, 2022).

Blackburn, S. (1999). *Think: A Compelling Introduction to Philosophy*. Oxford University Press: Oxford.

Blau, A. (2017). *Methods in Analytical Political Theory*. Cambridge University Press: Cambridge.

Bliss, C. I. (1967). *Statistics in Biology. Statistical Methods for Research in the Natural Sciences*. McGraw-Hill Book Company: New York.

Boix, C. and S. Stokes (2007). *The Oxford Handbook of Comparative Politics*. Oxford University Press: Oxford.

Borne, K. (2009). Scientific Data Mining in Astronomy. *ArXiv Preprint* (0911.0505).

Borne, K. D. (2010). Astroinformatics: Data-Oriented Astronomy Research and Education. *Earth Science Informatics 3*(1-2), 5–17.

Brattberg, E. and T. Maurer (2018). *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*, Volume 23. Carnegie Endowment for International Peace: Washington, DC.

Brennan, G., J. M. Buchanan, et al. (1980). *The Power to Tax: Analytic Foundations of a Fiscal Constitution*. Cambridge University Press: Cambridge.

Broeders, D. (2009). *Breaking Down Anonymity: Digital Surveillance of Irregular Migrants in Germany and the Netherlands*. Amsterdam University Press: Amsterdam.

Brown, W. (2004). "The Most We Can Hope For...": Human Rights and the Politics of Fatalism. *South Atlantic Quarterly 103(2/3)*, 451–463.

Browne, S. (2015). *Dark Matters*. Duke University Press: Durham.

Brucato, B. (2015). The New Transparency: Police Violence in the Context of Ubiquitous Surveillance. *Media and Communication 3*(3), 39–55.

Buchanan, J. M. (1968). *The Demand and Supply of Public Goods*, Volume 5. Rand McNally: Chicago.

Buchanan, J. M. and R. D. Tollison (1984). *The Theory of Public Choice*, Volume II. University of Michigan Press: Ann Arbor.

Burgess, A. and D. Plunkett (2013). Conceptual Ethics I. *Philosophy Compass 8*(12), 1091–1101.

Burita, L. and J. Chvátal (2016). Information Processing at the Period of Tomas Bata and Information System. In *Zlin: Proceedings of The 20th World Multi-Conference on Systemics, Cybernetics and Informatics*, pp. 183–188.

Burns, J. H. and T. Sprigge (2017). *The Correspondence of Jeremy Bentham. Volume 1: 1752-76*. UCL Press: London.

Burrows, T. (2016). The Town That Bata Built: A Modernist Marvel on the Marshes of Essex. *The Guardian*, September 8, 2016. https://www.theguardian.com/artanddesign/2016/sep/08/essex-architecture-weekend-east-tilbury-bata-shoe-factory (Accessed April 16, 2022).

Butt, J. and M. Awang (2017). Intention For Voting in Pakistan: The Role of Social Media, Ethnicity, and Religiosity. *International Journal of Multicultural and Multireligious Understanding 4*(5), 1–15.

Cappelen, H. (2018). *Fixing Language: An Essay on Conceptual Engineering*. Oxford University Press: New York.

Caramancion, K. M. (2020). An Exploration of Disinformation as a Cybersecurity Threat. In *3rd International Conference on Information and Computer Technologies (ICICT), 2020*, pp. 440–444. IEEE.

Chan, J. (2014). Hong Kong's Umbrella Movement. *The Round Table 103*(6), 571–580.

Chan, K. (2021). EU Court Opinion Leaves Facebook More Exposed Over Privacy. *AP News*, January 13, 2021. https://apnews.com/article/belgium-europe-data-privacy-93b5bdbf4eb35ae9692e08e037947137 (Accessed May 30, 2021).

Chan, P. C. (2015). Human Rights and Democracy With Chinese Characteristics? In *China, State Sovereignty and International Legal Order*, pp. 108–171. Brill Nijhoff: Leiden, Boston.

Chang, G. G. (2020). *The Great US-China Tech War*. Encounter Books: New York.

Chen, K. and A. I. Rea Jr (2004). Protecting Personal Information Online: A Survey of User Privacy Concerns and Control Techniques. *Journal of Computer Information Systems 44*(4), 85–92.

Chmielarz, K. (2019). *Asekuracja prawa do prywatności w kontekście polityki bezpieczeństwa w Polsce po 1990 roku*. Ph. D. thesis, Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej w Krakowie.

Clancy, T. K. (2010). The Fourth Amendment as a Collective Right. *Texas Tech Law Review 43*, 255–298.

Clarke, M. (2021). Settler Colonialism and the Path Toward Cultural Genocide in Xinjiang. *Global Responsibility to Protect 13*(1), 9–19.

Clifton, C., M. Kantarcioglu, J. Vaidya, X. Lin, and M. Y. Zhu (2002). Tools for Privacy Preserving Distributed Data Mining. *ACM SIGKKD Explorations Newsletter 4*(2), 28–34.

Clinton, R. N. (1990). The Rights of Indigenous Peoples as Collective Group Rights. *Arizona Law Review 32*, 739–748.

Coe, B. and P. Gates (1977). *The Snapshot Photograph: The Rise of Popular Photography, 1888-1939*. Ash & Grant: London.

Cofone, I. N. (2019). Nothing to Hide, But Something to Lose. *University of Toronto Law Journal 70*(1), 64–90.

Collins, B. (2016). Big Data and Health Economics: Strengths, Weaknesses, Opportunities and Threats. *Pharmacoeconomics 34*(2), 101–106.

Comey, J. (2018). *A Higher Loyalty: Truth, Lies, and Leadership*. Pan Macmillan: London.

Cooley, T. M. (1906). *A Treatise on the Law of Torts, or the Wrongs Which Arise Independently of Contract*, Volume 2. Callaghan: Chicago.

Coppedge, M., J. Gerring, C. H. Knutsen, S. I. Lindberg, J. Teorell, K. L. Marquardt, J. Medzihorsky, D. Pemstein, N. Alizada, L. Gastaldi, et al. (2021). V-Dem Methodology v11. *V-Dem Working Paper*.

Corfield, G. (2022). Privacy Is For Paedophiles, UK Government Seems to be Saying While Spending £500k Demonising Online Chat Encryption. *The Register*, January 20, 2022. https://www.theregister.com/2022/01/20/no_place_hide_campaign_anti_e2ee_ukgov/ (Accessed April 16, 2022).

Cox, W. H. (1990). Siege Mentality. *Parliamentary Affairs 43*(3), 380–382.

Crampton, J. W. (2015). Collect It All: National Security, Big Data and Governance. *GeoJournal 80*(4), 519–531.

Dahl, R. A. (2008). *Polyarchy: Participation and Opposition*. Yale University Press: New Haven and London.

Dambrine, B. (2015). The State of French Surveillance Law. *Future of Privacy Forum White Paper*, 22 December 2015.

Davidson, H. (2022). "It Feels Like the End of the World": Taiwan Civilians Practise for War as Ukraine Revives China Fears. *The Guardian*, April 11, 2022. https://www.theguardian.com/world/2022/apr/11/it-feels-like-the-end-of-the-world-taiwan-civilians-practise-for-war-as-ukraine-revives-china-fears (Accessed April 16, 2022).

De Bruin, B. (2010). The Liberal Value of Privacy. *Law and Philosophy 29*(5), 505–534.

De Keersmaecker, J. and A. Roets (2017). "Fake News": Incorrect, But Hard to Correct. The Role of Cognitive Ability on the Impact of False Information on Social Impressions. *Intelligence 65*, 107–110.

Dechand, S., A. Naiakshina, A. Danilova, and M. Smith (2019). In Encryption We Don't Trust: The Effect of End-to-end Encryption to the Masses on User Pperception. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 401–415. IEEE.

Delfanti, A. (2021). Machinic Dispossession and Augmented Despotism: Digital Work in an Amazon Warehouse. *New Media & Society 23*(1), 39–55.

Demick, B. (2020). *Eat the Buddha: The Story of Modern Tibet Through the People of One Town*. Granta: London.

Denton, J. (2021). The Fate of Facebook's Business Model May Lie in the Hands of the European Union Supreme Court. *Market Watch*, March 24, 2021. https://www.marketwatch.com/story/the-fate-of-facebooks-business-model-may-lie-in-the-hands-of-the-european-union-supreme-court-11616606837 (Accessed May 30, 2021).

Dingledine, R. (2009). Tor and Circumvention: Lessons Learned. *The Tor Project*. https://fahrplan.events.ccc.de/congress/2009/Fahrplan/attachments/1514_Tor-slides.pdf (Accessed April 16, 2022).

Dinstein, Y. (1976). Collective Human Rights of Peoples and Minorities. *International & Comparative Law Quarterly 25*(1), 102–120.

Doernberg, D. L. (1983). The Right of the People: Reconciling Collective and Individual Interests Under the Fourth Amendment. *New York University Law Review 58*, 259–298.

Dryzek, J. S., B. Honig, and A. Phillips (2008). *The Oxford Handbook of Political Theory*. Oxford University Press: Oxford.

Du, W. and M. J. Atallah (2001). Privacy-Preserving Cooperative Statistical Analysis. In *Seventeenth Annual Computer Security Applications Conference*, pp. 102–110. IEEE.

Duvall-Early, K. and J. O. Benedict (1992). The Relationships Between Privacy and Different Components of Job Satisfaction. *Environment and Behavior 24*(5), 670–679.

Dworkin, R. B. (1973). Fact Style Adjudication and the Fourth Amendment: the Limits of Lawyering. *Indiana Law Journal 48*, 329–368.

D'Amuri, F. and J. Marcucci (2017). The Predictive Power of Google Searches in Forecasting US Unemployment. *International Journal of Forecasting 33*(4), 801–816.

Einav, L. and J. Levin (2014). Economics in the Age of Big Data. *Science 346*(6210).

Eko, L. (2000). The Law of Privacy in the United States and France: One President's Impeachable Offense Is Another's Invasion of Privacy. *Communications and the Law 22*, 1–38.

Elias, B. (2009). *Airport and Aviation Security: US Policy and Strategy in the Age of Global Terrorism*. CRC Press: Boca Raton.

Esparza, M., H. R. Huttenbach, and D. Feierstein (2009). *State Violence and Genocide in Latin America. The Cold War Years*. Routledge: Abingdon.

Etzioni, A. (1999). A Communitarian Perspective on Privacy. *Connecticut Law Review 32*, 897–906.

European Commission (2017). Commission Fines Facebook 110 million EUR For Providing Misleading Information About Whatsapp Takeover. *EC Press Releases*, May 18, 2017. https://ec.europa.eu/commission/presscorner/detail/pl/IP_17_1369 (Accessed May 30, 2021).

Evans, R. and P. Lewis (2012). Undercover Police Had Children With Activists. *The Guardian*, January 20, 2012. https://www.theguardian.com/uk/2012/jan/20/undercover-police-children-activists (Accessed April 16, 2022).

Faust, G. (2017). Hair, Blood and the Nipple. Instagram Censorship and the Female Body. In U. U. Frömming, S. Köhn, S. Fox, and M. Terry (Eds.), *Digital Environments: Ethnographic Perspectives Across Global Online and Offline Spaces*, Media Studies, pp. 159–170. transcript Verlag: Bielefeld.

Felice, W. F. (1996). *Taking Suffering Seriously: The Importance of Collective Human Rights*. Suny Press: Albany, New York.

Fernback, J. (2013). Sousveillance: Communities of Resistance to the Surveillance Environment. *Telematics and Informatics 30*(1), 11–21.

Feshbach, S. and N. D. Feshbach (1978). Child Advocacy and Family Privacy. *Journal of Social Issues 34*(2), 168–178.

Fincher, L. H. (2016). China's Feminist Five. *Dissent 63*(4), 84–90.

Fincher, L. H. (2020). *Betraying Big Brother: The Feminist Awakening in China*. Verso Books: London, New York.

Floridi, L. (2002). What is the Philosophy of Information? *Metaphilosophy 33*(1-2), 123–145.

Frączek, K. (2013). *Ochrona danych osobowych w Polsce na tle standardów europejskich*. Ph. D. thesis, Uniwersytet Jagielloński.

Freeman, M. (1995). Are There Collective Human Rights? *Political Studies 43*(1), 25–40.

Fried, C. (1984). Privacy. A Moral Analysis. In F. D. Schoeman (Ed.), *Philosophical Dimensions of Privacy: An Anthology*, pp. 203–222. Cambridge University Press: Cambridge.

Fuchs, C. (2011). An Alternative View of Privacy on Facebook. *Information 2*(1), 140–165.

Ganeva, M. (2008). *Women in Weimar Fashion: Discourses and Displays in German Culture, 1918-1933*. Camden House: London.

Garbarino, J. (1977). The Price of Privacy in the Social Dynamics of Child Abuse. *Child Welfare 56*(9), 565–575.

Gavison, R. (1980). Privacy and the Limits of Law. *The Yale Law Journal 89*(3), 421–471.

Gebert, K. (2022). *Ostateczne rozwiązania. Ludobójcy i ich dzieło*. Wydawnictwo Agora: Warszawa.

Gillis, A. (1989). Crime and State Surveillance in Nineteenth-Century France. *American Journal of Sociology 95*(2), 307–341.

Glaes, G. (2018). *African Political Activism in Postcolonial France: State Surveillance and Social Welfare*. Routledge: London, New York.

Golbeck, J., C. Robles, and K. Turner (2011). Predicting Personality With Social Media. In *CHI'11 Extended Abstracts on Human Factors in Computing Systems*, pp. 253–262.

Gold, J. R. and G. Revill (2003). Exploring Landscapes of Fear: Marginality, Spectacle and Surveillance. *Capital & Class 27*(2), 27–50.

Goldenberg, S. (2013). Al Gore: NSA's Secret Surveillance Not Really "The American Way". *Guardian*, June 15, 2013. https://www.guardian.co.uk/world/2013/jun/14/al-gore-nsa-surveillance-unamerican (Accessed May 30, 2021).

Goldgeier, J. M. (1997). Psychology and Security. *Security Studies 6*(4), 137–166.

Goldstein, A. (2008). Privacy from Photography: Is There a Right Not to be Photographed Under New York State Law. *Cardozo Arts & Entertainment Law Journal 26*, 233–268.

Gonschior, A. (2017). Ochrona danych osobowych a prawo do prywatności w Unii Europejskiej. E-Wydawnictwo. Prawnicza i Ekonomiczna Biblioteka Cyfrowa. Repozytorium Uniwersytetu Wrocławskiego.

Goodin, R. E. (2017). *How to Write Analytical Political Theory*. Cambridge University Press: Cambridge.

Gouvin, E. J. (2004). Are There Any Checks and Balances on the Government's Power to Check Our Balances – The Fate of Financial Privacy in the War on Terrorism. *Temple Political & Civil Rights Law Review 14*, 517–542.

Gradoń, K. (2020). Crime in the Time of the Plague: Fake News Pandemic and the Challenges to Law-enforcement and Intelligence Community. *Society Register 4*(2), 133–148.

Greenwald, G. (2013). NSA Collecting Phone Records of Millions of Verizon Customers Daily. *Guardian*, June 6, 2013. https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (Accessed May 30, 2021).

Grey, T. C. (1983). *The Legal Enforcement of Morality*. Knopf: New York.

Gross, R. and A. Acquisti (2005). Information Revelation and Privacy in Online Social Networks. In *Proceedings of the 2005 ACM workshop on Privacy in the Electronic Society*, pp. 71–80. ACM.

Grzybczyk, K. (2021). *Skradziona kultura. Jak Zachód wykorzystuje cudzą własność intelektualną*. Wolters Kluwer: Warszawa.

Guttman, J. E. (1984). Primary Elections and the Collective Right of Freedom of Association. *The Yale Law Journal 94*(1), 117–137.

Halliday, T. (2016). My Friend Li Heping, a Man China Thinks Is "More Dangerous Than Bin Laden". *The Guardian*, June 8, 2016. https://www.theguardian.com/world/2016/jun/08/my-friend-li-heping-the-man-china-thinks-is-more-dangerous-than-bin-laden (Accessed May 30, 2021).

Hamlin, A. (2017). *Positive Political Theory*. Cambridge University Press: Cambridge.

Han, D. (2018). Search Boundaries: Human Flesh Search, Privacy Law, and Internet Regulation in China. *Asian Journal of Communication 28*(4), 434–447.

Hardt, M. and G. N. Rothblum (2010). A Multiplicative Weights Mechanism For Privacy-Preserving Data Analysis. In *2010 IEEE 51st Annual Symposium on Foundations of Computer Science*, pp. 61–70. IEEE.

Harris, D. J., M. O'Boyle, E. Bates, and C. Buckley (2014). *Law of the European Convention on Human Rights*. Oxford University Press: USA.

Harviainen, J. T. and R. Savolainen (2014). Information as Capability for Action and Capital in Synthetic Worlds. In *Proceedings of ISIC: the Information Behaviour Conference, Leeds, 2-5 September, 2014*, Volume 19. ISIC.

Haslanger, S. (2000). Gender and Race: (What) Are They? (What) Do We Want Them to Be? *Noûs 34*(1), 31–55.

He, B. (2005). Minority Rights with Chinese Characteristics. pp. 56–79. Oxford University Press: Oxford.

Hefferman, W. C. (1995). Privacy Rights. *Suffolk Universsity Law Review 29*, 737–808.

Heffernan, W. C. (2016). *Privacy and the American Constitution: New Rights Through Interpretation of an Old Text*. Palgrave Macmillan: Cham.

Hert, P. d. and F. Boehm (2012). The Rights of Notification After Surveillance is Over: Ready for Recognition? In J. Bus, M. Hildebrandt, and M. Crompton (Eds.), *Digital Enlightenment Yearbook 2012*, pp. 19–40. IOS Press: Amsterdam.

Hintz, A. (2015). Social Media Censorship, Privatized Regulation and New Restrictions to Protest and Dissent. pp. 109–126. Rowman & Littlefield London.

Houston, T. (2017). Mass Surveillance and Terrorism: Does PRISM Keep Americans Safer? University of Tennessee Honors Thesis Projects (Seniors Thesis).

Hualing, F., R. Cullen, et al. (2008). Weiquan (Rights Protection) Lawyering in an Authoritarian State: Building a Culture of Public-Interest Lawyering. *The China Journal* (59), 111–120.

Huey, L., K. Walby, and A. Doyle (2006). Cop Watching in the Downtown Eastside: Exploring the Use of (Counter)surveillance as a Tool of Resistance. pp. 161–178.

Inkster, N. (2014). The Snowden Revelations: Myths and Misapprehensions. *Survival 56*(1), 51–60.

Introna, L. D. (1997). Privacy and the Computer: Why We Need Privacy in the Information Society. *Metaphilosophy 28*(3), 259–275.

Irvin-Erickson, D. (2016). *Raphaël Lemkin and the Concept of Genocide*. Pennsylvania Studies in Human Rights. University of Pennsylvania Press: Philadelphia.

Isaak, J. and M. J. Hanna (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer 51*(8), 56–59.

Israel, D. J. and J. Perry (1991). *What is Information?* CSLI: Stanford.

Jackson, S. L. (2004). A USA National Survey of Program Services Provided by Child Advocacy Centers. *Child Abuse & Neglect 28*(4), 411–421.

Jenkins, R. V. (1975). Technology and the Market: George Eastman and the Origins of Mass Amateur Photography. *Technology and culture 16*(1), 1–19.

Jennings, H. (2012). *Pandaemonium 1660–1886: The Coming of the Machine as Seen by Contemporary Observers*. Icon Books Ltd: London.

Jingchun, C. (2005). Protecting the Right to Privacy in China. *Victoria University Wellington Law Review 36*, 645–664.

Johansson, Y. (2020). Speech by Commissioner Johansson at Webinar on "Preventing and Combating Child Sexual Abuse and Exploitation: Towards an EU Response". *European Commission*, June 9, 2020. https://ec.europa.eu/commission/commissioners/2019-2024/johansson/announcements/speech-commissioner-johansson-webinar-preventing-and-combating-child-sexual-abuse-exploitation_en (Accessed April 16, 2022).

Kapur, R. (2014). In the Aftermath of Critique We Are Not in Epistemic Free Fall: Human Rights, the Subaltern Subject, and Non-Liberal Search For Freedom and Happiness. *Law and Critique 25*(1), 25–45.

Kelly, G. (2017). *Newgate Narratives*. Routledge: London.

Kenneally, E. and D. Dittrich (2012). The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research. *SSRN*, August 3, 2012. http://dx.doi.org/10.2139/ssrn.2445102 (Accessed March 20, 2021).

Kennedy, D. (2004). *The Dark Side of Virtue: International Humanitarianism Reassessed*. Princeton: Princeton University Press.

Khoo, E. G., U. Hyvönen, and L. Nygren (2002). Child Welfare or Child Protection: Uncovering Swedish and Canadian Orientations to Social Intervention in Child Maltreatment. *Qualitative Social Work 1*(4), 451–471.

Kim, G.-H., S. Trimi, and J.-H. Chung (2014). Big-Data Applications in the Government Sector. *Communications of the ACM 57*(3), 78–85.

Kim, Y. M. (2018). Uncover: Strategies and Tactics of Russian Interference in US Elections. *University of Wisconsin-Madison School of Journalism and Mass Communication*, April 9, 2018. https://journalism.wisc.edu/wp-content/blogs.dir/41/files/2018/09/Uncover.Kim_.v.5.0905181.pdf (Accessed March 20, 2021).

Kirchgässner, G. (2014). The Role of Homo Oeconomicus in the Political Economy of James Buchanan. *Constitutional Political Economy 25*(1), 2–17.

Kiwanuka, R. N. (1988). Developing Rights: The UN Declaration on the Right to Development. *Netherlands International Law Review 35*(3), 257–272.

Klamberg, M. (2018). Lemkin on Vandalism and the Protection of Cultural Works and Historical Monuments During Armed Conflict. In M. Deland, M. Klamberg, and P. Wrange (Eds.), *International Humanitarian Law and Justice: Historical and Sociological Perspectives*, pp. 183–196. Routledge: Abingdon.

Klauser, F. (2016). *Surveillance and Space*. Sage: London.

Koch, S. (2021). Engineering What? On Concepts in Conceptual Engineering. *Synthese 199*(1), 1955–1975.

Königs, P. (2022). Government Surveillance, Privacy, and Legitimacy. *Philosophy & Technology 35*(1), 1–22.

Kooijmans, P. H. (1990). Human Rights – Universal Panacea? Some Reflections on the So-called Human Rights of the Third Generation. *Netherlands International Law Review 37*(3), 315–329.

Koomen, M. (2021). The Encryption Debate in the European Union: 2021 Update. *Carnegie Endowment for International Peace*, Washington. https://carnegieendowment.org/2021/03/31/encryption-debate-in-european-union-2021-update-pub-84217 (Accessed April 16, 2022).

Krause, H. D. (1965). Right to Privacy in Germany–Pointers for American Legislation. *Duke Law Journal*, 481–530.

Kuczma, E. (2017). *Generalny Inspektor Ochrony Danych Osobowych jako organ ochrony prawa do prywatności*. Ph. D. thesis, Uniwersytet w Białymstoku.

Kurtz-Phelan, D. (2021). Who Won the War on Terror? https://www.foreignaffairs.com/issue-packages/2021-08-24/who-won-war-terror (Accessed April 10, 2022).

La Cava, L., S. Greco, and A. Tagarelli (2021). Understanding the Growth of the Fediverse Through the Lens of Mastodon. *Applied Network Science 6*(1), 1–35.

Łakomiec, K. (2020). *Konstytucyjna ochrona prywatności. Dane dotyczące zdrowia*. Wolters Kluwer: Warszawa.

Landau, S. (2013). Making Sense From Snowden: What's Significant in the NSA Surveillance Revelations. *IEEE Security & Privacy 11*(4), 54–63.

Lash, K. T. (2004). The Lost Original Meaning of the Ninth Amendment. *Texas Law Review 83*, 331–430.

Lee, S., J. P. Forrest, J. Strait, H. Seo, D. Lee, and A. Xiong (2020). Beyond Cognitive Ability: Susceptibility to Fake News Is Also Explained by Associative Inference. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, pp. 1–8.

Leino-Kilpi, H., M. Välimäki, T. Dassen, M. Gasull, C. Lemonidou, A. Scott, and M. Arndt (2001). Privacy: A Review of the Literature. *International Journal of Nursing Studies 38*(6), 663–671.

Lemkin, R. (1947). Genocide As a Crime Under International Law. *American Journal of International Law 41*(1), 145–151.

Lemonidou, C., A. Merkouris, H. Leino-Kilpi, M. Välimäki, T. Dassen, M. Gasull, P. A. Scott, C. Tafas, and M. Arndt (2003). A Comparison of Surgical Patients' and Nurses' Perceptions of Patients' Autonomy, Privacy and Informed Consent in Nursing Interventions. *Clinical Effectiveness in Nursing 7*(2), 73–83.

Lennon, D. (1999). The Future of "Free" Information in the Age of the Internet. In *Aslib Proceedings*, Volume 51, pp. 285–289. MCB UP Ltd.

Leung, M. (2022). Exodus Hits Hong Kong Universities as Professors and Students Leave. *Advocate: Journal of the National Tertiary Education Union 29*(1), 36–37.

Lever, A. (2013). Privacy: Restrictions and Decisions. *American Philosophical Association Newletter on Philosophy and Law 13*(1), 1–6.

Levy, M. A. (1995). Is the Environment a National Security Issue? *International Security 20*(2), 35–62.

Liang, X., R. Lu, L. Chen, X. Lin, and X. Shen (2011). PEC: A Privacy-Preserving Emergency Call Scheme for Mobile Healthcare Social Networks. *Journal of Communications and Networks 13*(2), 102–112.

Liu, R. and D. Wei (2004). The Ethical and Legal Standardization to Gene Privacy. *Studies in Dialectics of Nature 9*, 77–81.

Locke, J. (2015). *The Second Treatise of Civil Government*. Broadview Press: Peterborough.

Lorek, K., J. Suehiro-Wiciński, M. Jankowski-Lorek, and A. Gupta (2015). Automated Credibility Assessment on Twitter. *Computer Science 16*(2)), 157–168.

Lubin, A. (2017). We Only Spy on Foreigners: The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance. *Chicago Journal of International Law 18*, 502–552.

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique. *Big Data & Society 1*(2), 1–13.

Lyon, D. (2018). Exploring Surveillance Culture. *On_Culture: The Open Journal for the Study of Culture 6*(6), 1–11.

MacKinnon, R. (2011). Liberation Technology: China's" Networked Authoritarianism". *Journal of Democracy 22*(2), 32–46.

MacLeod, C. (2011). Chinese Activists Disappear Amid Calls for Protests. *USA Today*, March 3, 2011. https://usatoday30.usatoday.com/news/world/2011-03-03-china04_ST_N.htm (Accessed May 30, 2021).

Macnish, K. (2018). Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World. *Journal of Applied Philosophy 35*(2), 417–432.

Macnish, K. (2020). Mass Surveillance: A Private Affair? *Moral Philosophy and Politics 7*(1), 9–27.

Madrigal, A. C. (2017). What Facebook Did to American Democracy. *The Atlantic*, October 12, 2017. https://www.theatlantic.com/technology/archive/2017/10/what-facebook-did/542502/ (Accessed April 16, 2022).

Malcolm, H. A. (2005). Does Privacy Matter? Former Patients Discuss Their Perceptions of Privacy in Shared Hospital Rooms. *Nursing Ethics 12*(2), 156–166.

Mani, A., T. Wilson-Brown, R. Jansen, A. Johnson, and M. Sherr (2018). Understanding Tor Usage With Privacy-Preserving Measurement. In *Proceedings of the Internet Measurement Conference 2018*, pp. 175–187.

Mann, S. (2016). Surveillance (Oversight), Sousveillance (Undersight), and Metaveillance (Seeing Sight Itself). In *2016 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pp. 1408–1417. IEEE.

Mann, S., R. Janzen, M. A. Ali, and K. Nickerson (2015). Declaration of Veillance (Surveillance is Half-truth). In *2015 IEEE Games Entertainment Media Conference (GEM)*, pp. 1–2. IEEE.

Mann, S., J. Nolan, and B. Wellman (2003). Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. *Surveillance & Society 1*(3), 331–355.

Mann, S., C. Pierce, J. Hernandez, Q. Li, B. C. Zheng, and Y. X. Xiang (2019). Drone Swarms for Sensing-of-Sensing. In *2019 IEEE Sensors*, pp. 1–4. IEEE.

Mansoux, A. and R. R. Abbing (2020). Seven Theses on the Fediverse and the Becoming of FLOSS. In *The Eternal Network: The Ends and Becomings of Network Culture*, pp. 124–140. Institute of Network Cultures: Amsterdam, and transmediale e.V.: Berlin.

Maras, M.-H. (2010). How to Catch a Terrorist: Is Mass Surveillance the Answer? *Journal of Applied Security Research 5*(1), 20–41.

Mare, A., H. M. Mabweazara, and D. Moyo (2019). "Fake News" And Cyberpropaganda in Sub-Saharan Africa: Recentering the Research Agenda. *African Journalism Studies 40*(4), 1–12.

Marwick, A. and E. Hargittai (2019). Nothing to Hide, Nothing to Lose? Incentives and Disincentives to Sharing Information With Institutions Online. *Information, Communication & Society 22*(12), 1697–1713.

Marx, V. (2013). Biology: The Big Challenges of Big Data. *Nature 498*, 255–260.

Mastor, W. (2017). The French Intelligence Act: The French Surveillance State. *European Public Law 23*, 707–722.

McClain, L. C. (1992). The Poverty of Privacy? *Columbia Journal of Gender and Law 3*, 119–174.

McGrath, J. (2004). *Loving Big Brother: Surveillance Culture and Performance Space*. Routledge: London.

McQuail, D. (1987). *Mass Communication Theory: An Introduction*. Sage Publications: London.

McQueen, F. (2017). Inside Emmanuel Macron's Draconian Anti-Terrorism Law. *The Conversation*, September 11, 2017. https://theconversation.com/inside-emmanuel-macrons-draconian-anti-terrorism-law-83834 (Accessed April 16, 2022).

McSherry, F. D. (2009). Privacy Integrated Queries: An Extensible Platform For Privacy-Preserving Data Analysis. In *Proceedings of the 2009 ACM SIGMOD International Conference on Management of Data*, pp. 19–30. ACM.

Melton, G. B. (1983). Toward Personhood For Adolescents: Autonomy and Privacy as Values in Public Policy. *American Psychologist 38*(1), 99—-103.

Melton, G. B. (1987). Children, Politics, and Morality: The Ethics of Child Advocacy. *Journal of Clinical Child Psychology 16*(4), 357–367.

Menges, L. (2020). Did the NSA and GCHQ Diminish our Privacy? What the Control Account Should Say. *Moral Philosophy and Politics 7*(1), 29–48.

Middlebrook, C. (2020). The Grey Area: Instagram, Shadowbanning, and the Erasure of Marginalized Communities. *SSRN*, February 17, 2020. http://dx.doi.org/10.2139/ssrn.3539721 (Accessed March 20, 2021).

Mitchell, N. J. and J. M. McCormick (1988). Economic and Political Explanations of Human Rights Violations. *World Politics: A Quarterly Journal of International Relations*, 476–498.

Mizutani, M., J. Dorsey, and J. H. Moor (2004). The Internet and Japanese Conception of Privacy. *Ethics and Information Technology 6*(2), 121–128.

Mlinek, E. J. and J. Pierce (1997). Confidentiality and Privacy Breaches in a University Hospital Emergency Department. *Academic Emergency Medicine 4*(12), 1142–1146.

Mohan, P., A. Thakurta, E. Shi, D. Song, and D. Culler (2012). GUPT: Privacy Preserving Data Analysis Made Easy. In *Proceedings of the 2012 ACM SIGMOD International Conference on Management of Data*, pp. 349–360. ACM.

Mohler, M., C. Campbell, K. Henderson, and B. Renauer (2022). Policing in an Era of Sousveillance: a Randomised Controlled Trial Examining the Influence of Video Footage on Perceptions of Legitimacy. *Policing and Society 32*(1), 52–70.

Moor, J. H. (1991). The Ethics of Privacy Protection. *Library Trends 39*(1 and 2, Summer/Fall 1990), 69–82.

Moore, A. D. (2003). Privacy: Its Meaning and Value. *American Philosophical Quarterly 40*(3), 215–227.

Mozur, P. (2018). A Genocide Incited on Facebook, With Posts From Myanmar's Military. *The New York Times*, October 18, 2018. https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html (Accessed April 16, 2022).

Mueller, J. and M. G. Stewart (2012). The Terrorism Delusion: America's Overwrought Response to September 11. *International Security 37*(1), 81–110.

Mullainathan, S. and J. Spiess (2017). Machine Learning: An Applied Econometric Approach. *Journal of Economic Perspectives 31*(2), 87–106.

Munir, S. (2018). Social Media and Shaping Voting Behavior of Youth: The Scottish Referendum 2014 Case. *The Journal of Social Media in Society 7*(1), 253–279.

Murumaa-Mengel, M., K. Laas-Mikko, and P. Pruulmann-Vengerfeldt (2015). "I Have Nothing to Hide": A Coping Strategy in a Risk Society. In A. Hepp, I. T. Trivundža, H. Nieminen, R. Kunelius, T. Olsson, E. Sundin, and R. Kilborn (Eds.), *Journalism, Representation and the Public Sphere*, Volume 195, pp. 195–298. Edition lumière: Bremen.

Nakashima, E., B. Gellman, and G. Miller (2013). New Documents Reveal Parameters of NSA's Secret Surveillance Programs. *The Washington Post*, August 21, 2013. https://www.washingtonpost.com/world/national-security/nsa-gathered-thousands-of-americans-e-mails-before-court-struck-down-program/2013/08/21/146ba4b6-0a90-11e3-b87c-476db8ac34cd_story.html (Accessed May 5, 2020).

Nesossi, E. (2015). Political Opportunities in Non-Democracies: The Case of Chinese Weiquan Lawyers. *The International Journal of Human Rights 19*(7), 961–978.

Newell, B. C., T. Timan, and B.-J. Koops (2018). *Surveillance, Privacy and Public Space*. Routledge: London.

Newell, P. B. (1995). Perspectives on Privacy. *Journal of Environmental Psychology 15*(2), 87–104.

News Wires (2009). US Support For Israel Prompted 9/11 Attacks, Says bin Laden Video. *France 24*, September 14, 2009. https://www.france24.com/en/20090914-us-support-israel-prompted-911-attacks-says-bin-laden-video- (Accessed May 30, 2021).

Niklas, J., K. Sztandar-Sztanderska, and K. Szymielewicz (2015). Profiling the Unemployed in Poland: Social and Political Implications of Algorithmic Decision Making. *Fundacja Paoptykon*, Raport.

Nyzio, A. (2022). Mity o skrzydlatym koniu. wokół debaty o pegasusie i kontroli operacyjnej. *Komentarze KBN UJ 4*(93), 1–16.

Ober, J. (2021). *The Polis as a Society: Aristotle, John Rawls, and the Athenian Social Contract*. Princeton University Press: Princeton.

Olen, H. (2019). A Pain-inducing Tilted Toilet Sounds Far-fetched. But No Wonder So Many People Were Livid. *The Washington Post*, December 20, 2019. https://www.washingtonpost.com/opinions/2019/12/20/pain-inducing-tilted-toilet-sounds-far-fetched-no-wonder-so-many-people-were-livid/ (Accessed April 16, 2022).

Ong, R. (2012). Online Vigilante Justice Chinese Style and Privacy in China. *Information & Communications Technology Law 21*(2), 127–145.

Parent, W. A. (1983). Recent Work on the Concept of Privacy. *American Philosophical Quarterly 20*(4), 341–355.

Parke, R. D. and D. B. Sawin (1979). Children's Privacy in the Home: Developmental, Ecological, and Child-Rearing Determinants. *Environment and Behavior 11*(1), 87–104.

Patil, H. K. and R. Seshadri (2014). Big Data Security and Privacy Issues in Healthcare. In *2014 IEEE International Congress on Big Data*, pp. 762–765. IEEE.

Peillon, A. (2016). *Résistance!* Média Diffusion: Paris.

Pernot-Leplay, E. (2020). China's Approach on Data Privacy Law: A Third Way Between the US and the EU? *Penn State Journal of Law and International Affairs 8*, 49–117.

Petronio, S., J. Sargent, L. Andea, P. Reganis, and D. Cichocki (2004). Family and Friends as Healthcare Advocates: Dilemmas of Confidentiality and Privacy. *Journal of Social and Personal Relationships 21*(1), 33–52.

Picardo, J., S. K. McKenzie, S. Collings, and G. Jenkin (2020). Suicide and Self-harm Content on Instagram: A Systematic Scoping Review. *PloS One 15*(9), e0238603.

Piketty, T. (2013). *Capital in the 21st Century*. Belknap Press: Boston.

Plunkett, D. and A. Burgess (2013). Conceptual ethics ii. *Philosophy Compass 8*(12), 1102–1110.

Posner, R. (1977). *The Economics of Law*. Little Brown: Boston.

Post, R. C. (1991 (2017)). Rereading Warren and Brandeis: Privacy, Property, and Appropriation. *Faculty Scholarship Series* (206), 125–158.

Powers, M. (1996). A Cognitive Access Definition of Privacy. *Law and Philosophy 15*(4), 369–386.

Prosser, W. L. (1960). Privacy. *California Law Review 48*(3), 383–423.

Pryce, D. (2008). Ghana's Conundrum: Obviating Electoral Fraud in the 2008 Presidential Election. *Modern Ghana*, January 22, 2008. https://www.modernghana.com/news/154344/ghanas-conundrum-obviating-electoral-fraud-in.html (Accessed April 16, 2022).

Pybus, J. (2019). Trump, the First Facebook President: Why Politicians Need Our Data Too. In C. Happer, A. Hoskins, and W. Merrin (Eds.), *Trump's Media War*, pp. 227–240. Palgrave Macmillan: Cham.

Quong, J. (2017). Contractualism. In A. Blau (Ed.), *Methods in Analytical Political Theory*, pp. 65–90. Cambridge University Press: Cambridge.

Rachel, L. and S. Amrani-Mekki (2012). Ad Hoc Information Report Data Protection: Redress Mechanisms and Their Use. Institut Français des Droits et Libertés (IFDL).

Rau, Z., K. M. Staszyńska, M. Chmieliński, and K. Zagórski (2018). *Doktryna Polaków: klasyczna filozofia polityczna w dyskursie potocznym*. Wydawnictwo Naukowe Scholar: Warszawa.

Rawls, J. (1971). *A Theory of Justice*. Belknap Press, Harvard University Press: Boston.

Raynes-Goldie, K. (2010). Aliases, Creeping, and Wall Cleaning: Understanding Privacy in the Age of Facebook. *First Monday 15*(1-4).

Ren, Y. (2018). The Theoretical System of Human Rights with Chinese Characteristics. *Chinese Studies 7*(3), 210–219.

Riezebos, P., S. A. De Vries, P. W. De Vries, and E. De Zeeuw (2011). The Effects of Social Media on Political Party Perception and Voting Behavior. In *Proceedings of the IADIS International Conference e-Democracy, Equity and Social Justice*, pp. 11–18. IADIS.

Riis, J. (1971). *How the Other Half Lives (1890)*. Reprint, Dover Publications: Mineola, New York.

Riis, J. A. (2018). *How the Other Half Lives. Studies Among the Tenements of New York*. Read Books Ltd: Redditch.

Rose, A. Z., G. Oladosu, B. Lee, and G. B. Asay (2009). The Economic Impacts of the September 11 Terrorist Attacks: A Computable General Equilibrium Analysis. *Peace Economics, Peace Science and Public Policy 15*(2), 217–244.

Ross, J. E. (2007). The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany. *The American Journal of Comparative Law 55*(3), 493–579.

Rossi, A. (2018). How the Snowden Revelations Saved the EU General Data Protection Regulation. *The International Spectator 53*(4), 95–111.

Rubenfeld, J. (1989). The Right of Privacy. *Harvard Law Review*, 737–807.

Rustad, M. L. and T. H. Koenig (2014). Wolves of the World Wide Web: Reforming Social Networks' Contracting Practices. *Wake Forest Laq Review 49*, 1431.

Rustad, M. L. and S. R. Paulsson (2004). Monitoring Employee E-mail and Internet Usage: Avoiding the Omniscient Electronic Sweatshop: Insights from Europe. *University of Pennsylvania Journal of Labor and Employment Law 7*, 829–904.

Salganik, M. J. (2019). *Bit by Bit: Social Research in the Digital Age*. Princeton University Press: Princeton.

Samonek, A. (2019). Violation of Privacy in Migration Control Decreases Citizens' Liberties and Public Accountability. *History Notebooks (Prace Historyczne) 2019*(146 (3)), 637–647.

Samonek, A. (2020). What Is the Future of European Cyber Security? Three Principles of European Cooperation and the Hybrid Joint Strategy of Cyber Defense. *Studies in European Affairs (Studia Europejskie) 24*(2), 43–60.

Samonek, A., D. Moeuthwil, B. Bornemann, G. Henry, S. Michaux, and A. Essende (2019). Credible, Engaging Media: Creating Smarter Media Consumers (Project Presentation). *Hack Belgium 2019* Presentation. https://prezi.com/p/ybpjfpb7guto/hack-belgium-2019/ (Accessed March 20, 2022).

Sandel, M. J. (1998). *Democracy's Discontent: America in Search of a Public Philosophy*. Harvard University Press: Boston.

Sanders, D. (1991). Collective Rights. *Human Rights Quarterly 13*, 368–386.

Sauer, N. (2019). French Counter-terrorism Targets Climate Activists. *The Ecologist*, April 4, 2019. https://theecologist.org/2019/apr/04/french-counter-terrorism-targets-climate-activists (Accessed May 30, 2021).

Schaefer, K., K. Atzwangerl, B. Wallner, and K. Grammer (1999). Urban Dwelling Features. *Collegium Antropologicum 23*(2), 369–378.

Schudy, S. and V. Utikal (2017). "You Must Not Know About Me" – On the Willingness to Share Personal Data. *Journal of Economic Behavior & Organization 141*, 1–13.

Schulze, M. (2015). Patterns of Surveillance Legitimization. The German Discourse on the NSA Scandal. *Surveillance & Society 13*(2), 197–217.

Schwartz, P. M. and K.-N. Peifer (2010). Prosser's" Privacy" and the German Right of Personality: Are Four Privacy Torts Better Than One Unitary Concept? *California Law Review*, 1925–1987.

Seidman, L. M. (1986). Public Principle and Private Choice: The Uneasy Case for a Boundary Maintenance Theory of Constitutional Law. *Yale Law Journal 96*, 1006–1059.

Sengupta, A. (2001). Right to Development as a Human Right. *Economic and Political Weekly*, 2527–2536.

Shalhūb-Kīfūrkiyān, N. (2015). *Security Theology, Surveillance and the Politics of Fear*. Cambridge University Press: Cambridge.

Shipler, D. K. (2011). *The Rights of the People. How Our Search for Safety Invades Our Liberties*. Vintage Books: New York.

Shklar, J. (1989). The Liberalism of Fear. In N. L. Rosenblum (Ed.), *Political Liberalism: Variations on a Theme*, pp. 21–38. University of Chicago Press: Chicago.

Simon, J. (2016). *Architecture and Justice: Judicial Meanings in the Public Realm*. Routledge: London, New York.

Smith, A. (2020). How To Register With the PSB, Police on Arrival in China. *China Scholar*, June 14, 2020. https://www.china-scholar.com/register-with-police-in-china-on-arrival/ (Accessed April 16, 2022).

Smith, H. J., T. Dinev, and H. Xu (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly 35*(4), 989–1016.

Smoschewer, F. (1930). *Das Persönlichkeitsrecht im Allgemeinen und im Urheberrecht*, Volume 3. Schriftenreihe der UFITA.

Snowden, E. (2019). *Permanent Record*. Pan Macmillan: London.

Soler, U. and M. Górka (2017). Populism as an Element of Security Policy. The 2016 Polish Anti-terrorism Law – A Case Study. *Sicurezza, Terrorismo e Società* (5), 69–87.

Solove, D. (2002). Conceptualizing Privacy. *California Law Review 90*(4), 1087–1155.

Solove, D. J. (2007). I've Got Nothing to Hide And Other Misunderstandings of Privacy. *San Diego Law Review 44*, 745–772.

Solove, D. J. (2011a). *Nothing to Hide: The False Tradeoff Between Privacy and Security*. Yale University Pres: New Havens.

Solove, D. J. (2011b). Why Privacy Matters Even If You Have Nothing to Hide. *Chronicle of Higher Education*, May 15, 2011. https://immagic.com/eLibrary/ARCHIVES/GENERAL/CHRON_HE/C110515S.pdf (Accessed April 16, 2022).

Solove, D. J. (2021). The Myth of the Privacy Paradox. *George Washington Law Review 89*, 1–51.

Song, T., C. Yi, and J. Huang (2014). Do We Follow Friends or Acquaintances? The Effects of Social Recommendations at Different Shopping Stages. In *International Conference on HCI in Business*, pp. 765–774. Springer: Dodrecht.

Spevack, E. (1997). American Pressures on the German Constitutional Tradition: Basic Rights in the West German Constitution of 1949. *International Journal of Politics, Culture, and Society 10*(3), 411–436.

Sprenger, P. (1999). Sun on Privacy: "Get Over It". *Wired*, January 26, 1999. https://www.wired.com/1999/01/sun-on-privacy-get-over-it/ (Accessed April 16, 2022).

Šram, Z. (2015). The Effects of Political Cynicism and National Siege Mentality on the Internalization of an Anti-European Sentiment. *International Journal in Management & Social Science 3*(11), 203–215.

Staerklé, C. and A. Clémence (2004). Why People are Committed to Human Rights and Still Tolerate Their Violation: A Contextual Analysis of the Principle-Application Gap. *Social Justice Research 17*(4), 389–406.

Stewart, M. G. and J. Mueller (2014). Cost-Benefit Analysis of Airport Security: Are Airports Too Safe? *Journal of Air Transport Management 35*, 19–28.

Stilwell, C. (2018). Information as Currency, Democracy, and Public Libraries. *Library Management 39*(5), 295–306.

Strahilevitz, L. J. (2010). Reunifying Privacy Law. *California Law Review*, 2007–2048.

Strahilevitz, L. J. (2012). Toward a Positive Theory of Privacy Law. *Harvard Law Review 126*, 2007–2048.

Szczygieł, M. (2014). *Gottland: Mostly True Stories From Half of Czechoslovakia*. Melville House: New York, London.

Szpor, G. (2000). Standardy ochrony prywatności w polskiej polityce społecznej na tle rozwiązań Unii Europejskiej. *Prace Naukowe/Akademia Ekonomiczna w Katowicach. Współczesna polityka społeczna Polski na tle Unii Europejskiej*, 37–52.

Tavani, H. T. and J. Moor (2001). *Privacy Protection, Control of Information, and Privacy-Enhancing Technologies*. Jones and Bartlett: Sudbury.

Taylor, N. (2002). State Surveillance and the Right to Privacy. *Surveillance & Society 1*(1), 66–85.

Taylor, R. B. (1988). *Human Territorial Functioning: An Empirical, Evolutionary Perspective on Individual and Small Group Territorial Cognitions, Behaviors, and Consequences*, Volume 8. Cambridge University Press: New York.

Teorell, J., M. Coppedge, S. Lindberg, and S.-E. Skaaning (2019). Measuring polyarchy across the globe, 1900–2017. *Studies in Comparative International Development 54*(1), 71–95.

Tettey, W. J. (2017). Mobile Telephony and Democracy in Ghana: Interrogating the Changing Ecology of Citizen Engagement and Political Communication. *Telecommunications Policy 41*(7-8), 685–694.

Thompson, C. (2007). The Visible Man: An FBI Target Puts His Whole Life Online. *Wired Magazine*, May 22, 2007. https://www.wired.com/2007/05/ps-transparency/ (Accessed April 16, 2022).

Thompson, J. (2002). *Taking Responsibility for the Past: Reparation and Historical Injustice*. Polity Press: Cambridge.

Thomson, T. (2019). In Front of the Lens: The Expectations, Experiences, and Reactions of Visual Journalism's Subjects. *Journalism & Communication Monographs 21*(1), 4–65.

Todolí-Signes, A. (2021). The Evaluation of Workers by Customers as a Method of Control and Monitoring in Firms: Digital Reputation and the European Union's General Data Protection Regulation. *International Labour Review 160*(1), 65–83.

Towadi, M., N. M. Kasim, R. Rumawi, and S. A. Tahir (2021). An Indication of China's Policy Towards Uighurs and its Implications by International Law Aspects. *Jambura Law Review 3*(1), 55–71.

Treacy, B. and M. Abrams (2008). A Privacy Law For China? *Complinet*, May 29 2008. https://www.huntonak.com/images/content/3/0/v2/3085/privacy_law_for_China.pdf, (Accessed April 16, 2022).

Tréguer, F. (2016). From Deep State Illegality to Law of the Land: The Case of Internet Surveillance in France. In *7th Biennial Surveillance & Society Conference (SSN 2016): Power, Performance and Trust*, pp. 1–72.

Trillò, T., R. Scharlach, B. Hallinan, B. Kim, S. Mizoroki, P. Frosh, and L. Shifman (2021). What Does# Freedom Look Like? Instagram and the Visual Imagination of Values. *Journal of Communication 71*(6), 875–897.

Trouille, H. (2000). Private Life and Public Image: Privacy Legislation in France. *International and Comparative Law Quarterly 49*, 199–208.

Twigg, R. (1992). The Performative Dimension of Surveillance: Jacob Riis' How the Other Half Lives. *Text and Performance Quarterly 12*(4), 305–328.

Tyner, J. A. (2018). *The Politics of Lists: Bureaucracy and Genocide Under the Khmer Rouge*. West Virginia University Press: Morgantown.

United Nations (2016). UN Experts Urge France to Protect Fundamental Freedoms While Combatting Terrorism. *United Nations News*, January 19, 2016. https://news.un.org/en/story/2016/01/520392-un-experts-urge-france-protect-fundamental-freedoms-while-combatting-terrorism (Accessed May 30, 2021).

Van Manen, M. and B. Levering (1996). *Childhood's Secrets: Intimacy, Privacy, and the Self Reconsidered*. Teachers College Press: New York.

Varian, H. R. (2014). Big Data: New Tricks for Econometrics. *Journal of Economic Perspectives 28*(2), 3–28.

Verble, J. (2014). The NSA and Edward Snowden: Surveillance in the 21st Century. *ACM SIGCAS Computers and Society 44*(3), 14–20.

Vidyasree, P., S. V. Raju, and G. Madhavi (2016). Desisting the Fraud in India's Voting Process Through Multi-modal Biometrics. In *2016 IEEE 6th International Conference on Advanced Computing (IACC)*, pp. 488–491. IEEE.

Von Gierke, O. (1895). *Deutsches Privatrecht: Bd. Allgemeiner Teil und Personenrecht*, Volume 1. Duncker & Humblot: Berlin.

Wagner, W. J. (1971). The Development of the Theory of the Right to Privacy in France. *Washington University Law Quarterly*, 45–72.

Wahl-Jorgensen, K., L. Bennett, and G. Taylor (2017). The Normalization of Surveillance and the Invisibility of Digital Citizenship: Media Debates After the Snowden Revelations. *International Journal of Communication 11*, 740–762.

Wallace, R. and H. K. Melton (2008). *Spycraft: The Secret History of the CIA's Spytechs From Communism to al-Qaeda*. Penguin: New York.

Wang, H. and X.-A. Lu (2007). Cyberdating: Misinformation and (Dis)trust in Online Interaction. *Informing Science 10*(18), 1–15.

Wang, K., B. C. Fung, and P. S. Yu (2005). Template-based Privacy Preservation in Classification Problems. In *Fifth IEEE International Conference on Data Mining (ICDM'05)*, pp. 466–473. IEEE.

Warren, S. D. and L. D. Brandeis (1890). Right to Privacy. *Harvard Law Review IV*(5), 193–220.

Warren, S. D. and L. D. Brandeis (1984). The Right to Privacy [The Implicit Made Explicit]. In F. D. Schoeman (Ed.), *Philosophical Dimensions of Privacy: An anthology*, pp. 75–103. Cambridge University Press: Cambridge.

Wasserstrom, R. A. (1984). Privacy: Some Arguments and Assumptions. *Philosophical Dimensions of Privacy: An Anthology 317*, 325–27.

Waters, S. (2018). The Effects of Mass Surveillance on Journalists' Relations with Confidential Sources: A Constant Comparative Study. *Digital Journalism 6*(10), 1294–1313.

Watts, J. and T. Branigan (2009). China Delays Launch of Internet Filter Green Dam. *The Guardian*, June 30, 2009. https://www.theguardian.com/world/2009/jun/30/green-dam-china-delay (Accessed May 30, 2021).

Weis, L. K. (2013). What Comparativism Tells Us About Originalism. *International Journal of Constitutional Law 11*(4), 842–869.

Westin, A. (1967). *Privacy and Freedom*. IG Publishing: New York.

Whittington, K. E. (2013). Originalism: A Critical Introduction. *Fordham Law Review 82*, 375–410.

Woeser, T. (2016). *Tibet on Fire: Self-immolations Against Chinese Rule*. Verso Books: London, New York.

Wolfers, A. (1952). "National Security" as an Ambiguous Symbol. *Political Science Quarterly 67*(4), 481–502.

Wright, D. (2011). Should Privacy Impact Assessments be Mandatory? *Communications of the ACM 54*(8), 121–131.

Wright, D. and R. Kreissl (2013). European Responses to the Snowden Revelations: A Discussion Paper. *IRISS, European Commission 43*, 27.

Wu, X., X. Zhu, G.-Q. Wu, and W. Ding (2013). Data Mining with Big Data. *IEEE Transactions on Knowledge and Data Engineering 26*(1), 97–107.

Wu, Y., T. Lau, D. J. Atkin, and C. A. Lin (2011). A Comparative Study of Online Privacy Regulations in the US and China. *Telecommunications Policy 35*(7), 603–616.

Wylie, C. (2019). *Mindf*ck: Cambridge Analytica And the Plot to Break America*. Random House: New York.

Yadav, S. and A. K. Singh (2013). A Biometric Traits Based Authentication System for Indian Voting System. *International Journal of Computer Applications 65*(15), 28–32.

Yang, J. (2008). Media Disclosure of Individual Privacy: A Proposed Framework for China. *East Asia Law Review 3*, 59.

Yao-Huai, L. (2005). Privacy and Data Privacy Issues in Contemporary China. In *The Ethics of Information Technologies*, pp. 189–197. Routledge: London.

You Yenn, T. (2018). *This Is What Inequality Looks Like*. Ethos Books: Singapore.

Zelikow, P. (2003). The Transformation of National Security: Five Redefinitions. *The National Interest* (71), 17–28.

Zenz, A. (2019). Brainwashing, Police Guards, and Coercive Internment: Evidence From Chinese Government Documents About the Nature and Extent of Xinjiang's "Vocational Training Internment Camps". *Journal of Political Risk 7*(7).

Zeronda, N. D. (2010). Street Shootings: Covert Photography and Public Privacy. *Vanderbilt Law Review 63*, 1131–1160.

Zhang, Z. and G. Negro (2013). Weibo in China: Understanding its Development Through Communication Analysis and Cultural Studies. *Communication, Politics & Culture 46*(2), 199–216.

Zheng, W. (2015). Detention of the Feminist Five in China. *Feminist Studies 41*(2), 476–482.

Zhou, B. and J. Pei (2008). Preserving Privacy in Social Networks Against Neighborhood Attacks. In *24th International Conference on Data Engineering*, Volume 8, pp. 506–515. IEEE.

Zhou, J., X. Lin, X. Dong, and Z. Cao (2014). PSMPA: Patient Self-Controllable and Multi-Level Privacy-Preserving Cooperative Authentication in Distributedm-Healthcare Cloud Computing System. *IEEE Transactions on Parallel and Distributed Systems 26*(6), 1693–1703.

Zhou, M. (2018). Fissures Between Human Rights Advocates and NGO Practitioners in China's Civil Society: A Case Study of the Equal Education Campaign, 2009–2013. *The China Quarterly 234*, 486–505.

Zhu, G. (1997). The Right to Privacy: An Emerging Right in Chinese Law. *Statute Law Review 18*, 208–214.

Zuboff, S. (2019). *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*. Profile Books: London.