

PRIVACY HARM: A DILEMMA IN DIGITAL AGE

by

Emine Nur İnce

**A Thesis submitted to the Graduate School of Social Sciences and
Humanities**

for the degree of

LL.M. in Public Law

Koç University

Fall 2019

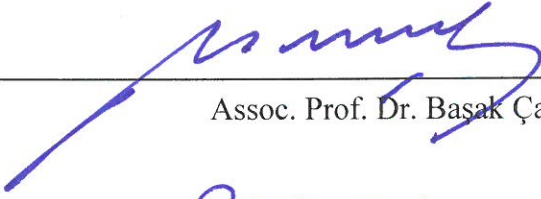
Koc University
Graduate School of Social Sciences and Humanities

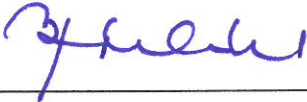
This is to certify that I have examined this copy of a master's thesis by

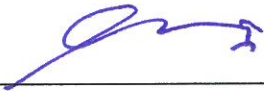
Emine Nur İnce

and have found that it is complete and satisfactory in all respects,
and that any and all revisions required by the final
examining committee have been made.

Committee Members:


Assoc. Prof. Dr. Basak Çalı


Prof. Dr. Bertil Emrah Oder


Asst. Prof. Dr. Mehmet Bedii Kaya

Date:

20.08.2019

Abstract

Privacy is often invoked as a shield when an intrusion occurs into people's private lives, and individuals are entitled to seek protection from this shield when they are harmed by the intrusion. This study argues that privacy harm requirement undermines the core of the right to private life and it prevents improvement and entrenchment of privacy rights. In the analysis, illustration of how two leading cultures have established and applied the privacy harm requirement is provided: jurisprudences of the United States and the European Court of Human Rights. The United States Constitution does not include any explicit provision on the protection of privacy rights, the Supreme Court determines whether there is a right to be protected by its case law. The European Court of Human Rights relies on the right to private life articulated by the European Convention of Human Rights, but still determines under what conditions privacy rights would be protected by its case law. Both of the courts employ privacy harm as a criterion to admit a case, and further to decide on the violation. However, in recent years, it is harder than ever to apply this criterion. This is because the privacy is not only an individual safeguard but also a societal value considering the mass surveillance and data collection by secret measures of governments. Persistence in traditional understanding of privacy harm does not make any contribution to improvement and entrenchment of international human rights. On the contrary, harm must be recognized as an inherent character of the privacy interferences without any demonstration. Abolishment of the privacy harm requirement would reconcile different implementations, solve the inconsistencies and contribute to the efforts for a uniformed international privacy standard.

Keywords: International public law, international human rights, privacy, privacy harm, mass surveillance

Öz

Mahremiyet yalnızca insanların özel hayatlarına bir müdahale olduğunda adeta bir kalkan olarak gündeme gelmektedir ve bireyler bu kalkanın korumasından sadece müdahaleden zarar gördüklerinde yararlanma hakkına sahiptir. Bu çalışma mahremiyet kaynaklı zarar şartının özel hayatın gizliliği hakkının özünü zedelediğini ve mahremiyet haklarının gelişmesini ve güçlenmesini engellediğini savunur. Analiz kısmında, öncü iki kültürün mahremiyet kaynaklı zarar şartını nasıl koyduğunu ve uyguladığını göstermektedir: Amerika Birleşik Devletleri içtihadı ile Avrupa İnsan Hakları Mahkemesi içtihadı. ABD anayasası mahremiyet haklarının korunması ile ilgili açık bir hüküm içermez, Anayasa Mahkemesi (Yüksek Mahkeme) korunacak hakkın varlığına karar vermektedir. AİHM, Avrupa İnsan Hakları Sözleşmesi'nde düzenlenen özel hayatın gizliliği hükmüne dayanır, fakat yine hangi koşullarda mahremiyetin korunacağına kendi içtihadıyla karar verir. Her iki mahkeme de gerek bir davanın kabul edilebilirliği gerekse ihlalin varlığına karar vermek için mahremiyet kaynaklı zarar koşulunu uygulamaktadır. Bununla birlikte, son yıllarda bu koşulu uygulamak her zamankinden daha zor hale gelmiştir. Çünkü devletlerin gizli tedbirleri ile yaygın şekilde gözetleme ve veri toplama faaliyetleri düşünüldüğünde, mahremiyet yalnızca bireysel bir koruma değil aynı zamanda toplumsal bir değerdir. Geleneksel mahremiyet yaklaşımında ısrarcı olmak uluslararası insan hakları hukukunun gelişimi ve güçlenmesine hiçbir katkı sunmamaktadır. Aksine, zararın, hiçbir kanıtı gerek duymaksızın her mahremiyet ihlalinin doğasında var olduğu kabul edilmelidir. Mahremiyet kaynaklı zararın ortadan kaldırılması farklı uygulamaların da önüne geçecek, çelişkileri giderecek, yeknesak uluslararası mahremiyet standardına ulaşma yolundaki çabalara katkı sağlayacaktır.

Anahtar kelimeler: uluslararası kamu hukuku, uluslararası insan hakları, mahremiyet, mahremiyet kaynaklı zarar, genel gözetleme

TABLE OF CONTENTS

- INTRODUCTION 1**
- BACKGROUND 1**
- PROBLEM STATEMENT AND RESEARCH QUESTION 3**
- SCOPE..... 4**
- METHODOLOGY 4**
- ORGANIZATION 5**
- CHAPTER I: CONTESTED BOUNDARIES OF THE RIGHT TO PRIVACY 7**
- A. AS A LEGAL CONCEPT 8**
- The Scope 9*
- B. AS HUMAN DIGNITY 11**
- C. AS AN INTERNATIONAL HUMAN RIGHT 13**
- CHAPTER II: JUDICIAL DEVELOPMENT OF PRIVACY HARM..... 18**
- A. EVOLUTION OF THE PRIVACY HARM IN THE UNITED STATES..... 19**
- 1. Recognition of Privacy Rights and Privacy Harm..... 20*
- 2. Privacy Harm in the Present 23*
- B. EVOLUTION OF THE PRIVACY HARM IN EUROPE: EUROPEAN COURT OF HUMAN RIGHTS V. THE COURT OF JUSTICE OF THE EUROPEAN UNION 31**
- 1. Jurisprudence of the European Court of Human Rights on the Harm Requirement 31*
- 2. The Court of Justice of the European Union..... 42*
- 3. Privacy Harm in the Present 44*
- CHAPTER III: CONTESTED BOUNDARIES OF PRIVACY HARM 48**
- A. CATEGORIZATION OF PRIVACY HARM 49**
- B. PRIVACY HARM RECOGNIZED BY THE UN 57**
- C. COUNTER ARGUMENTS 61**
- CHAPTER IV: THE CASE FOR ABOLISHING PRIVACY HARM 67**
- CONCLUSION 72**
- BIBLIOGRAPHY 75**
- TABLE OF CASES..... 80**

INTRODUCTION

Background

It has been six years since the famous revelations by Edward Joseph Snowden, a former Central Intelligence Agency of the United States (CIA) agent, that the National Security Agency (NSA) was collecting the telephone records secretly.¹ This was shocking news when first published in 2013². Immediately after the revelations, Max Schrems filed a complaint to the Irish Data Protection Authority and asked for prohibition of transfer his personal data by Facebook Ireland to Facebook Inc. in the US. Since the EU law governs that cross-border data sharing, the case came before the Court of Justice of the European Union (CJEU). The question put to the CJEU was whether the US ensures equivalent protection. CJEU delivered a seminal judgement invalidating the regime between the EU and US.³

This case has helped the European Union to have a reputation as an activist for the right to privacy, in particular in comparison to the United States (US) and the Council of Europe. The EU Charter of Fundamental Rights indeed includes rights that aims at data protection⁴ whereas the European Convention of Human Rights only has a general provision for the protection of private life. The EU also has General Data Protection Regulation which solely focusses on data protection⁵. Instead, privacy rights in the US and under the ECHR are primarily shaped by court decisions. The Supreme Court of US indirectly admits that there exists constitutional protection for the right to privacy; however, it also infers a requirement of privacy harm to

¹ The Guardian first reported the revelations in June 2013. Glenn Greenwald, NSA collecting phone records of millions of Verizon customers daily, 6 June 2013, available at <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>

² After Snowden, there have been several data breach scandals. 2018 was the pick. Bennett Cyphers, Gennie Gebhart, and Adam Schwartz, Data Privacy Scandals and Public Policy Picking Up Speed: 2018 in Review, The Electronic Frontier Foundation, 31 December 2018, available at <https://www EFF.org/tr/deeplinks/2018/12/data-privacy-scandals-and-public-policy-picking-speed-2018-year-review>

³ Maximillian Schrems v Data Protection Commissioner, C-362/14, 6 October 2015

⁴ Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, also *see infra* note 54.

⁵ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

establish a legal claim. European Court of Human Rights, on the other side, requires applicants to be victims of an alleged violation.

Yet, the requirement of demonstration of privacy harm has become a problematic doctrine, considering how much complicated personal data protection has become. Yet, the courts have been slow to catch up with technological developments. The US Supreme Court resists the admission of cases without privacy harm despite all the academic efforts for reconceptualization of privacy. The US Supreme Court and federal courts employ several doctrines to admit a case in this regard. The Supreme Court introduced ‘reasonable expectation of privacy’⁶, ‘specific present objective harm’⁷, ‘injury in fact’⁸, ‘*de minimis* intrusions’⁹. Objectively reasonable likelihood of being affected by surveillance measures was defended before the Court but failed.¹⁰ The harm must be concrete and particular at the same time, even if the alleged violation is a statutory violation.¹¹

The ECtHR finds certain cases admissible as an exception to the victim status principle without an actual privacy harm. Yet, it still has drawbacks in the analysis of these exceptionally admissible cases. The ECtHR admits abstract claims if the applicants are potentially affected.¹² However, it has also unclear decisions where it does not admit a case based on the wide margin of appreciation of the states.¹³ ECtHR itself is aware of conflicts in its jurisprudence, and of distinguished approaches regarding the victim status even after it admits the exceptional abstract reviews.¹⁴

⁶ *Katz v. United States*, 389 U.S. 347 (1967)

⁷ *Laird v. Tatum*, 408 U.S. 1 (1972). It is also introduced as ‘Article III standing doctrine’.

⁸ *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). Injury must be ‘concrete and particularized’, and also ‘actual or imminent’.

⁹ *United States v. Knotts*, 460 U.S. 276 (1983)

¹⁰ *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013). It also implied that chilling effect is not recognized as privacy harm.

¹¹ *Spokeo, Inc. v. Robins*, 578 U.S. ____ (2016)

¹² *Klass and Others v. Germany*, no. 5029/71, 6 September 1978.

¹³ In *Weber and Saravia v. Germany*, application no. 54934/00, 29 June 2006, the Court decided inadmissibility of the case where it should have decided under the merits of the case. The margin of appreciation is recognized, in terms of privacy interferences, to assess the necessity of the measure considering the balance between individual harm and societal harm.

¹⁴ *Roman Zakharov v. Russia*, no. 47143, 4 December 2015.

In order to guide judicial organs, and to improve human rights discussions, academy puts an effort to analyze privacy harm in more specific scheme. They intend to initiate at least a change in interpretation of modern privacy by judges. Some argue for categorizing harmful activities¹⁵, and harmful consequences¹⁶, and some others offer more general parameters¹⁷. Nevertheless, they are criticized for staying much more in theory.¹⁸

In 2018, the only binding international instrument, Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108) was updated so as to refer to “human dignity” and “societal value” in the preamble. It only regards data processing, does not clarify exactly what the safeguards should be, prepared with an exception clause as ECHR, and establish a committee with consultative powers.¹⁹

Problem Statement and Research Question

There is neither a clear definition of the privacy nor a specific determination of its scope. International human rights law instruments do not regulate right to privacy in detail. Most of the time, judges embrace textualism in applying and interpreting the law, which causes even more difficulty in modern privacy cases. The US Supreme Court and the European Court of Human Rights present the most obvious examples of this problem. The Constitution of the US and the European Convention on Human Rights do not properly guide the courts on how to implement the law in accordance with the modern realities and necessities. For this reason, privacy rights are determined and protected depending on the judge-made rules. In this context, both of these courts compel the applicants to prove their loss or damage to have a privacy claim. Yet, the constant pace of technological developments and the ability to survey, collect data on individuals by public and private organs, put the doctrine of privacy harm under considerable pressure. In the light of these new and emerging developments, this thesis asks whether the demonstration of privacy harm is necessary to have a legal claim for the right to privacy. In response, the thesis argues that it is indeed possible to omit the harm criterion out of the admission requirements for the privacy claims in the context of the ongoing digitalization of

¹⁵ Daniel J Solove, *A taxonomy of privacy*, 154 U. PA. L. REV. 477(2005).

¹⁶ DANIEL J SOLOVE, *UNDERSTANDING PRIVACY* 174-179 (Harvard University Press. 2008).

¹⁷ M Ryan Calo, *The Boundaries of Privacy Harm*, 3 IND LJ (2011).

¹⁸ Ann Bartow, *A feeling of unease about privacy law*, 155 U. PA. L. REV. PENNUMBRA (2006).

¹⁹ *infra* note 55.

social, economic and political life. Instead of protecting rights, the privacy harm requirement creates the dissonance between technological developments and privacy protection. Theory and practice of privacy rights need to correspond to transformation and digitalization of modern world. In this context, the significant and innovative characteristic of this study is that it defends total removal of the harm criterion by analyzing the conflicts in and of the founding legal cultures and practices together with the most recent developments.

Scope

Primary focus of the thesis is on the establishment and development of the privacy harm requirement by the US Supreme Court and the European Court of Human Rights, and how the Court of Justice of the European Union departs from them in this matter. Therefore, the thesis concerns international public law jurisprudences. It is interested in how technological developments intersect with the constitutional and human rights to privacy in the public law, and primary through a comparative case law analysis. At this point, it may only refer to regulations under private law with a particular comparison, but it indeed excludes any other national, regional or international laws in the private realm.

Methodology

This thesis has been prepared in the international public law context, and its approach is supposed be deemed as human rights approach. It provides how this requirement has been applied in American and European jurisprudences, two major legal cultures where the privacy rights protection is challenged by the technology. The establishment, and recent application, of the privacy harm criterion is explained by selected cases from the Supreme Court of the United States and the European Court of Human Rights.

For the US, case law is discussed in a chronological order from the first case which the Supreme Court actually accepts the constitutional protection of right to privacy, and the first case the Supreme Court lays down the privacy harm criterion. Other cases are selected according to their determinant roles in shaping the behavior of the Supreme Court, such as the cases which the Supreme Court strictly requires privacy harm, and other conflictive cases afterwards.

Under the ECtHR section, a chronological order of case law is followed in order to illustrate when the first Court departs from the privacy harm criterion, and when it decides otherwise. The most referred cases are analyzed, which may be called “precedents” of the ECtHR, regarding their determinant roles in creating the fundamental principles of the Court and their conflictive characters with each other.

Particular cases, which are related to the analyzed ECtHR cases with direct references, from jurisprudence of the Court of Justice of the European Union are also included in order to show how other legal contexts approach the harm of privacy violation. CJEU is compared with both US Supreme Court and the ECtHR, and symbolizes a reformist model.

Besides from the comparison of case laws, this study also covers the literature specifically on the privacy harm as well as the recent developments at the level of the United Nations that call for a radical thinking of the concept of privacy harm. Yet, the thesis also includes objections to the rethinking of privacy harm. Discussion of counter arguments allows for strengthening the argument, to make the research more persuasive, and to respond well to possible resistance of status quo against the privacy reform in international human rights.

Organization

The first chapter focuses on the concept of privacy under the legal philosophy of two western cultures and also under the international instruments. The chapter intends to show that privacy may be associated with individual interest or human dignity, but either way, it is a protected value under international human rights law. However, that protection is so weak that it is designed only in general terms. This handicap indeed constitutes the ground for redesigning privacy in international level with uniformed understanding and application considering the universal nature of the right. It also reveals why privacy is left to judge-made law which requires privacy harm as discussed by the following chapters.

In the second chapter, development on the privacy rights by the judge-made laws in two different legal cultures is examined with the precedent cases establishing the privacy harm criterion and the exceptional rules. The aim is to show how the courts struggle to build a consistent jurisprudence on the privacy harm criterion. In this regard, this chapter provides the development of the criterion and discusses the conflictive results, and constitutes the ground

for arguing the inconvenience of the criterion by all means. In this regard, the chapter also reveals how radical the change of privacy cases from past to present, and correspondingly how much we need the revolution in privacy protection by eliminating the harm criterion.

In the third chapter, responses from academia to that need of revolution are presented. The chapter reflects the theoretical aspect of the subject matter. Since the privacy, and also the privacy harm, is a philosophical concept, theoretical contentions and offers must be considered in reshaping the international protection. The academic criticism of the judgments, and offers by the scholars to enhance privacy protection are to contribute to embracing an innovative perspective in achieving the privacy revolution. The United Nations efforts presented in this chapter constitute a model initiative for how to begin to grasp the picture comprehensively, and it also presented as a confirmation of the need for privacy revolution at the international level. The counter-arguments, lastly, are given for indicating how kind of resistance such revolution may confront.

The final chapter reiterates that privacy models need to be reconciled but not through a synthesis but a revolution in the international level. This revolution will bring a uniformed understanding and application of privacy protection, and it is possible only with the total removal of the privacy harm requirement from the courts. It entails redesigning the international protection of the right to privacy in detail. This goal will be reached firstly by raising social awareness, then international cooperation, and finally judicial and political sincerity. This chapter is intended to underline the main argument of the study, to reflect the comprehensive perspective, and to suggest the ultimate idea of privacy revolution.

CHAPTER I: CONTESTED BOUNDARIES OF THE RIGHT TO PRIVACY

Introduction

This chapter is regarded privacy concept in the philosophical framework for a better understanding of what is the value behind it. The concept suffers from the lack of a singular definition. Neither the theoretical discussions nor the legal instruments could achieve an agreed concept.

In legal philosophy, some associate privacy with individuality. It resembles a personal zone where no one else is allowed to enter. On the other hand, it is associated with human dignity. It implies a societal value to be protected. The former approach is observed in the American culture whereas the latter is embraced by the European culture.

At the international level, it is a fundamental human right but not an absolute right. In certain circumstances, articulated by the respective instrument, it may be limited or interfered.

A. As A Legal Concept

Philosophical, political and legal discussions have not reached any certain settled definition of the concept of "privacy". There is still controversy about the exact meaning and scope of privacy as a legal concept. Nevertheless, most of the theorists agree on its value. In legal philosophy, the term has usually been associated with confidentiality. For a more clarified understanding, it is something provides us a safe zone clear from any interference.²⁰ This safe zone is firstly implied in Aristotle's distinction of public and private spheres. Privacy is symbolized in that distinction as a separator from governmental domain.²¹

Despite the lack of single and uniformed definition, efforts to conceptualize privacy are noteworthy for understanding its importance and protection. Among these efforts, the famous article by Warren and Brandeis of 1890 has led the way for further discussions. This article is mostly referred for the definition of privacy as a "right to be left alone"²², but their article contains further significant points. In their definition, spiritual nature of a person with the feelings and intellect are included, and they observe even the right to life as the right to enjoy life.²³ The base of this idea is the principle of "inviolable personality".²⁴

Another prominent work from the last century focuses on the different kinds of privacy rather than pure theoretical conceptualizing of a pure notion of privacy. In 1960, William Prosser identified privacy issues as four main types: (1) intrusion, (2) public disclosure, (3) misrepresentation, (4) appropriation.²⁵ He basically illustrated which types of violations were likely to be prevented. There should be, according to him, intrusion to one's intimacy or intimate relations, or revelation of confidential facts, or distortion of oneself in the public eye, or seizure of one's image. The classification method brought another dimension and a significant contribution to privacy discussions. However, Prosser has been criticized by scholars that he

²⁰ Judith DeCew, Privacy In Stanford Encyclopedia of Philosophy at 2 (Stanford, CA Metaphysics Research Lab, Stanford University Spring 2015 ed. 2015).

²¹ Id. at. 4.

²² Louis D. Brandeis Samuel D. Warren, *The Right to Privacy*, HARVARD LAW REVIEW 193(1890).

²³ Id.

²⁴ Id. at. 205.

²⁵ William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 391-401 (1960).

made difficult the reconciliation of the term²⁶, and that he does not provide an inclusive manner.²⁷

As opposed to this method of examining privacy, some scholars have defended the necessity of a singular concept. In 1976, Jeffrey Reiman explained the pattern of that camp, and he criticized certain approaches.²⁸ He believed that there is a unique character of privacy, and the right to privacy is directly related to "personhood" regardless of whether a person on a street or in confinement. His emphasis on the individuality, with or without being a part of society, constitutes an essential part of the efforts for theoretical interpretation of the term. He further conceptualized privacy as a "social ritual by means of which an individual's moral title to his existence is conferred" which is "a precondition of personhood".²⁹ The mere existence of a person, therefore, is the fundamental element which would compound different theories relying on social involvement or not. Clearly, privacy is such a notion in legal theory and legal philosophy that protects persons' entitlement to exist from the broadest perspective.

The Scope

As well as the definition as a legal concept of privacy, efforts for determining the scope of protection presents divergences. Having established that privacy is related to intimacy and an inner sphere, certain scholars state that not only confidential information is the object of privacy rights but also honor, religious, philosophical or political thoughts, economic situation, health or sex information, communications and place of home and work.³⁰

Similar to the classification method of Prosser, there have been attempts to put the scope of privacy into different categories such as information privacy, communication privacy, and even psychological privacy.³¹ In general, this method for determining the scope reveals certain

²⁶ See Edward J Bloustein, *Privacy as an aspect of human dignity: An answer to Dean Prosser*, 39 NYUL REV., 994 (1964).

²⁷ See DeCew, 6. 2015.

²⁸ Jeffrey H Reiman, *Privacy, Intimacy, and Personhood*, PHILOSOPHY & PUBLIC AFFAIRS 26(1976).

²⁹ Id. at. 39.

³⁰ Bernardo Perrián, *The Origin of Privacy as a Legal Value: A Reflection on Roman and English Law*, 52 AMERICAN JOURNAL OF LEGAL HISTORY 183, 187 (2012).

³¹ PRISCILLA M. REGAN, *LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY* (University of North Carolina Press. 1995).

distinctions that scholars tend to rely on: (1) border between the public and private spheres, (2) incentive of the claim, (3) personal decisions, and (4) informational privacy.³² In other words, there are no concrete limits around the privacy zone, rather it is perceived depending on one of these parameters. Likewise, there is no single detector to decide what falls under which category.

A relatively exhaustive list may be put three main aspects that (a) respect to privacy, (b) communication, and (c) respect to home; where under the first heading there would be (1) surveillance, (2) data privacy, (3) autonomous decisions on own body, (4) identity, (5) confidential relationships, (6) honor and reputation.³³

On the other side, there is a radical view that right to privacy, indeed, covers only informational privacy. Every issue arising out of the privacy-related claims should fall under the informational privacy of an individual to be entitled to protection. In this sense, privacy claims on the physical integrity of body are irrelevant.³⁴ They should rather be examined under the concept of autonomy. Simply, this sort of claim does not rely on privacy but possession of the body. Additionally, claims about the privacy of personal places are irrelevant themselves without any personal information. A particular place cannot be accepted and protected as private unless it is used to harm someone's informational privacy. Privacy of the places can only be protected under informational privacy.³⁵

Although it is not that radicalized so far, there is growing domination of informational privacy which individual autonomy also depends on.³⁶ The essential concern must be, anyway, to provide sufficient protection for individuality and personal integrity in all categories of this scope. In this manner, legal concept and scope of privacy are often associated with dignity as a social value as well as protection for individuality.

³² COLIN J BENNETT, *THE PRIVACY ADVOCATES: RESISTING THE SPREAD OF SURVEILLANCE* 3 (Mit Press. 2008).

³³ WALTER KALIN, et al., *THE LAW OF INTERNATIONAL HUMAN RIGHTS PROTECTION / THE LAW OF INTERNATIONAL HUMAN RIGHTS PROTECTION* 382-392 (Oxford University Press. 2009).

³⁴ R.L. David Hughes, *Two Concepts of Privacy*, 31 *COMPUTER LAW & SECURITY REVIEW* 527, 534 (2015).

³⁵ *Id.* at, 535.

³⁶ DANIEL J SOLOVE & PAUL SCHWARTZ, *INFORMATION PRIVACY LAW* (Wolters Kluwer Law & Business. 2014).

B. As Human Dignity

Privacy is conserved in social norms which shape our obligation to respect each other. Violation of these norms is assumed detrimental by its very nature since it is deemed as an attack to the self. At this point, once more we may need to split the privacy into two sub-concepts as individual autonomy and individual dignity, because such attack to the self is offensive against individual dignity but not necessarily against autonomy. Autonomy might be perceived as entitlement to identity whereas dignity depends on those norms behind the respect in society which are fundamental for civilization. This is why any violation of those norms is damaging inherently.³⁷

On the contrary, it has been argued that roots of the privacy are based on liberal individualism and promotes individuation rather than virtuous society.³⁸ The core of privacy consists of a preserved area of autonomous development and liberty against interventions of anyone.³⁹

These two distinct approaches appear separately in American and European cultures. In terms of legal philosophy, American law seems to follow the individual-centered pattern while European embraces dignity-based privacy. James Whitman summarizes this situation in a literary way as "gravitational orbit of liberty values" versus "orbit of dignity".⁴⁰

However, "inviolable personality" of Warren and Brandeis, from the American literature, could be and has already been interpreted as a reference to dignity.⁴¹ They defended that spiritual nature should be taken into account including emotions but there had not have any remedy for the violation of honor, unlike the Roman law.⁴² Roman law protects privacy through *actio iniuriarum* which means by an action against the perpetrator is required to introduce privacy right.⁴³ Even though there is not an explicit reference in the law, Roman privacy protection is

³⁷ Robert C Post, *Three Concepts of Privacy*, 89 GEO. LJ 2087, 2092-2093 (2001).

³⁸ BENNETT, 9. 2008.

³⁹ Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance. (2018).

⁴⁰ James Q Whitman, *The two western cultures of privacy: Dignity versus liberty*, 113 YALE LJ 1151, 1162 (2003). See also Post, GEO. LJ, 1162 (2001).

⁴¹ KHIARA M BRIDGES, *THE POVERTY OF PRIVACY RIGHTS* 154 (Stanford University Press. 2017).

⁴² Samuel D. Warren, *HARVARD LAW REVIEW*, 198 (1890).

⁴³ Perrián, *AMERICAN JOURNAL OF LEGAL HISTORY*, 190-199 (2012).

deemed to represent a safeguard for social value of honor.⁴⁴

Today, at the individual level, it is observable that people concern about privacy only when it is threatened. Then it starts to matter what and how threats their privacy. The source of those threats, such as mass surveillance and other modern technological ways of intrusions, does not belong to the individual level.⁴⁵ Indeed, the mere collection of personal information should be deemed degrading irrespective of unauthorized access. This degrading nature may be derived only from the assumptions made, or to be made, about the subject.⁴⁶

The significant nuance is the fact that scholars may point the social aspect of privacy in order only to show its effects on individual privacy.⁴⁷ Instead, the concentration must be on how privacy is "constitutive" of society⁴⁸. Focusing solely on the 'liberal self' as the subject of privacy issues implies the capacity of self-determination and autonomy which may lead the conclusion that loss of privacy does not affect this inherent capacity.⁴⁹ Simply, conceptualizing the matter only in the individual level, infringement of privacy would not necessarily cause any harm or vitiate the inherent autonomy of the individual. However, the real subject of privacy, beyond the liberal self, is socially constructed from preexistent cultural basis. In this regard, what privacy protects is highly dynamic that individualist approach cannot be sufficient to comprehend.

Furthermore, the absence of privacy protection mechanism is regarded as the hallmark of oppressive regimes and social control.⁵⁰ Political and legal contexts shape and force the privacy mechanism, assign protectable legal value to it, and determine the scope of it. Therefore, without sufficient constitutional guarantees designating a proper political model of government as a "respectful guardian of individual liberties", there would be the risk of totalitarian tendency of governments.⁵¹ Judicial interpretations and social awareness are the crucial factors against that slide towards an oppressive regime. Both of them are dynamic and involved in an

⁴⁴ Id. at. 192-193.

⁴⁵ REGAN, 23. 1995.

⁴⁶ BRIDGES, 162. 2017.

⁴⁷ REGAN. 1995. 26.

⁴⁸ See Solove, U. PA. L. REV., 487 (2005).

⁴⁹ Julie E Cohen, *What privacy is for*, 126 HARV. L. REV., 1905 (2012).

⁵⁰ BRIDGES, 153. 2017.

⁵¹ Perrián, AMERICAN JOURNAL OF LEGAL HISTORY, 201 (2012).

interaction with each other that can provide leverage against that risk.⁵²

C. As An International Human Right

The Universal Declaration of Human Rights (UDHR) of 1948 guarantees international rights and freedoms for every human being. In the very first sentence of the preamble, it begins by that “recognition of the inherent dignity” is the foundation of freedom, justice and peace. It indeed seems as a reconciliation of freedom and dignity centered theories at first sight. In the preamble, rule of law is shown as the safeguard of international human rights against any tyranny and oppression, which also seems to include dignity-based theory's social component of privacy.

Article 12 of the UDHR explicitly articulates that:

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

Article 12 of the UDHR has a unique significance that the right to privacy was recognized for the first time even when no constitution in the world had such a general guarantee for privacy. In this manner, the international human rights law is ahead of constitutional law.⁵³

European Convention of Human Rights (ECHR) in 1950, referred to the UDHR at the beginning of its preamble, and afterward emphasized the freedom and rule of law behind the Convention. Interestingly, despite the association with dignitary approach, the preamble of the ECHR does not contain the word “dignity” or “honor”.

In Article 8, ECHR gives two separate paragraphs, the first being an integral recognition, and the second on the exceptions. It reads as:

⁵² See Post, GEO. LJ, 2094 (2001).

⁵³ It articulated privacy rights for the first time human rights to be internationally protected. See <https://www.un.org/en/universal-declaration-human-rights/index.html>

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

There is an indication that the right to privacy would not be unlimited and absolute. It is rather derogable. It can be restricted according to the wording of this article. In the second paragraph, the grounds of justifications for privacy interferences are presented. Since the privacy is regarded broadly, interpretation and application of the European Court of Human Rights become determinant for the scope of protection.

After sixteen years, in 1966, the International Covenant on Civil and Political Rights (ICCPR) was adopted and entered into force in 1976. Similar to the UDHR, its preamble refers to inherent dignity. Article 17 of the ICCPR is as follows:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

The integral articulations in these three international instruments have been argued vague and unconsciously prepared without considering potential implications.⁵⁴ CCPR General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honor and Reputation by the Office of the High Commissioner for Human Rights (OHCHR) was adopted in 1988. It is an inseparable explanatory text for understanding Article 17 of the ICCPR. National laws, according to the

⁵⁴ Oliver Diggelmann & Maria Nicole Cleis, How the right to privacy became a Human Right, 14 Human Rights Law Review 441(2014). 457.

General Comment, must signify the specific conditions of government interference, together with the aim of it and the competent authorities.

International human rights law was formed in more detail under Organisation for Economic Co-operation and Development (OECD) in 1980⁵⁵. The Convention for the Protection of Individuals with regard to the Processing of Personal Data (Convention 108) was adopted after the OECD Privacy Guidelines, in 1981, by the Council of Europe. It was a huge step because the Convention 108 is the first binding document at the international level, which is open to member and non-member states. OECD Privacy Guidelines and Convention 108 had an impact on national legislations in the 1980s.⁵⁶

Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights (The Siracusa Principles) was adopted in 1984. It sets forth the fundamental framework against abuse of derogable rights.⁵⁷ Even though it seems as it has been ignored in the current discussions, the OHCHR refers to The Siracusa Principles for better understanding and application of privacy protection mechanisms in its Report on the Right to Privacy in the Digital Age.⁵⁸

In 2000, the European Union introduced its Charter of Fundamental Rights. Its preamble underlines human dignity and rule of law as well. It articulates privacy in two separate articles:

⁵⁵ The OECD Privacy Guidelines, which was updated in 2013, covers basic principles of privacy protection mechanisms, available at <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>

⁵⁶ COLIN J BENNETT & CHARLES D RAAB, *THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE* 75 (Routledge. 2003). Convention 108 is updated on June, 2018. In the modernized text, preamble includes the necessity to secure human dignity, and emphasized the societal dimension of right to personal data. Provisions are also rephrased in an elaborative way. Modernised version is available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf; the table showing both of the versions and changes is available at <https://rm.coe.int/cahdata-convention-108-table-e-april2018/16808ac958>.

⁵⁷ Impact of these principles can be seen in international courts including European Court of Justice and European Court of Human Rights. *See* R HOVEN VAN GENDEREN, *PRIVACY LIMITATION CLAUSES: TROJAN HORSES UNDER THE DISGUISE OF DEMOCRACY: ON THE REDUCTION OF PRIVACY BY NATIONAL AUTHORITIES IN CASES OF NATIONAL SECURITY AND JUSTICE MATTERS* 64-70 (2016).

⁵⁸ N Pillay, *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*, Human Rights Council. Twenty-Seventh Session. A/HRC/27/37 (2014).

Article 7 - Everyone has the right to respect for his or her private and family life, home and communications.

Article 8 - 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.

The Charter provides data protection as a human right per se for the EU⁵⁹ apart from the ECHR. Following the growing concern and guarantees on data protection as a human right, international efforts have been increased not only in international public law but also in international private law regarding particularly the transfer of personal data.⁶⁰

In international human rights law, therefore, states are obliged to protect privacy as both an individual freedom from interference and human dignity in accordance with the rule of law. It is accepted that states have the duty to respect, protect and fulfill the requirements of international privacy rights.⁶¹

In sum, there is no consensus on what privacy means and what it protects in legal philosophy. Two western cultures embrace different approaches. Apart from this discussion, international protection is provided for privacy as a fundamental right. This protection is mostly by the broad

⁵⁹ In the European Union Law, the Data Protection Directive (95/46/EC) had been the principal instrument governing the issue from 1995 until the General Data Protection Regulation in 2018. There had also been former Article 286 of the Treaty Establishing the European Community (EC Treaty) until the Lisbon Treaty replaced it with Article 16 in 2009. Together with this recognition of the Charter, right to data protection is considered as a separate fundamental right in the EU law.

⁶⁰ Asia-Pacific Economic Cooperation embraced its own framework in 2005, available at <https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework>. European Union and the United States recently started to follow the EU-US Privacy Shield, which has replaced the previous Safe Harbor Principles, in 2016, available at https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en#eu-us-privacy-shield.

⁶¹ See KALIN, et al., 392-395. 2009.

provisions without any specific determination regarding the scope. However, it is recognized that privacy is a derogable right, and states may interfere under certain conditions.



Chapter II: JUDICIAL DEVELOPMENT OF PRIVACY HARM

Introduction

Privacy protection is articulated by framework provisions in the laws. Therefore, criteria for the legal claims against privacy intrusions have been developed by the judicial bodies. In the United States, even the constitution does not include explicitly the right to private life. The Supreme Court recognizes the right inferring from the constitutional amendments. European Court of Human Rights, on the other hand, interprets what the general protection laid down in the Convention covers. Considering the improvement in international human rights discussions, the amount and complexity of the cases, these two courts presents the leading jurisprudence on the privacy rights. Both of them requires privacy harm for a case to be admissible. They do not admit abstract reviews or class actions for privacy rights in principle.

However, this requirement does not fit with the genuine issues any more. Nature of the privacy breaches does not need any consequence or effect per se, also in this digital era, the means for interference to privacy have been rapidly changed that people may not even know whether they are being watched. Persistence on the privacy harm compels judicial bodies to find contemporary responses to permanent problems, to balance societal harm and individual harm as if they are opposed to each other in privacy matters, and to render confusing decisions.

A. Evolution of the Privacy Harm in the United States

In the United States of America, the constitution does not explicitly articulate privacy right as a human right in the first place. Bill of Rights⁶², has indirectly paved the way for the US Supreme Court to hear privacy cases, such as the First Amendment including freedom of religion, speech, the press, and assembly, and the Fourth Amendment including unreasonable search and seizure⁶³. These two amendments only regulate several issues at constitutional level, which may be affiliated with privacy. The legal concept, anyhow, is developed under tort law in general, and by primitive steps of the doctrine as firstly reflected by the famous article of Warren and Brandeis "The Right to Privacy" in 1890.⁶⁴

The article is mostly concerned with the publication of personal information, especially images, under general tort law. The legal context is important when the perpetrator is another person, not the state. In case of an infringement, the authors suggest applying redress for the mental suffering, or the law of defamation, or the law of property. If there are not any actual damages under these laws, they offer the action of slander and libel.⁶⁵ The article apparently is a keystone for the evolution of privacy discussions at least in different forms. It is also significant for reflecting the nature and philosophy of privacy then. It has been playing a leading role for US doctrine which is presented in the next chapter.

In 1960, a prominent scholar William L. Prosser "translated"⁶⁶ that article to the new century's US law. Basically, judicial approach in the US has been shaped by this theory of Prosser that scrutinizes the issue under four main categories inferred from "right to be left alone"⁶⁷

⁶² 12 amendments were introduced in 1789, ten of them were adopted and have been called 'Bill of Rights'. They regulate basic human rights in the US. *See* <https://www.whitehouse.gov/about-the-white-house/the-constitution/>

⁶³ *Id.*

⁶⁴ Samuel D. Warren, *HARVARD LAW REVIEW*, (1890).

⁶⁵ *Id.* at. 213, 219.

⁶⁶ Prosser is regarded to have translated the former leading article in a way more compatible with the US legal system so that many of the States could adopt the similar approaches. *See* Paul M Schwartz & Karl-Nikolaus Peifer, "Prosser's" Privacy" and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?, 98 *California Law Review* 1925, 1986 (2010).

⁶⁷ Warren, *supra* note 4.

introduced by Warren and Brandeis.⁶⁸ Intrusion (I), public disclosure of facts (II), false light in the public eye (III), and appropriation (IV) are the main four headings of Prosser.⁶⁹ Since the infringement here still is a tort, it is suggested that special damages need not be proven, just as libel and slander.⁷⁰ Prosser's study is similar to the former article regarding the consequences of privacy intrusions.

In 1964, "An Answer to Dean Prosser" was published by E. J. Bloustein, which criticized Prosser that he excludes non-tort context.⁷¹ He stresses the need of comprehensive perspective rather than congeries of rules, a clear sense for judicial consensus, and analysis of the interest in privacy disputes.⁷² Invasion of privacy should be separated from other torts for relying on human dignity.⁷³ This perspective has invited scholars to a more sophisticated framework than tort law. Nevertheless, disagreement among the scholars would never end while the US Supreme Court used to struggle with the privacy claims against the governments in the previous century.

1. Recognition of Privacy Rights and Privacy Harm

Griswold v. Connecticut in 1965⁷⁴ is accepted as the establishment of the privacy right for the first time⁷⁵ in the US, because the constitution does not cover the right explicitly. Connecticut law did not allow any kind of drug to prevent pregnancy. The US Supreme Court found this law unconstitutional and invalidated it. The Court inferred the right to privacy from the constitutional amendments. *Griswold* has been the symbol of the constitutional right to privacy in the US, and recognition of the right to protection from governmental intrusion.

Then it was followed by *Katz v. United States* in 1967⁷⁶. *Katz* was accused of illegal transfer

⁶⁸ Saleh Sharari & Raed SA Faqir, Protection of Individual Privacy under the Continental and Anglo-Saxon Systems: Legal and Criminal Aspects, 5 Beijing L. Rev. 184, 187 (2014).

⁶⁹ Prosser, CAL. L. REV., 391-401 (1960).

⁷⁰ Id. at, 409.

⁷¹ Bloustein, NYUL REV., 994 (1964).

⁷² Id. at, 963.

⁷³ Id. at, 1003.

⁷⁴ *Griswold v. Connecticut*, 381 U.S. 479 (1965)

⁷⁵ KRIANGSAK KITTICHAISAREE, PUBLIC INTERNATIONAL LAW OF CYBERSPACE 55 § 32 (Springer. 2017).

⁷⁶ *Katz v. United States*, 389 U.S. 347 (1967)

of information. The accusation was directed to him by eavesdropping a public phone used by the suspect. Katz challenged that evidence. The discussions were concentrated on whether the protection includes wiretap a public phone booth. At the appeal, the challenge was not accepted for the lack of physical intrusion to the phone booth itself. The Supreme Court elaborated on the issue and developed the principle that 'reasonable expectation of privacy' must be considered to decide if the suspect's right is violated. Katz was entitled to the protection without a physical intrusion.⁷⁷

After these first steps of the 1960s, *Laird v. Tatum* in 1972⁷⁸ brought a new dimension to the privacy discussions. The case filed against a surveillance program in the army, and the Court stated that plaintiffs could not address any direct harm to themselves but the mere existence of the surveillance system. There should be an actual harm or a threat of specific future harm they experienced. The Court emphasized,

*"...allegations of a subjective chill are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm; the federal courts established pursuant to Article III of the Constitution do not render advisory opinions..."*⁷⁹

Therefore, according to the Court, there should be either 'specific present objective harm' or 'a threat of specific future harm'. Otherwise, the decision would be an advisory opinion of the judiciary, which is out of its competence according to Article III of the Constitution on the main function of the judicial branch⁸⁰.

Chilling effect, briefly, was found too abstract to substantiate the claim before the Court. It reminded previous cases regarding chilling effect that "constitutional violations may arise from the chilling effect of governmental regulations"; however, in none of them chilling effect had

⁷⁷ 'Reasonable expectation of privacy' has been employed by the Supreme Court as a parameter since then, and in doctrine it has been referred as 'Katz test'. Scholars have read the decision as expanding the protection of Fourth Amendment on warrantless search. See KITTICHAISAREE, 56. 2017.

⁷⁸ *Laird v. Tatum*, 408 U.S. 1 (1972)

⁷⁹ 408 U.S. 1, 14 (1972)

⁸⁰ Article III of the US Constitution regulates the judicial structure, power and competence within three sections. See <https://constitutioncenter.org/interactive-constitution/articles/article-iii>

arisen merely from the knowledge of the individuals regarding the certain activity.⁸¹ *Laird* has led the discussions on chilling effect of surveillance, and has established explicitly the 'Article III standing doctrine' as an admissibility criterion. Afterward, the Supreme Court expanded on Article III standing that it requires "injury in fact" which is "concrete and particularized" as well as "actual or imminent".⁸² Federal courts accepted the decision as precedent in similar cases.⁸³

Another dimension was unveiled by *United States v. Bailey* in 1980.⁸⁴ In the investigation of the alleged illegal laboratory, a beeper was installed in certain chemical materials. The Court applied the *Katz* test of a reasonable expectation of privacy. The government defended that just installing beeper could not be deemed as an offensive action because the intrusion is too minor. Although the Court had decided many times that an intrusion may be *de minimis* if it does not violate the legitimate expectation of privacy⁸⁵, in *Bailey* it decided otherwise. The Supreme Court seems to have struggled in establishing consistent and sustainable opinion with this doctrine.⁸⁶ It is still vague how much is too much?⁸⁷

Legal foreseeability and proportionality have been tentative due to the complicated approach

⁸¹ *Baird v. State Bar of Arizona*, 401 U. S. 1 (1971); *Keyishian v. Board of Regents*, 385 U. S. 589 (1967); *Lamont v. Postmaster General*, 381 U. S. 301 (1965); *Baggett v. Bullitt*, 377 U. S. 360 (1964). 408 U.S. 1, 11 (1972)

⁸² *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). Then followed by *Doe I v. Individuals*, 561 F Supp. 2d 249, 257; *Doe v. Chao*, 540 US 614 (2003); *Fed. Aviation Admin v. Cooper*, 132 S. Ct. 1441, 1441 (2012) which federal courts and Supreme Court generally demand that privacy plaintiffs show not just harm, but "concrete", "fundamental", or "special" harm. For further see Margot E Kaminski, *Standing After Snowden: Lessons on Privacy Harm from National Security Surveillance Litigation*, 66 DEPAUL L. REV. 413, 415 (2016).; JEFFREY L VAGLE, *BEING WATCHED: LEGAL CHALLENGES TO GOVERNMENT SURVEILLANCE* 51-70 (NYU Press. 2017).

⁸³ Some federal courts had been waiting for *Laird* to decide on pending cases. Afterwards, they recognized that mere existence and knowledge of surveillance based governmental activities would mean a subjective chilling effect, and that it would not be sufficient to substantiate the claim under Article III standing doctrine. See VAGLE, 108. 2017.

⁸⁴ *United States v. Bailey*, 628 F.2d 938, 940 (6th Cir. 1980)

⁸⁵ See e.g. *United States v. Dubrofsky*, 581 F.2d 208, 211 (9th Cir. 1978); *United States v. Moore*, 562 F.2d 106, 112 (1st Cir. 1977); 35 U.S. 926, 98 S.Ct. 1493, 55 L.Ed.2d 521 (1978); *United States v. Knotts*, 460 U.S. 276 (1983)

⁸⁶ In *United States v. Jones*, 132 S. Ct. 945 (2012), the US Government relied on this jurisprudence of the Court; however, the Court ruled otherwise.

⁸⁷ Jeffrey Brown, *How Much Is Too Much: The Application of the De Minimis Doctrine to the Fourth Amendment*, 82 MISS. LJ, 1097-1099 (2013).

by the judiciary. Federal courts and the Supreme Court had to decide on the facts of the case each time by assessing the concrete harm, specific harm, negligible harm, etc. We see the decision is delivered sometimes under Article III standing, sometimes as *de minimis*, and from *Lujan v. Defenders of Wildlife* explicitly as ‘injury-in-fact’⁸⁸.

2. Privacy Harm in the Present

From the beginning of this millennium, we can call it information age or technological era, the privacy issues have been increased dramatically. Privacy happens to be extremely serious to protect as it becomes vulnerable to various attacks and threats. The more information protection becomes the fundamental ground of the claims, the harder it becomes to apply traditional behavior of the courts. Violation of privacy rights does not cause particular injury anymore. This is simply because of the intangible and immaterial nature of the breaches. Considering the internet speed and other connections via electronic means, as well as the variety of technological tools for tracking people regardless of with time or place, it gets more difficult to determine how serious and immediate danger an individual could be in.

Consequently, the center of discussions also becomes confidentiality of personal information which leads us to modern data collection through advanced surveillance systems. The concern is now, not only being watched but also the knowledge of gathering and preserving one's information for retainment or further use. At this point, Article III standing doctrine cannot require any injury-in-fact any more, since such injury would be "imminent without being physically present".⁸⁹

Clapper v. Amnesty

In 2013, *Clapper v. Amnesty International USA*⁹⁰ led a clear and crucial discussion of modern times privacy. Press members, lawyers, and non-governmental organizations challenged an act on electronic surveillance of non-U.S. citizens outside of the country for intelligence. They claimed that the act was facially unconstitutional. Plaintiffs stated that there is an objectively

⁸⁸ *Supra* note 66.

⁸⁹ Seth F Kreimer, *Spooky Action at a Distance: Intangible Injury in Fact in the Information Age*, 18 U. PA. J. CONST. L. 745, 792 (2016).

⁹⁰ *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013)

reasonable likelihood of being intercepted according to the law. To avoid such advanced surveillance, they also claimed that they had to take costly measures.

The claim was not found convincing. The District Court decided that there was no standing for the challenge but only an abstract subjective fear without proof of being monitored. It asserted that to establish Article III standing, an injury must be concrete, particularized, and actual or imminent. A threat should also be certainly impending. The Court of Appeals reversed the decision that there are a standing and a reasonable fear of injury or costs to prevent such injury. The Supreme Court, however, held that potential future surveillance would not constitute an injury required by Article III standing. It should be certainly impending. A previous decision by the Court of Appeal was found to have improperly accepted such standing that such decision would water down the essential requirements of Article III. The Court, based on *Lujan* and *Laird*, reversed the decision.

Clapper has certain implications. First, if the claimants could prove that they were exposed to an interception, it would give them standing before the Court. Interception of communication, therefore, could be deemed as an injury-in-fact. Second, indirectly, the governmental activity of collection and retainment of personal information could be also sufficient for injury. Considering the reason of the Court and analysis of the Court of Appeal, that would be a reasonable fear from ongoing surveillance. Third, chilling effect is still not be enough itself without an actual breach or illegal collection of data.⁹¹

Surveillance activities by governments carry a serious risk, but with *Clapper*, the Supreme Court reversed a major judgment opposed to traditional harm theory. In another significant case of 2007, *American Civil Liberties Union v. National Security Agency*⁹², the Supreme Court did not seem to change its behavior. In *ACLU*, the Appeal Court decided not to grant standing against National Security Agency, for the plaintiffs could not prove themselves being the targets of the challenged surveillance program. The Supreme Court had dismissed the application for appeal without any comment.

⁹¹ Scholars contend that even after an actual breach there will be a chilling effect. So, it should have been recognized by the Supreme Court as a privacy harm anyway. *See* Kaminski, *DEPAUL L. REV.*, 422-438 (2016).

⁹² *ACLU v. NSA*, 493 F.3d 644 (6th Cir. 2007).

Persistence of the Court in harm theory is critical for surveillance-related conflicts, because in most of the time government activities are, by definition, secret. Neil M. Richards asserts that after *Clapper* we must rethink how ignorant we are on this topic, except for science fiction dystopias.⁹³ The drawback is the lack of perception on how and why surveillance activities may constitute a violation itself in theory and practice according to him.⁹⁴ At the level of theory, chilling effect, which might be called intellectual surveillance since it may violate intellectual privacy, prevent exercising civil liberties including communicating in political and social contexts. It further creates discrimination and coercion. At the practical level, mass surveillance and secret surveillance including internet records can be carried out without authorization. It must be declared totally illegal, regardless of public or private surveillance⁹⁵. The harm thereof would not be excluded under the constitutional standing doctrine.

Klayman v. Obama

In the same year with *Clapper*, a federal court rendered a judgment on bulk collection of metadata by the United States. In *Klayman v. Obama*⁹⁶, District Court of Columbia decided in favor of the plaintiffs, based on the *Katz* test of reasonable expectation. The Court also referred to *Clapper* for sufficiency to demonstrate a certainly impending injury but concluded that the case was not the same, since the plaintiffs could prove that their information had been collected. The Court explained why it does not exactly follow the precedents that "the almost-Orwellian technology enabling the government to store and analyze metadata is unlike anything that could have been conceived in 1979".⁹⁷ Non-governmental organizations and other activists have continued to challenge mass surveillance and bulk collection programs and to challenge the constitutionality of the underlying legislations. However, federal courts could not achieve a

⁹³ Neil M Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934(2013).

⁹⁴ *Id.* at, 1935.

⁹⁵ Traditionally, surveillance notion is associated with government, but Richards reiterates that in our age of "liquid surveillance", government and non-government surveillance are strongly connected to each other. *See id.* at, 1940-41. His point is also significant for reconciliation of privacy concepts from public and private law, particularly constitutional law and tort law. This is relevant because when the actor is a real person or a private company it would be considered under tort law while if it is a public authority the violation would have a constitutional character. Unfortunately, courts tend to distinguish public and private surveillance as well. *See Kaminski*, DEPAUL L. REV., 431 (2016).

⁹⁶ *Klayman v. Obama*, 957 F. Supp. 2d 1 (2013)

⁹⁷ 957 F. Supp. 2d 1, 49 (2013).

common point on Article III standing doctrine regarding surveillance measures.⁹⁸

Spokeo, Inc. v. Robins

In 2016, The Supreme Court had to confront with another standing conflict in *Spokeo, Inc. v. Robins*⁹⁹. Spokeo had a people-search engine, a website providing personal information about individuals such as contact information and current professional situations. Robins was one of those individuals whose information was provided incorrectly through the website. He filed a lawsuit on his own and others' behalf who were suffering similar inaccuracies.

The district court dismissed the case based on the standing doctrine. The appeal court reversed the decision that there was a particular injury in fact. The Supreme Court found the analysis of the appeal court incomplete on the concrete and particularized injury. The Court highlighted the requirement of both -concrete-and-particular- at the same time, where the appeal court had focused only on the second -particular-. Concreteness, according to the Supreme Court, must not be overlooked. A concrete injury must be *de facto*, which means to exist in reality, even though it is not directly tangible. However, intangible harms are also subject to Article III standards. Accepting intangible harms does not imply to entitle a person to vindicate his right; in other words, Article III standing doctrine entails a concrete injury even for a statutory violation. After these explanations, the Court rendered that in this case incorrect information about a person would not be proven harmful itself. After all, interestingly the Court remained silent on the judgment of the appeal court on whether Robins have the standing, but only remanded the case.

⁹⁸ In *ACLU v. Clapper* 14-42 (2d Cir. 2015), American Civil Liberties Union challenged the National Security Agency's metadata collection program. ACLU claimed unconstitutionality of the call-recording program of NSA which constitutes metadata illegally. The case was discussed also together with Klayman and Clapper that courts are not sure how to deal with standing issues. *See* Benjamin Wittes, Standing Confusion in *Obama v. Klayman*, <https://www.lawfareblog.com/standing-confusion-obama-v-klayman>. In *Wikimedia Foundation v. NSA/CSS*, No. 15-2560 (4th Cir. 2017), ACLU filed a case based on unconstitutionality of NSA's mass surveillance through internet. The case was dismissed by the first instance but reversed partially by the Court of Appeals. ACLU was the only one having a standing before the Court. These surveillance cases apparently seem to be hard to substantiate standing under Article III. The scholars concern that unless the judiciary step back from strict application of Article III standing doctrine, most of the potential subjects may never be able to challenge such programs, activities or legislations. *See* VAGLE, 151. 2017.

⁹⁹ *Spokeo, Inc. v. Robins*, 578 U.S. ____ (2016)

With *Spokeo*, the Supreme Court gave the signal that it would follow the established injury-in-fact doctrine after all. It was clarified that a bare procedural violation without any concrete harm would not meet the injury-in-fact requirement. Considering the behavior of the federal courts after *Spokeo*, it is obvious that the doctrine needs 'adaptation' for each case.¹⁰⁰ In this regard, *Spokeo* cannot be said to have provided more protection to individual claims for privacy before the courts. Instead, it might be regarded to ensure federal courts to dismiss those claims. The Supreme Court should definitely be criticized for not resolving the skepticism over standing discussions in privacy cases.¹⁰¹ *Spokeo* was a chance to elaborate on the relationship between the concreteness of harm and substantial risk of harm¹⁰². It may have brought an innovative turn to the harm discussions, but the Court remained silent. The decision is condemned to create rather an ambiguity in this regard.¹⁰³

In re Zeppos.com, Inc. Customer Data Security Breach Litigation

In 2018, the US Court of Appeals delivered *In re Zeppos.com, Inc. Customer Data Security Breach Litigation*¹⁰⁴ concerning the stolen personal data of millions. Most of them could not prove that their stolen data was used or they suffered any other concrete harm. Their standing was denied by the district court. It was argued by the defendants that future harm is not sufficient for the standing, but the appeal court admitted that there was a substantial risk of misuse of stolen data. Therefore, the distinct approaches of federal courts have become more obvious.¹⁰⁵

Carpenter v. United States

¹⁰⁰ After *Spokeo*, inconsistency of the federal courts continued. See Kaminski, DEPAUL L. REV., 418-419 (2016). The judgements were found confusing and conflicting with *Spokeo*. Especially *Perlin v. Time Inc.*, No. 2:2016cv10635 - Document 27 (E.D. Mich. 2017), and *In Re: Nickleodeon Consumer Privacy Litig.*, No. 15-1441 (3d Cir. 2016).

¹⁰¹ *Id.* at, 420.

¹⁰² In contrary to the general approach, there were cases held that future risk of harm gives standing to the plaintiff. See *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010).

¹⁰³ The Supreme Court should have rendered more precise and clear approach on the discussion from *Clapper*, but created even more ambiguity. See Daniel J Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 Tex. L. Rev. 737, 742 (2017).

¹⁰⁴ 9th Cir. 2018

¹⁰⁵ For a sample table of other conflictive decisions, see Daniel Solove, *In re Zappos: The 9th Circuit Recognizes Data Breach Harm*, 9 April 2018, available at <https://teachprivacy.com/in-re-zappos-9th-circuit-recognizes-data-breach-harm/>

Most recent case under this section is *Carpenter v. United States*¹⁰⁶ regarding the mobile phone location history. The conflict was about accessing location history through mobile phones. A suspected was charged with several crimes who claimed that seizure of his records violated the rule of warrantless search and seizure under the Fourth Amendment rights. The claim was denied by the district court, then upheld by the appeal court. It was held that there was no reasonable expectation of privacy since the location information was first shared with the wireless carriers, and such business records would not be under the Fourth Amendment.

The Supreme Court firstly underlines the Fourth Amendment which safeguards the privacy against arbitrary invasions. Then, it states that the case law would not be applied directly to the case at hand, since the concern was about a digital storage of personal data. It implies that the privacy expectations in this age may exceed what precedents have anticipated. *United States v. Knotts*¹⁰⁷ is referred regarding the use of a beeper for tracking a vehicle, where reasonable expectation of privacy was denied. It is noted there is a clear distinction between rudimentary tracking and other surveillance methods. In more recent surveillance case, *United States v. Jones*¹⁰⁸, a different approach was employed, since every moment was tracked for a longer-term. These two cases are given to represent the first set of decisions on the expectation of privacy in physical tracking.

In the second set, the main point is the information shared with others by the data subject. The Court reiterates the third-party principle that there is no legitimate expectation of privacy if the information is shared voluntarily. This "third-party principle" is introduced in *United States v. Miller*¹⁰⁹ and *Smith v. Maryland*¹¹⁰. In *Miller*, the claim was rejected relying on the assumption that financial information was not under the control of the plaintiff but the bank. It was accepted that the commercial transactions of the plaintiff were not confidential information of him, but an instrument belonging to the relevant bank. In *Smith*, this principle was applied to a telephone company.

¹⁰⁶ *Carpenter v. United States*, 585 U.S. ____ (2018)

¹⁰⁷ 460 U.S. 276 (1983)

¹⁰⁸ 132 S. Ct. 945 (2012)

¹⁰⁹ *United States v. Miller*, 425 U.S. 435 (1976)

¹¹⁰ *Smith v. Maryland*, 442 U.S. 735 (1979)

In *Carpenter*, a new phenomenon is tracking the phone signals. Although the wireless carrier may correspond to the third party as in *Smith* and *Miller*, the Court does not extend the rule. Instead, considering the unique circumstances at hand such as technological tracking methods, the Court decides to accept legitimate expectation of privacy. In contrast to the first set of decisions, it refers to *Katz* that constitutional protection may cover personal information even in an area accessible to the public. Further, the third-party principle is associated with the sharing information, but *Smith*, *Miller* or *Carpenter* was not concerning only the act of sharing. In any case, sharing location through a mobile phone is not the same with others literally.

Carpenter is in the news heading ‘The Supreme Court Just Greatly Strengthened Digital Privacy’¹¹¹ and evaluated as an update of privacy protection in the digital era. Upon the decision, there would be no room for the government to obtain personal information from mobile phones -service providers indeed- without a warrant. That device apparently has not changed only our daily lives and social dynamics but also created a great effect on the law and order. It might be the most obvious victory against the governmental activities before the Supreme Court.

In sum, existing precedents and principles do not seem to fit with the modern issues which highly advanced technologies involved. We see in *Clapper*, fear, and anxiety were found too speculative, and in *Spoeko*, injury-in-fact was still applied; then, how much fear would be enough to claim a right to private life before the federal courts of the US? There is still not any convincing response.

If a mere procedural violation without a concrete harm could not be precluded by the judiciary, then where can we put the Fourth Amendment right to be free from arbitrary searches? It can be deduced that an officer may freely delve into one's bag or mobile phone without causing any harm. If this is accepted as a harmless violation and not precluded by the law, including case law, then we must also accept the legality of evidence found incidentally. The chain of deductions and possible scenarios could be endless. This would destroy the legal philosophy behind the constitutional right to privacy, including the Fourth Amendment rights against warrantless search and seizure.

¹¹¹ Louise Matsakis, <https://www.wired.com/story/carpenter-v-united-states-supreme-court-digital-privacy/>

Leaving the federal courts, or even the Supreme Court, on their own to find temporary solutions for each case is not a sustainable way to guarantee privacy protection. It is not too difficult to guess what the future judgments would do: presentation of the distinct approaches and probably debatable justification for their decision according to the facts of the instant case. It will be debatable because privacy issues are getting more sophisticated day by day that in the near future there may be even greater conflicts without any 'concrete and particularized harm'. Even existing cases or daily life problems with privacy protection are complicated enough to entail a novel approach. All the courts will also need reasonable justification for each time which should be incoherence with the jurisprudence, and should ensure foreseeability of the case law while delivering sufficient and proper judgments.

Regarding the third-party principle of the Supreme Court, we can see how privacy issues could vary depending on the context. The principle is based on the first action of the individual to share information with another private actor. Voluntarily shared information, as assumed by the principle, can be used by public authorities irrespective of the reasonable expectation of privacy. This is another major problem regarding the standing doctrine, in addition to the unwillingness to recognize privacy harm.

The Supreme Court has to put more effort to harmonize its case-law according to this millennium's facts. Immediate recognition of inherent privacy harm is necessary for the abolishment of both strict standing doctrine and public-private division.¹¹² Even though *Carpenter* has been a sample case for adaptation of existing rules, it only represents one dimension of the multi-dimensional issue. The jurisprudence of the US¹¹³ federal courts including the Supreme Court is still far away from comprehensive, consistent, coherent, sustainable and uniformed doctrine.¹¹⁴

¹¹² *Supra* note 79.

¹¹³ Another common law country Canada follows a similar path with the US. There is no singular legal context and implementation of privacy law. Three contexts are applicable: constitutional, regulatory and tort law. Reasonable expectation of privacy and minimum intrusion doctrines are almost the same. Recently, the courts struggle to decide elaborately on complicated matters as well, but they cause a confusion while trying to stick with the established rules. *See* Michael Ryan, *Persona Non Data: How Courts in the EU, UK and Canada are Addressing the Issue of Communications Data Surveillance vs. Privacy Rights* (2016).; Hughes, *Computer Law & Security Review*, (2015).

¹¹⁴ In detailed summary and critics of judicial approach *see* Solove & Citron, *Tex. L. Rev.*, 739-750 (2017).

B. Evolution of the Privacy Harm in Europe: European Court of Human Rights v. the Court of Justice of the European Union

1. Jurisprudence of the European Court of Human Rights on the Harm Requirement

Totally different framework operates in Europe. European Court of Human Rights (ECtHR) interprets the rules outlined in the European Convention on Human Rights (ECHR). The main provisions are articulated under Article 8 on the right to privacy. Before that article, an application must meet the admissibility criteria under Articles 34 and 35. The criteria determine if a claim may be brought before the Court. Article 35 articulates the criteria for admissibility in general, but the discussions arise rather from the wording of Article 34:

“The Court may receive applications from any person, nongovernmental organisation or group of individuals claiming to be the victim of a violation by one of the High Contracting Parties of the rights set forth in the Convention or the Protocols thereto. ...”

Victim status is the first and foremost requirement related to the applicant. ‘Victim’ implies a person directly and indirectly affected by the alleged unlawful action.¹¹⁵ The requirement also entails a prohibition for complaints *in abstractio* and *actio popularis*. It means that the Court does not authorize itself for abstract reviews of domestic legislations or practices under the Convention. Likewise, applicants must convincingly submit that a violation is, or will be, occurred to their rights.¹¹⁶

After the admissibility, the Court determines whether the application is substantiated under Article 8:

- “1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except

¹¹⁵ SARL du Parc d’Activités de Blotzheim v. France, no. 72377/01, § 20, 11 July 2006; Vallianatos and Others v. Greece [GC], nos. 29381/09 and 32684/09, ECHR 2013

¹¹⁶ Klass and Others v. Germany, no. 5029/71, 6 September 1978, Series A no. 28; Georgian Labour Party v. Georgia, no. 9103/04, ECHR 2008; Burden v. the United Kingdom [GC], no. 13378/05, ECHR 2008;

such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”¹¹⁷

Private life, family life, home, and correspondence are the four main headings inferred from Article 8. The main purpose of the article is to protect private and family life, home, and correspondence from arbitrary interference.¹¹⁸ Physical and moral integrity, identity-related matters, data protection, and surveillance may be put under private life in general. In the exceptional circumstances recognized by the second paragraph of Article 8, the Convention legitimizes interference by the public authorities if the interference is in accordance with the law, and necessary in a democratic society for national security, safety or economic well-being. If it is for providing the law and order, for the protection of health or morals, or other people's rights, the interference is also justified.

The unique character of the privacy violations, especially in the recent times, leaves the ECtHR in the line between strict interpretation of the victim requirement and evasion or at least adapting the rule to hear the claims.

¹¹⁷ Right to private life, under Article 8, has a broad scope. In his classification, van der Sloot gives 10 categories for ECtHR jurisprudence of Article 8 and reduces them to 5 to simplify: (1) physical and psychological integrity, (2) family and relations, (3) communication, (4) home and location, (5) honor and reputation, (6) data protection, (7) surveillance, (8) environment, (9) personality and identity, (10) property and economical privacy. First, bodily and psychological integrity includes sexual and medical issues, issues regarding the personal identity and reputation, healthy environment etc. Relational privacy, secondly, includes all the cases regarding personal relationship with others. Third is the informational privacy which consists of surveillance by all means, interception of communication, and data gathering. Fourth is the locational privacy which concerns private area of an individual. Finally, economical privacy, which is introduced by van der Sloot, covers the enjoyment of property or other financial rights. He puts this fifth heading for the cases concerning destruction of homes, loss of property or assets, being subjected to special tax obligations due to the family or relational matters, deprivation of certain opportunities because of sexual choices. *See* Bart van der Sloot, *Where Is the Harm in a Privacy Violation*, 8 J. Intell. Prop. Info. Tech. & Elec. Com. L. 322, 22-23 (2017).

¹¹⁸ In *Odièvre v. France* [GC], no. 42326/98, 13 February 2003, the Court clarified that state parties undertake not only to abstain from an arbitrary interference but also to adopt measures to assure respect for private life. Article 8, therefore, imposes positive and negative obligations to the states, which are not covered explicitly by the wording of the provision. *See* § 40. A few years later, the Court underlined the same in *Evans v. The United Kingdom* [GC], no. 6339/05, § 75, 10 April 2007. An interesting aspect of the case is the discussion of a conflict between two private persons but also the legislation concerning the public interest. *See* § 73-74

Klass v. Germany of 1978¹¹⁹, presents the first and foremost decision delivered by the Court with a deliberate discussion on the surveillance measures. The applicants challenged government surveillance contrary to the Convention. Actually, what they challenged was not the authorization for surveillance but the omission of notifying the subjects and of remedies against the execution. The applicants were not yet aware of any measure applied to them.

It is emphasized that such unawareness would not prevent the Court to admit the case, potentially affected people could also claim their rights. Besides, alleged unlawful legislation might affect all the citizens unaware of being targeted without any subsequent notification. The victim status, therefore, accepted by the Court exceptionally, without proving exposure to a measure; consequently, continued to review the challenged legislation's compatibility with the Convention.¹²⁰

The Court, therefore, examined the interference, and the justifications of the interference. The mere existence of a legislation on the interception of communication would be an interference, according to the Court, since all the users of the communication services would be affected. However, it is necessary to determine whether there was any justification for the interference under the second paragraph of Article 8. The exceptions provided by the second paragraph, on the other side, is supposed to be interpreted narrowly. An interference would only be acceptable if it is in accordance with the law and strictly necessary for democratic order.

Individual measures must comply with the specific conditions set out by the respective national law. National security, the aim of the government's interceptions in the instant case, is one of the acceptable justifications. However, the government has to guarantee during the whole implementation that measures are remained within what is strictly necessary in a democratic society. The applicants' contention is significant at this point so that the Court also noted; the second paragraph of Article 8 protects democratic society from sliding towards totalitarianism.

The Court considered the increasing need for national security measures and evaluated secret surveillance in this manner. State parties have their own discretion to take such measures. Besides, that discretion is limited for not to endanger democracy instead of defending it.

¹¹⁹ No. 5029/71 (1978)

¹²⁰ § 36-38

Adequate and effective guarantees must be provided by the state against any abuse, regarding the nature, grounds, scope, and duration of the possible measures, competent authorities, and the remedies.¹²¹ In addition, the Court explained that surveillance should be subjected to a review not only during the implementation but also after the termination.¹²²

The last point, which should be noted, was the highlight of the societal harm beneath the individual cases.¹²³ Although the Court did not elaborate on the consequences of surveillance activities for a democratic society, it is accepted that privacy-related matters are vulnerable to abuse.

Even though the interference was decided justified under Article 8 – (2) in *Klass*, presented discussions have started to form general principles under the exceptions for justifying interferences to private life, and served as a model for ‘conventionality review’.¹²⁴

In 1987, *Leander v. Sweden*¹²⁵ was delivered. The applicant challenged the personnel control procedure that he was subjected to. In this case, examinations of the Court under Article 8 are presented in a systematic order. Sub-headings outline the order: first, it is discussed whether there is any interference, and then whether the interference is justified. *Leander* organizes the discussions of *Klass*, and guide the following cases' scheme.

For the first question, it was stated that private information was collected, stored and released without allowing the applicant to object. For the second question, national security was accepted as a legitimate aim. The other questions of the Court must be asked then: whether this interference was in accordance with the law, and whether it was necessary in a democratic society.

The requirement of being in accordance with the law means a legal basis in domestic law which

¹²¹ § 50

¹²² § 55

¹²³ § 56

¹²⁴ Bart Van der Sloot, *Privacy As Virtue: Moving Beyond The Individual In The Age of Big Data* (2017) University of Amsterdam). However, he also reminds a similar case concerning abstract review, *Hilton v. The United Kingdom*, application no. 12015/86, 06 July 1988, where the case was compared to *Klass* and concluded an opposite decision.

¹²⁵ *Leander v. Sweden*, no 9248/81, 26 March 1987.

is accessible and foreseeable by any individual. Indication of when and how surveillance measures may be carried out is a must, as well as the indication of discretionary powers and competent authorities. The requirement of the need in a democratic society implies a pressing social need, and also proportionality of the measures with the legitimate aim of the government. The Court found state parties entitled to a wide margin of appreciation in this assessment; nevertheless, it is emphasized that resort to secret surveillance for national security could endanger democracy instead of strengthening it. Thus, in balancing public security with individual privacy, states must ensure the Court against any abuse.

Leander may be regarded as *Klass* 2.0. *Klass* was a radical decision granting the victim status to the applicants. The Court showed its willingness to further discussions on the government measure against individual privacy. Introduction of particular concepts, requirements, and criteria led the following cases including *Leander*. The Court could have dismissed the case in the first place based on the victim requirement since the applicants did not know if they were targeted let alone to prove any privacy harm. Instead, it has given the primary example of abstract review. *Leander* is highly dependent on *Klass*. These two cases together were intended to have constituted the anatomy of further privacy discussions. They have shaped the Court's approach to the fundamental protection of Article 8, and even more significantly, the application of the second paragraph. The second paragraph entails a sensitive balance of individual privacy and public security, and these cases illustrate that privacy harm is not necessarily required to lose on this balance. Rather the qualifications of the domestic law and arbitrary actions of the government is decisive. Even the wide margin of appreciation should be limited to what is necessary in a democratic society, as stated by the Court.

Third fundamental case, *Weber and Saravia v. Germany*¹²⁶, followed this scheme for a similar discussion in 2006. The applicants submitted that they could not prove actual monitoring applied to them but challenged the national legislation behind the secret surveillance. The Court approved their victim status. Besides, by referring to *Klass*, it underlined that the mere existence of such legislation for secret surveillance was a threat in general terms without any specific action taken against the applicants. In other words, it accepted conventionality and abstract review once more.

¹²⁶ *Weber and Saravia v. Germany*, application no. 54934/00, 29 June 2006

Justification of the interference was discussed in a similar order with an advanced examination on the quality of national law. Accessibility and foreseeability of the law were stressed as the previous cases, with the significance of adequate and clear indications for surveillance conditions considering the risk of arbitrariness emerged by modern technology. Furthermore, Weber introduced a set of criteria to be provided by the states: description of offenses for the possible interception, targeted people, certain duration of the measures, the procedure of the application, precautions in data transfer, conditions for the destruction of data.¹²⁷ In this manner, it resembles *Klass* where the Court required guarantees on the nature, grounds, duration, and scope of the measures, competent authorities and remedies, from the government against any arbitrary implementation.¹²⁸

Weber reflected a parallel approach with *Klass* and *Leander* in the admissibility stage. The Court granted victim status to the applicants; however, it declared the application manifestly ill-founded according to Article 35-(3) and (4) of the Convention. It found existed guarantees adequate and effective against abuse. It decided that the state was in the fairly wide margin of appreciation, and was entitled to interfere secretly to the communications considering the interests of national security.

Interestingly *Weber* presents the discussion on the interference, which the others have in the merits of the case, in the admissibility. Abstract review, therefore, is carried out under Article 8-(2) in the previous two cases while it is under Article 35 in *Weber*. In this manner, it indeed brings a confusion that therefore in addition to the victim status, the applicants need to substantiate their challenge against domestic law or a measure to defend the right to privacy under Article 8. In other words, it might be concluded that for the Court to examine the merits of the case it should be convinced on the violation. Persuasion of violation would be another admissibility criterion for privacy cases. It would impose an excessive burden on applicants to prove violation has been occurred twice: for admissibility and the merits of the case. Despite this criticism, *Weber* has been playing a key role with its clarifications on the abstract review.¹²⁹

¹²⁷ no. 54934/00, § 95

¹²⁸ *Supra* note 107. *Weber* indeed refers directly to *Klass* for these safeguards to be satisfied. *See*, no. 54934/00, § 106. In addition, for effectiveness of the remedies, the Court reiterated *Klass* to highlight that subsequent notification of surveillance measures is highly relevant.

¹²⁹ Case of Liberty and others v. the United Kingdom, application no. 58243/00, 01 July 2008 is a famous case relevant to abstract review, highly based on *Weber*. The Court distinguished *Weber* for its focus was on

*Kopp v. Switzerland*¹³⁰ and *Amann v. Switzerland*¹³¹ were other notable decisions by their contribution to *Weber*. Both cases examined the justification for the interception by government measures, through their legal basis¹³² and quality of that legislation. *Kopp* indicated that the law in question should have sufficient clarity on the details of the application of measures so that the applicant could enjoy the minimum safeguards as the rule of law requires. The Court found a breach of Article 8. *Kopp* underlined the necessity to illustrate the scope and manner of the surveillance activities considering the technological developments, and *Amann* further underlined the necessity to clarify discretionary powers conferred on the authorities against the risk of arbitrariness. *Amann* analyzed not only the interception but also storing personal data thereof¹³³. It clarified that the mere storing of data constitutes an interference irrespective of any use of such data¹³⁴; and since the interference was not in accordance with the law, there was a violation of Article 8.

These cases are significant for elaboration on the qualifications of domestic law behind privacy intrusions. Sufficient clarity on the details is required, including even the use of discretionary powers. The Court, in one sense, stipulates self-restriction of the state¹³⁵. It should be appreciated that this paradigm brings reliability to the parameters of abstract review by the Court as well. This is simply because such self-restriction instruments would provide the Court

strategic monitoring while the instant case on a specific action; but still it decided to follow the same principles. The applicants alleged that their communications had been intercepted by the government for years. The interception was not regulated properly, in contrary to foreseeability, accessibility, proportionality and accordance with the law. The Court did not elaborate on victim status, found the case admissible and directly examine the merits of the case. Under the examination of interference, it was stated that the mere existence of permission for secret surveillance constitutes a threat to all community which was sufficient to be deemed as an interference under Article 8 even without any implementation against the applicants. Moreover, in *Liberty*, there was an individual application of surveillance measure, and it was found as a breach of Article 8.

¹³⁰ Judgment of 25 March 1998, *Reports* 1998-II

¹³¹ [GC], no. 27798/95, 16 February 2000

¹³² The Court includes both written and unwritten law in this concept, *see Kopp* § 60.

¹³³ The Court referred to the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which came into force on 1 October 1985, for defining personal data as "any information relating to an identified or identifiable individual". *See Amann* § 67.

¹³⁴ *Amann* § 69

¹³⁵ *Klass* was required the strict conditions and procedures to be laid down in the domestic legislation itself. *Klass* § 43.

definite grounds to assess both conventionality of them and compliance of the governmental actions. Moreover, the finding of *Amann* that the storing of data is sufficient to be an interference itself is crucial. The Court did not look for any other use of data. It breaks new ground in privacy harm discussions regarding data retention.

After several months the Court delivered *Rotaru v. Romania*¹³⁶. It reminded the principle for victim status that any individual could have victim status without addressing any specific harm on himself. Under Article 8, storing and release of personal information¹³⁷ amounted to interference to the private life; and justification for this interference according to the second paragraph should be interpreted so narrowly that secret surveillance might only be acceptable if strictly necessary for democracy. In contrast with the stress on the wide margin of appreciation recognized by *Leander* and *Weber*, *Rotaru* reminded that the second paragraph is only an exception rule which is supposed to be subject to a narrow interpretation, following *Klass*. It is significant that even being strictly necessary must be for the sake of democratic institutions, instead of public security. In addition, effective supervision which is expected by an independent judicial body was pointed once more after *Klass* and *Kopp*. Interference of the state, considering all the requirements, was not found in accordance with the law.

Even though they have their own differences regarding the privacy interference discussions, these cases were the landmark cases. They have given the signal that neither victim status nor the exception provision for privacy cases would not be engraved on traditional jurisprudence of the ECtHR. Nevertheless, the Court was struggling with shaping its own case-law for these unusual applications since the variety of cases was driving it to find different conclusions in similar cases. The applicants were entitled to victim status without a demonstration where the legislation itself is found to be capable of affecting them, which indeed an open door for further abstract review and even class actions before the Court. Conventionality review, therefore, has been introduced thanks to the abstract nature of privacy itself. In particular, adaptation or relaxation of victim status in these cases directly acknowledged that privacy harm, directly or

¹³⁶ *Rotaru v. Romania*, no 28341/95, 4 May 2000

¹³⁷ In the instant case it is noted that the holding of a secret register was containing information about the applicant, whose existence was publicly revealed during judicial proceedings. *Rotaru* §36. The Court once more referred to the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which came into force on 1 October 1985, for defining personal data as "any information relating to an identified or identifiable individual". *Rotaru* §43.

indirectly, might not be required in case of a serious unconventional concern. The Court even underlined the societal harm¹³⁸ behind the privacy breaches.

On the other hand, individual claims had to be balanced against the governments' justifications under the second paragraph of Article 8. The exceptional circumstances of the second paragraph were depending on the necessity in a democratic society. Further, it was asserted that the ground for the protection of national security might endanger democracy itself¹³⁹. In this manner, the Court recognized either wide margin of appreciation¹⁴⁰ or narrow interpretation¹⁴¹ of the exceptional situations so that we could not grasp how it set the balance between individual harm and societal harm.

In 2010, *Kennedy v. The United Kingdom*¹⁴² the applicant maintained that his communications had been intercepted, but in any case, he did not have to demonstrate an actual interference relying on the jurisprudence of the Court in this manner. The Court reminded that abstract review was only an exception for particular features of secret surveillance. In this case, the Court decided to look for any remedy provided at the national level, and the risk of being a target of the surveillance measures in order to challenge the mere existence of legislation. If there is no remedy, according to the Court, public anxiety of mass surveillance must be considered even the individual risk to be exposed to such measure is low.¹⁴³ The application was found admissible, but the Court did not observe 'any significant shortcoming'¹⁴⁴ in the surveillance regime.

Kennedy reiterated the general principles of strict necessity of surveillance, effective safeguards for democratic institutions, and supervision in which the abuse is potentially harmful for democratic society as a whole. A significant discussion in this case was on the ambiguity of 'national security' and 'serious crime'. The Court emphasized that national security is used often in both domestic and international instruments, including Article 8-(2). Further, qualified

¹³⁸ *Supra* note 109.

¹³⁹ *Klass* § 50, *Leander* § 60, *Rotaru* § 59, *Weber* § 106.

¹⁴⁰ *Leander* § 59, *Weber* § 106. In *Leander*, necessity explained as a 'pressing social need'; however, the Court even recognize wide margin to the state in determining such pressing social need. *See* § 58-59.

¹⁴¹ *Klass* § 42, *Rotaru* § 47

¹⁴² *Kennedy v. The United Kingdom*, No. 26839/05, 18 August 2010

¹⁴³ *Kennedy* § 124

¹⁴⁴ *Kennedy* § 169

domestic law does not need to enlist national security matters. Similarly, serious crime is supposed to be understood from domestic law interpretations.¹⁴⁵ The Court, however, did not attempt to make any description, determination or identification for in which situations national security is at stake.

Recently, discussion of the interference to private lives has reached another dimension with *Roman Zakharov v. Russia*¹⁴⁶. It provides an inclusive map for the existing case-law of the Court on the connected concepts of victim status and abstract review. The Court put forward the consistent denial of *actio popularis* and *in abstracto* claims, and explicit requirement of Article 34 that an applicant must be directly affected by the impugned measure. General challenges without any direct application to an individual, however, are permitted due to the nature of secret surveillance measures. Fundamentally, two parallel approaches have been followed regarding victim status.¹⁴⁷ In the first camp, there should be a reasonable likelihood of interference, even there is no exact proof of being affected. In the second camp, the laws and applications of secret surveillance themselves constitute a threat for all the possible targets, irrespective of a concrete interference. Basically, the former is associated with the reasonable likelihood whereas the latter reflects the cases of abstract, or conventionality, review. *Zakharov* also noted *Kennedy* as the most recent case then, regarding the availability of the remedies, the risk of being targeted by the measure, and common concern among the public of abuse of powers.

Having noted the diversity of the case law, the Court addressed the need for harmonization victim status for a uniform and foreseeable approach. *Zakharov* determines two issues to challenge the secret surveillance measures: the scope of the secret surveillance that the applicant might be targeted, and the effectiveness of the remedies. In case of an absence of effective remedy, the public concern of government abuse is to be considered. The individual, further, does not need to demonstrate any risk of being monitored. In other cases, where effective remedies are provided, the applicant needs to illustrate a potential risk of application of surveillance measures to him.¹⁴⁸ Therefore, the Court has decided when to require a demonstration from the applicant. A compromise between the two camps, in one sense, with

¹⁴⁵ *Kennedy* § 159.

¹⁴⁶ *Roman Zakharov v. Russia*, no. 47143, 4 December 2015

¹⁴⁷ *Zakharov* § 167-168.

¹⁴⁸ *Zakharov* § 171.

the help of *Kennedy*.

Considering the broad scope of the legislation, and the lack of effective remedies in *Zakharov*, the Court decided to make an abstract review and forwarded to the examination of the quality of the law. Domestic law, in this manner, should be accessible, foreseeable and covering effective guarantees for individuals. It is significant that the Court accepted 'certain' margin of appreciation which is also subjected to European supervision¹⁴⁹. *Zakharov* also highlights the three-staged review -at the beginning, operation, and afterward- of the surveillance measures in such a field where any abuse may have societal harms in democracies. The Court detected serious shortcomings and arbitrariness in practice due to the lack of adequate safeguards in the domestic law, and found the interference out of what is necessary in a democratic society.

*Szabó and Vissy v. Hungary*¹⁵⁰, is another notable and recent case where the applicants claimed that they could potentially be subjected to government surveillance. The Court follows the harmonized approach of *Zakharov*, and relying on the lack of effective remedy, declared the application admissible.

The Court set forth the principle that justification could only be granted if the interference was strictly necessary for protection of democratic institutions. Certain margin of appreciation of the states, in this regard, would be subjected to European supervision in *Szabó* as well. The Court assesses the quality of the law as usual, and based on the lack of sufficient protection, it decided in favor of the applicants.

Szabó observes present-day terrorism and pre-emptive measures are correspondingly proceeding. The more this simultaneity gets complicated the harder an average citizen conceive how monitoring operations are actually being applied. In this regard, the Court formulated another question: whether the progress of surveillance methods is accompanied by the progress of the safeguards¹⁵¹. Another innovative paradigm of the judgment is the interpretation on the strict necessity test that it has two dimensions: (1) the interference must be strictly necessary in

¹⁴⁹ *Zakharov* § 232.

¹⁵⁰ *Szabó and Vissy v. Hungary*, no. 37138/14, 12 January 2016

¹⁵¹ *Szabó* § 68

general for democracy, and (2) in particular for collecting individual information.¹⁵²

2. The Court of Justice of the European Union

Zakharov and *Szabó* are important for direct reference to the European Union case-law.¹⁵³ The Court of Justice of the European Union, in the joint cases of *Digital Rights Ireland* and *Seitlinger and Others*¹⁵⁴, makes a significant statement that collection and use of personal data without any notification to the subject would cause a public concern of being monitored. CJEU also emphasizes the strict necessity and requirement of sufficient safeguards by clear and precise rules against the risk of abuse.

CJEU delivered *Schrems*¹⁵⁵ after *Digital Rights Ireland*, where it reached a radical conclusion for cross-border data sharing. Facebook Ireland was transferring personal data to Facebook Inc. in the United States. Schrems requested the Data Protection Commissioner (DPA) to restrain such transferring of his own data since the United States provide adequate protection for personal data neither by law nor by practice.¹⁵⁶ DPA decided that there was no proof for US authorities had reached Schrems' data, further the Decision 2000/520 on the data sharing between EU and US (safe harbor regime) implied for adequate protection in the US. Schrems challenged this rejection before the High Court.

The High Court forwarded the case to the CJEU with questioning the legality of the safe harbor regime that it did not meet the basic requirements derived from Articles 7 and 8 of the Charter, and the principles set forth by the CJEU in *Digital Rights*.

CJEU considered the fair balance between the free flow of data and individual interests. In this balance, sufficient protection must be ensured by the Union under the rule of law, and case law of the Court. In this particular matter, CJEU stated that the existence of an instrument such as

¹⁵² Szabó § 73

¹⁵³ Zakharov §147, Szabó §23.

¹⁵⁴ Joint Cases C-293/12 and C-594/12 *Digital Rights Ireland and Others*, 8 April 2014. CJEU also refers to European Court of Human Rights cases, such as *Liberty* and *Rotaru*.

¹⁵⁵ Maximilian Schrems v Data Protection Commissioner, C-362/14, 6 October 2015

¹⁵⁶ He referred to the revelations made by Edward Snowden regarding the unlawful collection and processing personal data by the US public authorities, particularly the National Security Agency.

Decision 2000/520 would not be excluded from supervisory. EU must regulate the scope and execution of measures as well as minimum safeguards against arbitrariness. Any derogation or limitation to this protection may be justified only if it is strictly necessary as underlined by *Digital Rights*. CJEU invalidated, therefore, the safe harbor regime.¹⁵⁷

Joint Cases *Tele2 Sverige AB v Post-och teletyrelsen* and *Secretary of State for the Home Department v Tom Watson and Others*¹⁵⁸ should also be noted at that point. CJEU referred to the strict necessity test and evoking the common concern of being subjected to secret surveillance. Further, only the purpose of fighting serious crime was found capable to legitimize such interference. CJEU followed the established case law that any misuse and/or arbitrariness should be prevented at the national level even after the termination of surveillance. The impugned legislation was found exceeding the boundary of strict necessity by the Court.

On 26 July 2017, Grand Chamber of the Court of Justice of the European Union delivered Opinion 1/15¹⁵⁹ upon the request by the European Parliament, regarding the draft agreement between Canada and the EU on sharing passengers' data (PNR). The Court referred to *Schrems*, *Tele2 Sverige*, *Digital Rights Ireland*. In the balance between liberty and security, the Court considered mass surveillance as tolerable at least in theory, because it is necessary and a useful tool for prevention of terrorism. Yet, it insisted that there should be highly strict rules as to the concrete implementation of such surveillance. For this reason, it found certain provisions of the draft agreement incompatible with Articles 7 and 8, in conjunction with Article 52 of the Charter of Fundamental Rights of the European Union.

CJEU has apparently a similar perspective with the ECtHR on the protection of privacy rights. It may even be more activist considering the 'feeling of being subject to constant surveillance' in *Digital Rights Ireland*¹⁶⁰ which is a much-cited case in the following decisions. CJEU also had to balance business interest and individual interest in *Schrems*, apart from the usual comparison between public and private interests. It is a prominent case where the Court still pursue privacy protection in cross-border data transfer for commercial purposes. *Schrems* indeed implies that the attempt of the Court, by the invalidation of that transfer regime based

¹⁵⁷ In July 2016, Privacy Shield replaced the invalidated regime by *Schrems*. See Bignami & Resta. 2018.

¹⁵⁸ C-203/15 and C-698/15, 21 December 2016

¹⁵⁹ Available at <http://curia.europa.eu/juris/document/document.jsf?text=&docid=193216&doclang=EN>

¹⁶⁰ § 37

on the lack of sufficient safeguards, was to protect whole the European community.

3. Privacy Harm in the Present

In 2018, the European Court of Human Rights continues to face with sophisticated cases. The struggle seems obvious between the settled case-law and needs of the recent cases.

Ben Faiza v. France

In *Ben Faiza v. France*¹⁶¹, the applicant challenged the order to a telephone operator to obtain records and fixing of a geolocation device onto his vehicle before the ECtHR. He was arrested as a suspect of drug trafficking relied on this geolocation data. During the national proceedings, he challenged the validity of that order and the installation of the geolocation device. The Court indicated that geolocation and further use of the data constituted an interference with the applicant's private life. The lack of precise rules on discretionary powers vested in the public authorities violated Article 8. However, in the examination of the national court's order to access and use phone records, and to locate the suspect by phone signals, it was found that the measure was in accordance with the law. The application of the measure itself did not violate the article. In other words, *Ben Faiza* examines the law and the application separately and find the law in violation of the Article 8 whereas the application is not because it follows the domestic law violating Article 8.

Centrum för Rättvisa v. Sweden

Several months after *Ben Faiza*, the Court delivered the case of *Centrum för Rättvisa v. Sweden*¹⁶² questioning the legislation permitting the bulk interception of electronic signals in Sweden for foreign intelligence purposes. A system of secret surveillance was alleged to be directed all users of mobile telephones and the internet, without their being notified or being provided any domestic remedy. In the abstract review, the Court found that Swedish system had effective guarantees against abuse. The scope was clear in the law, with review and complaint mechanisms available. The Court stressed the State's discretionary powers in protecting national security given the present-day threats of global terrorism and serious cross-

¹⁶¹ application no. 31446/12, 8 February 2018

¹⁶² Application no. 35252/08, 19 June 2018.

border crime.

Big Brother Watch and Others v. The United Kingdom

The European Court of Human Rights has been dealing with these issues in many cases from *Klass* of 1978. The cases include the interception of communications, obtaining and recording of data, or tracking of individuals electronically. Case of *Big Brother Watch and Others v. The United Kingdom*¹⁶³ looks at three different types of surveillance: bulk interception of communications, intelligence sharing, and the obtaining of communications data from the service providers.

Following the revelations by Edward Snowden relating to the electronic surveillance programs operated by the intelligence services of the US and the UK, non-profit organizations and activists believed that due to the nature of their activities, their electronic communications were highly likely to be intercepted by the UK intelligence services. They claimed that the bulk interception regime is lacking the quality of law in terms of accessibility and efficient protection of individuals.

The applicants defended that *Weber* requirements were not satisfied for this case. Moreover, they invited the Court to consider additional criteria to justify the interference: reasonable suspicion supported by objective evidence, judicial warrants, and the subsequent notification of the surveillance. This effort was significant for discussions regarding the secret activities of intelligence services. The Court might have taken another step forward in creating a consistent and strict doctrine for Article 8-(2). In addition to the six *Weber* criteria, the Court only took into account the supervision, notification mechanisms and legal remedies as in *Zakharov*¹⁶⁴.

The Court referred two cases regarding bulk interception regimes: six minimum criteria of *Weber*, and consideration of sufficient clarity, adequate protection against abuse, and wide discretion of *Liberty*. The criteria would be adapted, and additional considerations including the ones in *Zakharov* would be assessed accordingly. CJEU principles, in *Digital Rights* and *Tele2 Sverige*, were also regarded. The Court accepted the potential risk of the applicants

¹⁶³ Applications nos. 58170/13, 62322/14 and 24960/15, 13 September 2018. The judgement was referred to the Grand Chamber on 4 February 2019.

¹⁶⁴ *Big Brother Watch* § 307, *Zakharov* § 238.

having their communications intercepted by the intelligence regime. However, it stuck to the availability of remedies as set forth by *Zakharov*, and granted the victim status primarily because there was no effective remedy.

In the case, two violations were found by the legislations but none for the measure itself. Certain serious matters of concern remain. Indeed, the ECtHR did not abolish the threat by interceptions and data sharing regimes. It resembles *Ben Faiza* that the Court interestingly finds the measures justified but the underlying laws not. Both of these decisions create confusion about how to decide conventionality of a measure based on unconventional legislation.

A comparison with relevant case-law of the Court of Justice of the European Union, i.e. *Digital Rights Ireland*, *Schrems*, *Tele2 Sverige* and *Opinion 1/15* with rather high privacy and data protection standards, would help to put this judgment into perspective: the extensive safeguards established in Luxembourg should remain the point of reference within Europe.¹⁶⁵ Strasbourg should not be lowering these thresholds instead. The applicants' proposal for expanding the criteria has unfortunately been missed.

The CJEU, in *Digital Rights Ireland* and especially in *Tele2 Sverige*, clarifies that legislation for mass retention of metadata by communications service providers exceeds the limits of what is strictly necessary. This is because retention or creation of such a database does not directly follow a legitimized aim most of the time. If the ECtHR, as did the CJEU in *Opinion 1/15*, had added the "reasonable suspicion" criterion to its jurisprudence in *Big Brother Watch*, it would have gone further than *Zakharov*.

Catt v. the UK

*Catt v. the UK*¹⁶⁶ delivered in 2019 is the last case from Europe in this section¹⁶⁷. The applicant challenged the systematic collection and retention of information about him in a searchable

¹⁶⁵ Judith Vermeulen, 'Big Brother may continue watching you', 12 October 2018, <https://strasbourgobservers.com/2018/10/12/big-brother-may-continue-watching-you/#more-4225>

¹⁶⁶ Application No. 43514/15, 24 January 2019.

¹⁶⁷ *Breyer v. Germany*, Application No. 50001/12, is one of the pending cases, which has been expected to be delivered for further discussions at that point. The application regards storage of personal information by the service providers, due to a legal obligation on the providers to do so. The judgement will show broader perspective including the private sector responsibilities vis-a-vis individuals, legal requirements, and free flow of data.

database. It was alleged that no sufficient safeguards were provided and the interference was arbitrary. Since the data was mostly related to the applicant's activism and never been used for criminal proceedings by police, this interference would cause a chilling effect.

Mere storing has already been accepted as interference by the Court, as mentioned in *Leander*, *Amann*, and *Kopp*. The interference would be necessary in a democratic if there is a pressing social need, and such determination falls within the state's margin of appreciation. The Court stated that it does not make this assessment on behalf of the national authorities; however, in this case, there are compelling reasons to do so. Even though the collection of data by the police is justified by the pressing social need, retention of data is not. There may be a pressing need for retention provided that clear rules set a time limit and effective procedural safeguards.¹⁶⁸ The Court stressed the requirement of even higher protection for personal data revealing the political opinion and approved the probability of chilling effect¹⁶⁹.

In sum, both the US and the ECHR jurisprudence could not achieve to construct comprehensive paradigm in response to modern drawbacks. They rather evaluate the cases separately, follow different principles, and reach contradictory conclusions. US Supreme Court and federal courts insist on the privacy harm even with small steps towards the adaptation of precedents while the ECtHR struggles to depart from the rule by allowing the abstract claims. ECtHR, in this regard, seems to fall behind the CJEU which is willing to provide stricter protection based on the EU law.

¹⁶⁸ *Catt* § 119.

¹⁶⁹ The Court has several exceptions in case of surveillance measures or discriminative measures against certain groups. The applicant can claim that there is a chance to suffer from harm in the future in any case, either from the activity itself or from self-restraint. *Michaud v. France*, application no. 12323/33, 06 December 2012, regarded the obligation of lawyers to inform on people ask them for advice, particularly regarding the financial crimes. The Court clarified the exclusion of *actio popularis* by the Convention, and case-law (The Court decided not to deduce an *actio popularis* in compliance with the Convention, in *Norris v. Ireland*, 26 October 1988, § 31, Series A no. 142, and among many other authorities, *Burden v. the United Kingdom* [GC], no. 13378/05, § 33, ECHR 2008). Having put a 'however' afterwards, exceptional circumstances were indicated that even in the absence of individual measure, a person may have the victim status in case of an obligation to modify his conduct, or in case of being one of the targeted people by the general measures. (The Court had established this exception in *Marckx v. Belgium*, 13 June 1979, § 27, Series A no. 31; *Johnston and Others v. Ireland*, 18 December 1986, § 42, Series A no. 112; *Norris*, § 31; and *Burden*, § 34) Considering the applicant being lawyer in financial law, he would be exposed to the respective legislation and had the victim status to submit his case. The Court also adapted the victim requirement as the situation entails, in *Dudgeon v. the United Kingdom*, application no. 7525/76, 22 October 1981. In a recent case regarding warrantless stop and search, ECtHR continued to apply the exception for the applicant: *Colon v. the Netherlands*, application no. 49458/06, 15 May 2012.

Chapter III: CONTESTED BOUNDARIES OF PRIVACY HARM

Introduction

In those efforts to solve the instant case before the courts, conceptualizing the privacy and determination of genuine harm are ignored most of the time. It also creates a tension between the theory and practice. However, academic efforts are precious to guide legislators and judiciary. They have been discussing the proper and comprehensive framework for an effective response to privacy violations. The traditional understanding of harm does not suffice to determine peculiar privacy harms. This is because of the very nature of privacy harm.

Several methods are employed by scholars to reduce privacy harm to a scheme or formula. In the digital sphere, it seems that outputs are mostly derivatives of informational privacy. Without any consequence attached, collection of data and surveillance in any manner would constitute privacy harm per se. Privacy interferences are assumed as inherently harmful. That harm, moreover, is not only for the victim but for the whole society. Nevertheless, there are still opponents to the protection of privacy let alone the inherent harm.

A. Categorization of Privacy Harm

Privacy, in the application, has been developed rather by jurisprudence since it has been confined only to a framework in legislative manners, by national or international instruments. Intrusions may be multidimensional in so much as any general provision would not be efficient to solve. Therefore, since Warren and Brandeis, scholars have been urging upon conceptualizing the notion itself and privacy harm.

Intrusions to private lives may be justified by the governments' excuse for national security or other arguments regarding the public well-being. Inevitably, supervisory authorities redress the balance between public interest and individual interest. Privacy, in this balance, unfortunately, seems to be the loser most of the time against long and growing counterweights.¹⁷⁰ There have been several prominent offers and discussions by scholars to contribute improvement of privacy rights and to guide the legislative and judicial authorities.

Productive scholar Daniel Solove offers the categorization method for harmful activities against privacy. He attributes the failure of balancing privacy against the counterweights to this struggle in recognizing privacy harm.¹⁷¹ He believes that the classification of the actions would draw the framework for better understanding and protection for privacy rights. He firstly puts the drawback that people including lawmakers and judges fail to recognize and formulate the privacy harm whereas the concerns on the other issues such as free speech are much more readily articulated. Understanding the concept of privacy is highly depending on understanding privacy problems according to him. Understanding the privacy problems, further, is based on the variety of harmful activities rather than scrutinize it as a unitary concept. This is the idea behind his theory.

¹⁷⁰ Cohen, HARV. L. REV., 1904 (2012).

¹⁷¹ Solove, U. PA. L. REV., 480 (2005). He states that due to conceptual confusion, judges often fail to recognize privacy problems, and thus no balancing takes place at all. Privacy does surely not always win in the balance, but it should not be ignored just because it is misconstrued. *See id.* at 558.

Information collection

- **Surveillance**
- **Interrogation**

Information processing

- **Aggregation**
- **Identification**
- **Insecurity**
- **Secondary use**
- **Exclusion**

Information dissemination

- **Breach of confidentiality**
- **Disclosure**
- **Exposure**
- **Increased accessibility**
- **Blackmail**
- **Appropriation**
- **Distortion**

Invasion

- **Intrusion**
- **Decisional interference**

Dignitary harms, apart from physical injury, has been asserted since Warren and Brandeis called it ‘injury to the feelings’¹⁷². In their times, it might be considered under tort law, as a reputational injury or defamation. Solove addresses this beginning of the discussion but puts it forward that modern problems are ‘architectural problems’ in two kinds: risk-enhancing activities and chilling effect¹⁷³. These problems either increase the chance of suffering or affect the individual's behavior in society¹⁷⁴. At this point, although the focus and consequences seem to be on the individual, privacy is not an individualistic right but is constitutive of society.[6] In this regard, he strictly supports the societal value of privacy. In his taxonomy, he makes four basic groups for the wrongful activities.¹⁷⁵ In the first group, surveillance covers the monitoring, listening or recording activities, and interrogation stands for any searching activity for reaching information. The second group is concerning how the information is retained. Gathering the pieces of personal data, make a connection between information and the person, failure to protect collected personal data, using the data in a way other than the initial purpose, and precluding individuals from the processes are listed. In the third, there is the failure of keeping secret information, the revelation of mental facts, the revelation of physical facts, making data more accessible, threatening through the personal data, using the identity information for others' interests, spreading false or misleading information. The third group is concerning revelation and spreading personal information, or threatening to do so. The final group involves invasions into the private affairs of people. Apart from the other categories, it does not directly concern personal information.

¹⁷² Samuel D. Warren, *HARVARD LAW REVIEW*, (1890).

¹⁷³ He claims that chilling effect can be greater where people are aware of their being watched. Solove, U. PA. L. REV., 495 (2005). Other studies support this hypothesis. For the first time, Alex Marthews and Catherine Tucker published their analysis on whether Google users’ search behavior changed after the revelations of NSA’s secret surveillance programs. They documented that there is really a chilling effect on the internet users because of government surveillance, mostly in the US allies. It indeed clearly supports Solove on the awareness-increasing-chilling-effect argument. Interestingly, they also found that government surveillance programs are affecting business of US based internet firms. *See* Alex Marthews & Catherine E Tucker, *Government Surveillance and Internet Search Behavior* at [https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564.](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564), and ‘The Impact of Online Surveillance on Behavior’ by Marthews and Tucker in D. GRAY & S.E. HENDERSON, *THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW* (Cambridge University Press. 2017).

¹⁷⁴ A parallel approach is embraced by Neil Richards, particularly on the surveillance. Threat for intellectual privacy and chilling effect together with imbalance of power create a legally recognizable injury. Harm arising from the surveillance can only be articulated by understanding privacy. *See* Richards, *HARV. L. REV.*, 1934, 1945 (2013).

¹⁷⁵ Solove, U. PA. L. REV., 490 (2005).

This grouping shows the gap between the traditional approach and modern veracity of privacy matters. Today, not only the use or collection of information itself amount to an infringement, even the effort for gathering the data is taken into account. Problems may arise from the way that data is reached, managed, or processed. Besides, Solove underlines a neglected fact that it is not important if the personal information is public or not. Even if the intention of keeping the information secret is not obvious, increasing accessibility is still deemed as a violation of privacy. It is a significant point considering the fact that modern surveillance is also carried out by the private sector. In this regard, he addresses another drawback of distinction between public and private actors.¹⁷⁶

Solove suggests a list of consequences of these wrongful acts which are individual and societal harms: physical, financial, reputational, emotional and mental harms, relationship harms, vulnerability, chilling effect, and power imbalance.¹⁷⁷

This approach introduced by Solove has been influencing both the academy and the judiciary¹⁷⁸. Nevertheless, it is criticized that these categorized activities need to be recognized by competent authorities and society to a certain extent. In case of a need for a new type of harm, the recognition of it would be necessary as well, or we would resort to analogy where the subsequent questions might be emerged such as which parameters to be employed.¹⁷⁹ Solove's

¹⁷⁶ Surveillance is being carried out in public and private places, by public and private sectors. *See id.* at 559-560. He also underlines the misleading public-private distinction on surveillance measures that there is no reasonable expectation in data collection by third parties according to the US case-law. *See SOLOVE*, 193. 2008. Experiments have shown that individuals also distinguish the public and private surveillance in terms of consent. *See Nili Steinfeld, Track me, track me not: Support and consent to state and private sector surveillance*, 34 *TELEMATICS AND INFORMATICS* 1663(2017). They also have revealed that politics can influence people to accept the surveillance measures. *See Eva-Maria Trüdinger & Leonie C Steckermeier, Trusting and controlling? Political trust, information and acceptance of surveillance policies: The case of Germany*, 34 *Government Information Quarterly* 421(2017). It has been suggested that awareness may be raised by stressing the identity consequences rather than addressing surveillance as a general threat. *See id.* at. Also *see supra* note 79.

¹⁷⁷ *SOLOVE*, 174-179. 2008.

¹⁷⁸ Solove's pragmatic and inclusive approach to privacy is referred many times, even by the federal courts. *See, e.g., Nat'l Cable & Telecomms. Ass'n v. Fed. Commc'ns Comm'n*, 555 F.3d 996, 1001 (D.C. Cir. 2009); *Doe v. Biang*, 494 F. Supp. 2d 880, 892 (N.D. Ill. 2006). Over seventy secondary sources have cited to A Taxonomy of Privacy since its publication in 2006. *See Calo, IND LJ*, 1139 (2011).

¹⁷⁹ Ryan Calo contends that certain consequences attributed to privacy harm should not be deemed as so. Taxonomy, in this regard, creates a confusion and uncertainty for separate harms concerning different values. *See id.* at, 1141-1142.

taxonomy is found useful for only descriptive purposes that it does not offer a solution for the reformation of balancing the privacy rights with the counterweights. Further, it is emphasized by the critics that the taxonomy method is attempting to define activities outside the person which draws the focus away from the individual. Considering the inner characteristic of privacy, individual's view and fear of harm are determinative what is a violation of the right.¹⁸⁰

Ryan Calo, one of the critics of Solove, aims to distinguish between privacy harm and privacy violation since they do not necessarily entail each other. Solove rather associates the two for those harmful activities violate privacy. Calo contends that those harmful activities, and others perhaps, may cause complicated violation where privacy harm is hard to be determined. He finds the taxonomy pragmatic only for theoretical approach, but without his 'limiting principle' and 'rule of recognition', certain harms would highly likely be confused. Limiting principle primarily concerns with another value if it is more directly affected than privacy. Otherwise, he argues, there is a risk to miss what is really worrisome regarding privacy in particular. When there is no other harm regarding another value, privacy harm is to be addressed. It leads us to rule of recognition -of the privacy harm finally- which allows to address correctly to the privacy issue.¹⁸¹

He offers two categories for privacy harms, generally from the loss of control over the personal information: subjective and objective. Under the subjective category, it is enough for an activity to be unwanted and considered harmful, regardless of intent to cause harm. Perception of observation is the main factor for this category. Objective category covers the harms arising from the use of information to commit a crime. In practice, he suggests that both of the components are testable by questioning whether the individual felt observed, gave consent to the collection of data, or was aware of subsequent use of data.¹⁸²

Particularly on the surveillance measures, Richards explains where is the privacy harm in theory and practice. In theory, he gives priority to the chilling effect, for all activities including thinking, reading and social communications with others. It may be called 'intellectual

¹⁸⁰ David Hughes is another opponent of the taxonomy. He expresses that the core of privacy is not the conceptual basis but the individual fear, so the protection is concerning only the individual not the information neither the activities. *See* Hughes, *Computer Law & Security Review*, 533-534 (2015).

¹⁸¹ Calo, *IND LJ*, 1138 (2011).

¹⁸² *Id.* at, 1154.

surveillance' which violates our 'intellectual privacy'. Secondly, similar to Solove's argument for power imbalance, he states that surveillance affects the power balance between the watcher and the watched. This imbalance would cause various harms including discrimination, coercion, or blackmail. In practice, he introduces four principles for future development: abolishment of public-private divide, the prohibition of secret measures, the prohibition of mass surveillance, recognition of harm in surveillance. He emphasizes the complicated and highly connected public and private watchers, the illegitimacy of secret surveillance, high risk of abuse in mass surveillance and the principal harm in surveillance increasing the risk for violations to privacy. Recognition of the harm in the mere existence of surveillance measure would not be a radical change since such recognition has been granted to other rights such as free speech.¹⁸³

A significant study is carried out to reveal the effects of surveillance. It embraces a different method to illustrate a broader perspective in which social reactions are also involved. It asks questions to six main socio-political groups: politicians, consultants, providers, the press, non-governmental organizations, and the public. Resistance or adaptation to surveillance is examined depending on the different forms of surveillance.¹⁸⁴ The study firstly states that we become a surveillance society with ubiquitous monitoring activities. It creates an inevitable chilling effect in addition to the threat to democratic institutions, principles, freedoms and the rule of law. In order to prevent negative effects of surveillance, resilience strategies are supposed to concentrate on decreasing surveillance while increasing social awareness. These strategies include also transparency, accountability, supervision, preemptive and punitive measures. On top of them, such strategies or increased public awareness would not be achieved without international cooperation.¹⁸⁵

¹⁸³ Richards, HARV. L. REV., 1935-1964 (2013). He stressed that surveillance is not only a tool for undemocratic governments but for all, particularly aftermath of the 9/11 terrorist attacks. In addition, governments and public authorities are involved in the private companies in a 'surveillant symbiosis' which he called 'age of liquid surveillance'. *See id.* at, 1938-1941. Since the work of Mr. Richards addresses the US law, he criticized the rejection of surveillance cases based on the lack of standing, and propose the recognition of harm per se.

¹⁸⁴ David Wright, et al., Questioning surveillance, 31 Computer Law & Security Review 280(2015). All these groups should be concerned on the lawfulness, necessity, proportionality, and purpose of the surveillance systems. Since the surveillance creates not only an individual harm but also societal one. David Wright, et al., *Questioning surveillance*, 31 COMPUTER LAW & SECURITY REVIEW 280, 283 (2015).

¹⁸⁵ Wright, et al., COMPUTER LAW & SECURITY REVIEW, 282 (2015). They suggest certain measures for enhancing resilience in surveillance societies. (1) Political and regulatory measures: accountability and oversight, consent, strengthening legal and constitutional protections of privacy, deliberation, awareness and communication, test of proportionality. (2) Individual measures: radical solutions, resilient attitudes, privacy

Mass surveillance, particularly the collection of mass data is even called ‘informational capitalism’¹⁸⁶. Bulk data is not being used only for one purpose surely. It is obviously vulnerable to abuse and unauthorized sharing, within and out of the public institutions. Partnerships between public and private sectors on collection, retention and transmission of data¹⁸⁷; procedures and measures for these activities, under the name of surveillance or other purposes such as commercial ones; secrecy of these measures; legitimacy of these procedures, purposes and use of the data are all questionable, due to the lack of sufficient transparency, accountability, and review mechanisms¹⁸⁸. Big data created by online and offline collection of personal data is worth noting not only for a huge amount of data but also the capability of producing intelligence by linking different pieces of personal data.¹⁸⁹

Big data poses significant challenges to the current legal paradigm which is not even well-established. The problem of this era is not solely an individual interest but the interests of large groups, sometimes a nation as a whole. The danger brought by such enhanced technology and legal predicament undermine directly to the rule of law. Big data also complicates the balance between individual privacy and public security for two reasons¹⁹⁰. Firstly, it becomes more difficult to identify the interests of both sides in order to balance them properly. Since the gathering of information is occurred without an initial purpose, and open to any further use for any purpose decided after the gathering, the interests of both sides naturally become

enhancing technologies. (3) Societal measures: collective actions composed of individual responses, demonstrations, influential groups, promotion of democracy and equality, raising the voice of public opinion, and activist press. Id. at, 287-291.

¹⁸⁶ Sami Coll, Power, knowledge, and the subjects of privacy: understanding privacy as the ally of surveillance, 17 *Information, Communication & Society*, 1258 (2014). Designation of ‘liquid surveillance’ is made by Richards *see supra* note 75. Scholars also refer to this data collection phenomenon as ‘dataveillance’, ‘datafication’ and ‘dataism’. Roger Clarke, *Information technology and dataveillance*, 31 *COMMUNICATIONS OF THE ACM* (1988). José Van Dijck, Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology, 12 *Surveillance & Society* 197(2014). Regarding the scope of such information gathering, they call ‘transaction surveillance’. Christopher Slobogin, *Transaction surveillance by the government*, 75 *MISS. LJ* 139(2005).

¹⁸⁷ Such activities are not carried out only in domestic manner, for specific trans-border data flows *see* KITTICHAISAREE. 2017.

¹⁸⁸ Regarding particularly the data retention, justification of the circumstances, accountability, and transparency should be pointed out as three main topics to focus on, similar to Wright, et al., *Computer Law & Security Review*, (2015). *See* Ryan, 3. 2016.

¹⁸⁹ Richards, *HARV. L. REV.*, 1939-40 (2013).

¹⁹⁰ van der Sloot, *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, 71-76 (2017).

unidentifiable. Secondly, the values associated with both sides cannot be considered as opposed to each other. It is implied that security stands for the general interest or public values, while the privacy stands for the individual interest. However, since the violation of privacy has occurred via enhanced technological tools, an individual is only one of the victims among the whole society. In a simple way, mass collection of data or mass surveillance in a more comprehensive manner is a threat for both public security as well as each member of the society. Therefore, privacy is easily, indeed inevitably, linked to general interests.

At this point, it should be asked: if the harm was not inherently embedded in privacy violations why would it rise a public concern and generate legislations regarding the protection of personal data?¹⁹¹ The inherent harm is argued to be risk and anxiety which should be recognized by the laws. The approach of jurisprudence and doctrine not accepting 'risk' as a privacy harm per se is criticized that many other remedies for legal offenses relied on risk, such as medical malpractice, environmental measures, drunk driving, etc. Therefore, the risk is already a reasonable and recognizable foundation in legal terms. Anxiety is similarly the underlying factor of defamation law, which is a tort law not requiring any specific suffering in physical terms.¹⁹² The judiciary might abstain from a large number of class-actions and might be unwilling to abolish the harm requirement for this reason. Nevertheless, denying the actual deficiency in privacy protection hampers the development of the law, and also prevent the law from answering rapidly and effectively to the current issues.¹⁹³

¹⁹¹ Id. at. They refer to the situation in the US; however, Europe and many other countries have adopted data protection laws as can be examined via <https://www.dlapiperdataprotection.com/index.html>. The UN Special Rapporteur gives significant attention to the issue and submitted a work in his third annual report on the expanding data protection laws. See Appendix 2: Graham Greenleaf, Data Privacy Laws 2017: 120 National Data Privacy Laws, including Indonesia And Turkey, A/HRC/37/62 (28 February 2018), available at http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix2.docx

¹⁹² Solove and Citron argues that legal foundations for risk and anxiety are already existent in the law, but for other offences than privacy. They also refer to Warren and Brandeis' 'injury to feelings' where they address tort law basics for recognition of emotional distress by the privacy violations. Daniel J Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 756-764 (2017).

¹⁹³ Id. at, 781, 784.

B. Privacy Harm Recognized by the UN

All of the presented concerns and suggestions are shared by the United Nations.¹⁹⁴ In 2014, UN High Commissioner for Human Rights delivered a report ‘The Right to Privacy in the Digital Age’¹⁹⁵. The vulnerability of digital privacy against mass surveillance by rapid innovation in technology is the main point. The Report also underlines that other fundamental human rights are also affected by mass surveillance, interception of communications and collection of personal data: freedom of expression, freedom of association, right to family life, health. Ill-treatment including torture, geolocation for lethal drone strikes through the collection and processing digital data are reported.¹⁹⁶ Big data is also discussed in the Report, and the argument that the mere collection of data would not be interference to privacy rights is not found persuasive. In this regard, *Digital Rights Ireland* is referred for its finding that certain conclusions may be drawn from the metadata which would be amount to interference; and *Weber* is referred that the mere possibility of collection of communication information constitutes an interference. The governments are supposed to prove the measures not arbitrary nor unlawful.¹⁹⁷

Since 2016, The Special Rapporteur on the Right to Privacy (SRP), Prof. Joseph Cannataci has been preparing reports to the Human Rights Council. In his first annual report, he emphasized the fact that ordinary citizens may be exposed to state monitoring measures which are indeed unnecessary, disproportionate and excessive.¹⁹⁸ Beyond the offensive measures, he drew attention to the lack of modern regulations under international law. There is not an exact definition of the concept of privacy, but further, the provisions remained from the international agreements from tens of years ago would not be sufficient to address newly emerged

¹⁹⁴ In the UN’s agenda, data protection is about to evolve into an international human right inferred from the traditional framework of the Universal Declaration of Human Rights, Article 12, and International Covenant on Civil and Political Rights, Article 17. Bignami & Resta, 3. 2018.

¹⁹⁵ UN, The Right to Privacy in Digital Age, A/HRC/27/37 (30 June 2014), available at <https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx>

¹⁹⁶ Id. para. 14

¹⁹⁷ Id. para. 20. The report elaborates on the conditions for arbitrary or unlawful actions afterwards. It also refers to Siracuse Principles, as covered in the beginning of this study, for the meaning of arbitrary and unlawful, para. 22.

¹⁹⁸ UN, Report of the Special Rapporteur on the Right to Privacy, A/HRC/31/64 (24 November 2016), para 10, available at <https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx>

conflicts.¹⁹⁹ Therefore, it was the primary conclusion that there is a need to reach a common understanding of privacy regardless of any other parameter. The Special Rapporteur undertook as a duty, in his report, to work on the more detailed and universal meaning of the right to privacy; besides, amendment of the legal instruments accordingly would be the prior issue. He stated that the protection of the right could be improved, or completely replaced through international law.²⁰⁰ This report, besides, referred to the indications by *Schrems* and *Zakharov*.²⁰¹

In his second report in 2017²⁰², the SRP mainly focused on government surveillance. Reference to the famous indication of *Tele2 Sverige* on the feeling of being monitored is note-worthy. Further, he referred to the statement of CJEU that the retention of data must be the exception for the fight against crime. Even in this case, there should be precise limitations, safeguards, and remedies for the targeted people, effective supervision and review mechanisms.²⁰³ The critic was provided in the report that *Tele2 Sverige* was a radical decision failing to strict analysis of the actual harm in the respective conflict. The SRP also agreed on the necessity of rigorous analysis on proportionality and reminds the subjective sphere of such public feelings depending on the cultures.²⁰⁴ Besides, the report put forward the principles of *Zakharov* and *Tele2 Sverige* as the model for further developments, indicating that the key requirement should be reasonable suspicion, and the key consideration should be the risk.²⁰⁵ Finally, as a recommendation, the SRP suggested a brand-new agreement for a detailed regulation on government surveillance in cyberspace for internet privacy.²⁰⁶

¹⁹⁹ Id. para 21.

²⁰⁰ Ten point action plan of the first annual report: (1) the meaning of the right to privacy, (2) increasing awareness, (3) creation of a structured, ongoing dialogue about privacy, (4) a comprehensive approach to legal, procedural and operational safeguards and remedies, (5) a renewed emphasis on technical safeguards, (6) a specially dialogue with the corporate World, (7) promoting national and regional developments in privacy protection mechanisms, (8) harnessing the energy and influence of çivil society, (9) cyberspace, cyberprivacy, cyberespionage, cyberwar and cyberpeace, (10) investing in international law. Id. para 45-55.

²⁰¹ Id. para 31 ff.

²⁰² UN, Report of the Special Rapporteur on the Right to Privacy, A/HRC/34/60 (24 February 2017), available at <https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx>

²⁰³ Id. para 14-15.

²⁰⁴ Id. para 16-18.

²⁰⁵ Particularly, the SRP advises the United States to follow European principles, in para 44-(c).

²⁰⁶ The SRP explained the efforts for a new legal instrument specifically based on the internet surveillance, in para 46-(j).

In 2018, he prepared the third report.²⁰⁷ Certain findings of the SRP were the lack of national surveillance legislation satisfying the international standards of privacy rights, and only a few countries were discussing this issue.²⁰⁸ The SRP explained how he had been working on the development of an international instrument for global surveillance standards in MAPPING Project further in the report. In Annex 7²⁰⁹ to this annual report, he submitted the draft text to the Human Rights Council. The text has been open to debate and participation, which certain opinions and concerns from the stakeholders had already been received, so that another report would be prepared in March 2021.²¹⁰ He believes that uniform instrument created by the consensus of governments and non-governmental groups could offer effective solutions for internet privacy and also jurisdiction problems in cyberspace.²¹¹

Within this third report, the SRP presented certain documents regarding his works and efforts on the issue. In his recommendation regarding big data²¹², it was stated that there is not any definition for the big data but some certain characteristics as the size of the data and particular retention methods²¹³ Through the use of algorithmic processing of data gives governments to control, target or otherwise harm certain communities. Besides, since there are so many digital means and variables, it is not probable to allocate responsibility in case of any harm. Further, since the nature of this enormous database is based on exploration, there is no initial purpose of the collection but it is to be decided at the end of the process.²¹⁴ Therefore, there is a risk posed by big data to undermine international human rights, especially regarding

²⁰⁷ UN, Report of the Special Rapporteur on the Right to Privacy, A/HRC/37/62 (28 February 2018), available at <https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx>

²⁰⁸ Id. para 103-104.

²⁰⁹ Available at http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf

²¹⁰ Id. para 116-118.

²¹¹ Id. para 127. Jurisdiction in cyberspace is another complicated issue emerged by the modern technology. For a significant example, *see* Appendix 6: Amicus Curiae to the United States Supreme Court in the Matter of the US Government Vs Microsoft Corporation, A/HRC/37/62 (28 February 2018), available at http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix6.pdf

²¹² Appendix 4: Interim Report and Preliminary Recommendations of Big Data Open Data Thematic Action Stream Taskforce, A/HRC/37/62 (28 February 2018), available at http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix4.docx. The SRP have established the Taskforce on Big Data and Open Data concentrating on the modern challenges by new methods of collecting data, 'Big Data', and governments' tendency to make such data accessible, 'Open Data'. *See id.* para 22.

²¹³ Id. para 16.36. ff.

²¹⁴ Id. para 68-69.

discrimination²¹⁵.

In the most recent report by the SRP, the issues of intelligence oversight, gender perspective to privacy and protection of health data were scrutinized.²¹⁶ The fundamental connection between privacy and other rights was set forth that the enjoyment of the other rights can be constrained by the infringements to privacy rights.²¹⁷ In the report, it was indicated that gender-based technological breaches to privacy causes serious harm to individuals such as fraud, job loss, loss of educational opportunities, constraint on freedom of movement, freedom of association, freedom of dressing oneself, freedom of parenting, reputational and emotional damages, violence, domestic violence, discrimination, imprisonment, and even death.²¹⁸

None of the arguments mean that privacy is an absolute right, on the contrary, it can surely be limited. However, any limitation to the right, or interference, cannot be arbitrary or unlawful, as reiterated by the SRP. The terms of arbitrariness and unlawfulness were explained by referring to the international human rights law instruments.²¹⁹ He also reported the developments regarding the security and surveillance including the General Data Protection Regulation (GDPR) of the European Union, and the modernization of the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).²²⁰ The report put forward two ECtHR cases which might have a worldwide impact: *Rättvisa* and *Big Brother Watch*.²²¹ The final point to be highlighted, it was stated that governments' interests are outweighed by the collective interest of society in democracy.²²² In other words, on the state's side of the coin, the interferences may occur for public security, but on the other side, there is also the public concern for democratic order. SRP shares the argument that balance between the public and individual interest does not work

²¹⁵ Id. para 73.

²¹⁶ UN, Report of the Special Rapporteur on the Right to Privacy, A/HRC/40/63 (27 February 2019), available at <https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx>

²¹⁷ Id. para 4. The report stressed that the risk to privacy posed by the governments using advanced technological measures also threatens other human rights including freedom of expression, association, and religion or belief. Id. para 33.

²¹⁸ Id. para 96-97.

²¹⁹ Id. para 11. The SRP referred to the General Comment 16 and 31 by the Human Rights Committee, European Court of Human Rights, and ECHR in the following paragraphs.

²²⁰ Id. para 27.

²²¹ Id. para 29-30

²²² Id. para 103.

anymore.

C. Counter Arguments

Privacy harm is still not an agreed notion. Either the existence or significance is denied. The traditional approach does not allow to admit the abstract nature of the concept. Some of the arguments directly on privacy harm, some concerns the societal value, and some for the concept of privacy itself.²²³

Ann Bartow has harsh criticism for Solove's taxonomy and approach to privacy harm. She finds the taxonomy too far from the real harms of privacy invasions, too involved with the doctrine, lack of enough dead bodies. She comments, on the approach of Solove, that privacy harm is restricted in theoretical terms without genuine effects beyond feelings of unease.²²⁴ Causality is explained more than the impact in the taxonomy. She asserts that the 'lack of blood and death, or at least of broken bones and buckets of money' takes privacy apart from the other torts.²²⁵

Solove responds to Ms. Bartow that privacy problems inherently are without 'dead bodies'; only a few privacy violations could be recognized otherwise. His taxonomy, indeed, does not aim to discuss consequences but rather to clarify why any interference to privacy is anyway harmful.²²⁶

Richard Allen Posner, who was a judge of the US Court of Appeals in Chicago until 2017, published an article in 2008²²⁷. It is a prominent article by the radical discourse of Mr. Posner that 'privacy is the terrorist's best friend'²²⁸. He contends that most of the disclosure of personal information is voluntarily occurred, in employing, buying insurance, bank transactions including getting a credit card or loan, even e-mailing. Privacy is already blown in an ordinary

²²³ For some of the general arguments in sum, *see* CHARLES J. SYKES, *THE END OF PRIVACY* 223 (St. Martin's Press 1st ed. ed. 1999).; DeCew, 11-16. 2015.

²²⁴ Bartow, U. PA. L. REV. PENNUMBRA, 52 (2006).

²²⁵ *Id.* at, 61-62.

²²⁶ Daniel J Solove, *I've got nothing to hide and other misunderstandings of privacy*, 44 SAN DIEGO L. REV. 745(2007).

²²⁷ Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245(2008).

²²⁸ *Id.* at, 251.

day²²⁹ He implies that privacy claims could not be raised upon personal data if they have been shared voluntarily. Apparently, he supports the third-party doctrine as a judge.

He argues for the resemblance of medical examination with the intelligence services: people are not uncomfortable with the medical examination of their bodies because it is only a professional interest of the doctor. Similarly, we can 'hope' that the intelligence service can be trusted to use its database only for national security. The people losing their privacy on the other side would be compensated by the assurance of national security.²³⁰ As a matter of fact, the search programs of intelligent services hide irrelevant data from the officers²³¹. In any case, search programs are not sentient so that they could not invade personal privacy, an only human search could.²³²

Posner finds reasonable suspicion criterion too restrictive for effective counterterrorism, especially to identify who may be involved in terrorist activities, or maybe an accessory. Even if the target is not the probable suspect, assurance is necessary by intercepting his electronic communications.²³³

Final significant suggestion from the article is to create comprehensive electronic dossiers for all the citizens in the United States, which would be periodically updated.²³⁴

Posner has another article published in the Washington Post.²³⁵ He states his opinion firstly in the Washington Post that machine collection could not invade privacy, for not being a sentient and also for processing only relevant data. Considering the public security, a counterclaim may only be the fear of misuse of collected data such as blackmailing or intimidating in other ways the political opponents. However, the government has to prevent terrorist attacks effectively, and for this reason, valuable intelligence may have to be gathered from innocent people as well.

²²⁹ He states that even Google reads all the electronic mails communicated via Gmail. It is, consequently, inevitable to be totally free from monitoring. *See id.* at, 247, 249.

²³⁰ *Id.* at, 251.

²³¹ *Id.* at, 246.

²³² *Id.* at, 254.

²³³ *Id.* at, 255-256.

²³⁴ *Id.* at, 248.

²³⁵ Richard A. Posner, *Our Domestic Intelligence Crisis* at <http://www.washingtonpost.com/wp-dyn/content/article/2005/12/20/AR2005122001053.html>.

This is because those innocent and irrelevant people may be the neighbors of targeted people and may have useful intelligence about them.

Eric Goldman, at about the same time, published a study on how can even machines be biased and managed by objectives. Even the core operations are not automated as assumed, but all the procedures are formed to be controlled according to the required data.²³⁶ Posner's opinion on the machine-based invade is already impugned unintentionally by Goldman.

However, Goldman supports the engine bias for being beneficial to optimize internet users' experience. He makes us question the automated actions but also gives us the counter-arguments for more privacy for commercial purposes. In another study, Goldman focuses on data mining for direct marketing activities. In this context, data mining is another beneficial factor for users that social welfare would improve with an effective marketing method.²³⁷ He challenges the harm of data mining that it could only cause consequential harm in case of misuse of the data.

In this manner, both Posner and Goldman agree on that data mining, without a misuse, does not pose privacy harm. Solove answers to this counter camp, directly to Posner indeed, that such an approach only focuses on the harm created by the dissemination of information such as disclosure and blackmail. However, an important point about data mining is the fact that third parties are the primary sources of personal data most of the time which means the US courts do not recognize the reasonable expectation of privacy!²³⁸

Goldman defines data mining as data aggregation and sorting for preparation of the subsequent use. He argues therefore, data mining can be deemed only as a preparatory action before the use of data.²³⁹ Also, the data subject is not aware of the preparatory steps regarding the use of

²³⁶ Eric Goldman, *Search Engine Bias and the Demise of Search Engine Utopianism*, 8 *YALE J. L. & TECH.* 188(2006). This study focuses on the 'search engine bias' that search engines do not display automated results. Goldman underlined that none of the procedures are free from human control. Eric Goldman, *Search Engine Bias and the Demise of Search Engine Utopianism*, 8 *YALE J. L. & TECH.* 188, 189-190 (2006).

²³⁷ Eric Goldman, *Data Mining and Attention Consumption*, in *PRIVACY AND TECHNOLOGIES OF IDENTITY* (Daniela Stan Raciú Katherine J. Strandburg ed. 2006).

²³⁸ SOLOVE, 192-193. 2008.

²³⁹ Goldman goes further to question the characteristics of privacy. He argues that privacy harm from data mining cannot be proven, and there is not a single authority to determine what is the fundamental right. Therefore, it is not reasonable to accept data aggregation and sorting is inherently harmful. Goldman, *Data Mining and Attention Consumption* 229. 2006.

his data. Goldman gives the ancient Zen parable at this point: if a tree falls in a forest where no one could hear, does it make a sound? Moreover, why would we care?²⁴⁰

Ryan Calo supports the same idea that if the alleged victim never knows about the data breach or other threats, there would be neither subjective nor objective harm unless the information is misused. Notification for breach might be assumed to create subjective harm in Calo's theory, but even in that case, he does not think there would be any harm. This is because the likelihood of a consequence is not the consequence itself: 'a risk of privacy harm is no more privacy harm than a chance of burn is a burn'.²⁴¹ He does not accept any increased risk of harm or vulnerability: 'a feeling of greater vulnerability can constitute privacy harm, just as the apprehension of the battery can constitute a distinct tort'.²⁴² Calo implicates that he denies the second category of harm, subjective harm, of his theory by these words. He also admits that subjective privacy harm can occur due to mental illness or coincidence.²⁴³

Calo agrees with Goldman and Posner on the consequential harm that privacy violation may cause. Behind this conclusion, there is the distinction between privacy harm and privacy violation. In this regard, he states that the efforts to define privacy harm are erred to describe privacy violation instead. It must absolutely be reminded once more at this point: 'the concept of harm is not linked to the concept of violation.'²⁴⁴

He also expresses his opinion on the societal dimension of privacy harm, and the architectural problems stemming from privacy harm, particularly by Solove. He contends that architectural harms should be categorized as divergent harms which may be composed of privacy harms together with other harms.²⁴⁵ Basically, he does not share the idea that privacy harm solely constitutes societal harm. It can only be a component of societal harms. In that case, lack of privacy may only be a contributor, for instance with ruined intellectual property regime or educational rights, to a distinct structural problem.

²⁴⁰ Id. at, 225-226.

²⁴¹ Calo, IND LJ, 1156 (2011).

²⁴² Id. at, 1158. It is ironic that two years later than Calo's work, before the District Court for the Northern District of California increasing battery usage was addressed as an injury in fact under Article III standing doctrine. In re Google Android Consumer Privacy Litig., No. 11-MD-02264 JSW (N.D. Cal. Mar. 26, 2013).

²⁴³ Id. at, 1159.

²⁴⁴ Id. at, 1159, 1161.

²⁴⁵ Id. at, 1158.

In this manner, other scholars agree with the human-specific approach to privacy harm. David Hughes narrows the privacy claims to individual concern to be harmed by misuse of information. The fear of harm matters. The harm depends on the subject's perception here.²⁴⁶ It resembles the subjective harm of Calo, but he does not deny it that radically. On the contrary, he recognizes it as the only privacy harm. He sums his theory as follows: privacy claim entails subjective harm -fear- or actual harm, if such harm is not justifiable then a privacy right can be raised.²⁴⁷ There are privacy claim, privacy harm, and privacy right: privacy claim needs unjust harm in order to become a privacy right. Privacy right seems to be used interchangeably with privacy violation. It is implied, therefore if there is justifiable harm, there would not be a privacy violation. Once more, a similar theory leads us to the distinction between privacy harm and privacy violation. However, Hughes' draw privacy violation as a subset of the privacy harm where Calo draws them as two separate sets which may have an intersection set.

The last argument is a popular saying against the claims for privacy protection: nothing to hide, nothing to fear. It shows how crucial the role of raising public awareness²⁴⁸. Many others share the idea that if they have nothing to hide from anyone, including government, they do not perceive any threat to their privacy. In fact, it conceptualizes privacy as a shield when they get involved in any unlawful activity. It reminds the arguments of Posner.²⁴⁹ Solove contends that this argument is the underlying reason for imbalance between privacy against security.²⁵⁰ This argument also reads backward as law-abiding citizens must not have anything to hide, otherwise, they should not be entitled to claim for the privacy of their illegal acts²⁵¹ The handicap is the assumption of hiding bad things behind privacy, and it overlooks the variety of privacy harms other than just disclosure of information or being monitored.²⁵²

In sum, theoretical efforts intend to guide practitioners not to overlook the multidimensional consequences of privacy violations. Some prefer to enlist those consequences one by one

²⁴⁶ Hughes, *Computer Law & Security Review*, 534 (2015).

²⁴⁷ Hughes, *COMPUTER LAW & SECURITY REVIEW*, (2015).

²⁴⁸ Stuart & Levine, *European Journal of Social Psychology*, 705 (2017).

²⁴⁹ *Supra* note 213.

²⁵⁰ Solove, *SAN DIEGO L. REV.*, (2007). Also *see* Stuart & Levine, *European Journal of Social Psychology*, (2017).

²⁵¹ Solove, *SAN DIEGO L. REV.*, 751 (2007).

²⁵² *Id.* at, 767-768.

whereas some introduce general parameters. The essential suggestion is to recognize the inherent harm of privacy by the competent authorities. It is significant that the United Nations organs also share the growing concern on the erosion of privacy rights, and even democratic institutions, by advanced technology.



Chapter IV: THE CASE FOR ABOLISHING PRIVACY HARM

The main problem of conceptualizing privacy is the drawback for recognizing inherent harm of privacy, that every breach is harmful inherently. Considering the lack of uniform understanding and regulation, both in the national and global level, three main handicaps occur. First, the privacy issue is handled differently in the constitutional context, tort law, and international human rights law. They all have their own privacy models²⁵³ contrary to the unique character of the right. Secondly, the judiciary is competent to decide on privacy issues where they could not achieve a comprehensive formula for privacy violations. There are confusing decisions even in the same jurisprudence.²⁵⁴ The debate never ends at the hands of judges. It decelerates the development of a human right, and risks to deliver justice. Thirdly, common law and civil law judicial authorities reflect their own cultures. The American approach is based on liberty whereas the Europeans embrace the dignity notion.²⁵⁵ The dichotomy does not seem to end. European Court at least struggles to provide an exception for mass violations. The US still insists on the standing doctrine.²⁵⁶ However, privacy has a global sphere of influence that apart from its universality of international human right, cross border business suffers from the divergent standards.²⁵⁷

All these three handicaps can be solved by the abolishment of the harm requirement entirely. In other words, recognizing the inherent harm of privacy would remove all these drawbacks in

²⁵³ Tort law context does not require any privacy harm in United States, *supra* notes 49, 54, 177. However, privacy harm is mostly required in the constitutional context, *see supra* note 66. European Court of Human Rights interprets the victim requirement articulated in Article 34 of the Convention according to the instant cases, *supra* note 99. In addition, David Hughes describes how three types of claims -constitutional, regulatory, tort- are available in Canada, which discusses privacy in totally different ways. Either dignitary privacy is embraced which admits privacy is intrinsically valuable, or resource privacy which is related to the consequence. *Supra* note 97.

²⁵⁴ *Supra* notes 70, 84, 89, 131.

²⁵⁵ *Supra* note 23.

²⁵⁶ Privacy harm must be demonstrated not only for standing doctrine, as an admissibility criterion, but also for the substantiate the claim afterwards. Solove & Citron, *Tex. L. Rev.*, 750 (2017). American law seems to behind the European protection of privacy. Whitman, *YALE LJ*, 1157-1167 (2003).

²⁵⁷ Personal data become the precious material of international business. Data flow, therefore, become another counterweight of privacy. It is mostly subjected to the bilateral agreements between US and Europe. *Supra* note 141. *See also* KITTICHAISAREE, 71-84. 2017. Jurisdictional conflicts often arise particularly in cyberspace. *See* UN, Report of the Special Rapporteur on the Right to Privacy, A/HRC/37/62 (28 February 2018), available at <https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx>

order for radical reform in privacy understanding and judicial practice. Recognition of inherent harm provides a huge step towards uniformity in privacy for all senses. In addition to the main drawbacks, public-private divide²⁵⁸ would be abolished. The strictly regulated field gives judiciary minimal discretion so that any conflict within the jurisprudence would be abolished. Reconciliation of common and civil law cultures may happen. Immediate adaptation of the traditional paradigm to the dynamic needs of today's privacy would be highly likely.

In order to reach this utopic picture, it must be well assessed where we stand now. From the philosophical perspective, dignity and liberty should not be a versus. In the current picture, the US is conservative in the requirement of privacy harm. It may be from the liberal thought that unless the liberty is not taken away they might not perceive a legally enforceable right. ECtHR seems to be more willing to relax the harm criterion by admitting abstract review in certain cases. However, there is still a subtle problem. Once the interference is accepted by the Court, justification grounds are to be examined where balance the interests of the individual and society is decisive. The balance, indeed, is to weigh individual harm against societal harm. Today, there is not such a sharp contrast²⁵⁹ due to the societal value of privacy and the public threat of mass surveillance, including data collection²⁶⁰. In this manner, justification grounds under the ECHR must only be interpreted narrowly and in favor of the subject not the perpetrator.²⁶¹ Therefore, liberty and dignity perspectives together may clear the hurdle by recognizing inherent privacy harm for both individual and society, and by concentrating on the strict governing of interference, rather than unfruitful discussions on the consequences of the interference.

²⁵⁸ *Supra* notes 79, 161.

²⁵⁹ *Supra* note 175.

²⁶⁰ Efforts by the UN Special Rapporteur are appreciated that he explicitly emphasizes how other human rights are dependent on the privacy protection. *Supra* notes 202-203. Types of privacy, *i.g.* private life, family life, home, correspondence, freedom from warrantless search and seizure, are also highly dependent on the informational privacy today. Surveillance does not mean physical observation of a person but mostly an electronic monitoring which includes access and collection of personal data. Interception of communication also means to collect data. The core of the right, therefore, is predominantly informational privacy. *See supra* notes 17-18, 94.

²⁶¹ As noted in *Klass* that Article 8-(2) is a guarantee against the totalitarian tendency of governments. Also *see supra* note 34. Turning to 'virtue ethics' is suggested by van der Sloot relevant at this point. Virtue ethics does not focus mainly on the subject but on the actor and its duties. Van der Sloot, 6. 2017. In the public law philosophy, the focus is on the governing activity, and the actor likewise. *See* MARTIN LOUGHLIN, *THE IDEA OF PUBLIC LAW* (Oxford University Press Oxford. 2004).

In where we stand now, it seems to be left to the individual fights against the invasion of privacy. What we need is a preventive mechanism. It is only possible with international cooperation, not only for reaching the global standard but also for the independent supervision of national practice. Such reform must be occurred in the international human rights context²⁶². International human rights law should catch the pace with the private international law; further, it may prevail over and supervise as it deserves²⁶³. Human rights law should prevail over any context in any manner, it is the essence of sustainable law and order aside from the political and commercial concerns. It surely takes time to establish that global standard for privacy, but not much more than waiting for the states to develop their own²⁶⁴. Otherwise, "harmless violations" would continue to spread.

In this regard, modernization of the Convention 108 is a significant step.²⁶⁵ It is open to any state party other than the members of the Council of Europe. Human dignity, societal value, the relation between free speech and the other human rights, global promotion of privacy, and need of international cooperation are explicitly referred in the preamble of this modernized version. Specific terms regarding data protection are defined. The public sector is also covered by the Convention. Nevertheless, it only regards data processing, does not clarify exactly what the safeguards should be, prepared with an exception clause as ECHR, and establish a committee with consultative powers.

Another significant step is the preparation of a brand-new instrument introduced by the SRP.²⁶⁶ The main purpose is to regulate state surveillance through technological means. Surveillance is defined as any monitoring or observing of persons, listening to their communications or other activities, and any collection of personal data. Further retention, analyze and use of the data are also included. It implies the attempt to create or use big data is also amount to surveillance.

²⁶² International human rights law has influence, even enforcement, on the national constitutional laws. *See* Diego Garcia Ricci, *The Contribution of International Human Rights Law to the Protection of Privacy: The Case of Mexico* *see id.* at University of Toronto).

²⁶³ Opinion 1/15 of the Grand Chamber of CJEU is an excellent example at this point. The nuance is the fact that its framework is shaped by the EU directives, protocols and data protection laws which are deemed as private law instruments. *See supra* note 143.

²⁶⁴ The SRP reports that very few country discusses privacy even after the Snowden revelations. *See* A/HRC/37/62 (28 February 2018), available at <https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx>

²⁶⁵ *Supra* note 55.

²⁶⁶ MAPPING Project, *supra* note 194.

Moreover, the activities regarded as surveillance in the instrument may also be carried out by other actors than the state itself. Addressing the public-private divide is also a significant detail of this draft. Finally, it offers to establish a supranational authority for monitoring the application of the instrument and supervising data flow among the members. There will surely be a phenomenal debate on this draft. It will be the best answer to harsh criticism that privacy harm is nothing but a theoretical discussion.

In addition to this work, it is not a far-fetched expectation to establish a body under the United Nations particularly on privacy rights. There are human rights bodies for specific fields such as discrimination, children rights, migrants, etc.²⁶⁷ Why does the UN not establish a brand-new body for such a significant and growing human right issue for privacy? That draft instrument may also lead this establishment for a designated authority to apply. It can work in cooperation with the national authorities which envisaged by the draft instrument, including the existing national data protection authorities.²⁶⁸

Apart from these efforts, the urgent need for the European Court of Human Rights, as the leading and binding international mechanism, is to harmonize its case law on the victim status of the applicants and review its analysis of Article 8-(2). Firstly, it must be clear on the admission of abstract claims regarding the intrusive acts and actions of the states. It should not be the exception of victim requirement, but the rule pertaining to Article 8. If the unwillingness to do so stem from the avoidance of possible workload, the Council of Europe must immediately start to discuss on how to resolve it in a reasonable time. Also, it should employ a super strict approach to the justification grounds for state interference by updating *Weber* criteria. Reasonable suspicion is a must in such update²⁶⁹. That strict approach also entails a very limited margin of appreciation for states, which may only be in procedural aspects. The substantial safeguards and conditions of interferences should be clearly defined by the jurisprudence, particularly on what circumstances it would not be deemed as effective

²⁶⁷ There are ten human rights treaty bodies established separately by the UN treaties. <https://www.ohchr.org/en/hrbodies/Pages/HumanRightsBodies.aspx>

²⁶⁸ Especially in the EU, each country has its own data protection authority as required by the General Data Protection Regulation.

²⁶⁹ It is possible and even being promoted to have privacy by design and by default. See Aaron Segal, *Design and Implementation of Privacy-Preserving Surveillance* (2016) Yale University.; Omer Tene, *A new Harm Matrix for cybersecurity surveillance*, 12 COLO. TECH. LJ 391(2014).

protection. The Court currently prefers to remain silent in critic evaluations.²⁷⁰

For the United States, it should be noted that opponents of the right to privacy presented in this study are American scholars. It is unfortunate that even a judge shares an extreme opinion against privacy.²⁷¹ 9/11 attack has an undeniable role in this firm position against privacy among scholars.²⁷² In the judiciary, strict application of the injury-in-fact requirement, namely Article III standing doctrine, prevents to deliver justice. In this respect, reasonable expectation and third-party doctrine create further confusion. These doctrines do not help to improve or to entrench human rights at the constitutional level. Consistent jurisprudence and abolishment of these frustrating doctrines is the urgent need for the US.

Last, but not least, a suggestion is to raise social awareness. This may even be the most practical option in the short term. All of the change offered in this study is only possible with public support. Twenty years ago, Charles Skyes shared his anticipation that sooner or later there will be a revolution in personal privacy which begins by the attitudes of individuals. The revolution can happen by a "presumption of privacy as the default setting of the information age". The first thing in this way is not the legislations but the change of "climate"²⁷³. The victory will be of privacy when we say "it is none of your business" without any hesitation.²⁷⁴

²⁷⁰ The Court confine itself most of the time to determining margin of appreciation. Wide margin is recognized in *Leander* and *Weber* to assess necessary measures under Article 8-(2). Pressing social need is one of those untouched concepts in the assessment which in *Catt* the Court finally attempt to discuss. *Supra* note 152.

²⁷¹ *Supra* note 213.

²⁷² 9/11 attack is often referred in privacy and terrorism related discussions. *See* for example Richards, HARV. L. REV., (2013).

²⁷³ CHARLES J. SYKES, 246. 1999.

²⁷⁴ CHARLES J. SYKES, THE END OF PRIVACY 257 (St. Martin's Press 1st ed. ed. 1999).

CONCLUSION

The thesis asks whether the demonstration of privacy harm is necessary to have a legal claim for the right to privacy, and it argues that harm requirement should be abolished in all terms. The approach of the thesis is of the international human rights approach.

Legal philosophy and the contested boundaries of the concept of privacy is firstly presented. The concept suffers from the lack of definition and strictly determined scope as a human right. Therefore, judges have had certain discretion to determine how to apply privacy protection in individual cases. This research focuses on how this requirement has been applied in American and European human rights jurisprudences, two major legal cultures where the privacy protection is challenged by the advanced technology. The establishment, and recent application, of the privacy harm criterion is comparatively analyzed by selected cases from the Supreme Court of the United States and the European Court of Human Rights. Court of Justice of the European Union jurisprudence is also provided for the analysis, as a reformist model and an alternative approach.

The research reveals how the US Supreme Court and the ECtHR have founded privacy harm requirement and have failed to establish consistent case law. Anyhow, the US Supreme Court insists on the strict requirement of harm, whereas the ECtHR seems to be more likely to make exceptions for privacy protection even if it is still wide of the mark. Court of Justice of the European Union, on the other hand, refers to jurisprudence of the ECtHR, but provides more extensive discussions implying the abolition privacy harm.

In addition to the comparison of case laws, this study also presents the literature specifically on the privacy harm as well as the recent developments at the level of the United Nations. Literature diverges on the privacy concept and how to solve modern privacy rights issues without any concrete harm. Scholars suggest alternative methods either to detect the privacy harm or reconceptualize it. United Nations is also aware of the fact that international human rights law falls behind the pace of technological change, and has introduced a new office for the Special Rapporteur on the right to privacy.

Nevertheless, there is still resistance to an innovative and radical thinking of privacy rights. In order to make the thesis more persuasive and reliable, the opponents' arguments against stricter

protection of privacy and abolishment of the harm requirement are included in the research. It is also helpful to well respond to possible resistance of status quo against the privacy reform by abolishing the harm requirement in international human rights. These counter arguments particularly concentrated on either the necessity of harm requirement to demonstrate a violation or the prevailing public interest against the individual privacy.

All in all, the international human rights law, including its case law, do not satisfy the immediate need for sustainable, comprehensive and reliable privacy protection mechanism. Privacy harm requirement, and indeed the traditional understanding of privacy harm, is the fundamental drawback to the improvement of privacy protection.

Reaching a global standard which excludes the harm criterion in total, recognizes the inherent harm of privacy intrusions and regulates newly emerged needs of privacy protection, would be the ultimate relief. There have already been certain efforts to amend existing agreements and even for a new international instrument. An independent human rights body for privacy violations under the United Nations is offered by this study.

Apart from these long-term goals, American and European jurisprudences on the privacy rights need to reevaluate, determine, perceive and embrace the concept of privacy harm regardless of a concrete harm or consequence in the meantime. American practice must abandon the strict harm requirement and related doctrines such as reasonable expectation of privacy and third-party doctrine. European practice must accept that the need for abstract review should not be the exception but the rule. Besides, in abstract reviews, there should also be objective criteria in order to provide a fair balance the privacy against counterweights.

Finally, in short-term, rising social awareness will be the first step towards achievement for all. Change, in every term, seems possible only by public support and awareness.



BIBLIOGRAPHY

Aaron Segal, *Design and Implementation of Privacy-Preserving Surveillance* (2016) Yale University).

Aaron Segal, *Design and Implementation of Privacy-Preserving Surveillance* (2016) Yale University).

Ann Bartow, *A feeling of unease about privacy law*, 155 U. PA. L. REV. PENNUMBRA (2006).

Avelie Stuart & Mark Levine, *Beyond 'nothing to hide': When identity is key to privacy threat under surveillance*, 47 EUROPEAN JOURNAL OF SOCIAL PSYCHOLOGY 694(2017).

Bart Van der Sloot, *Privacy As Virtue: Moving Beyond The Individual In The Age of Big Data* (2017) University of Amsterdam).

Bart Van der Sloot, *Privacy As Virtue: Moving Beyond The Individual In The Age of Big Data* (2017) University of Amsterdam).

Bart van der Sloot, *Where Is the Harm in a Privacy Violation*, 8 J. INTELL. PROP. INFO. TECH. & ELEC. COM. L. 322(2017).

Bernardo Perrián, *The Origin of Privacy as a Legal Value: A Reflection on Roman and English Law*, 52 AMERICAN JOURNAL OF LEGAL HISTORY 183(2012).

Bernardo Perrián, *The Origin of Privacy as a Legal Value: A Reflection on Roman and English Law*, 52 AMERICAN JOURNAL OF LEGAL HISTORY 183(2012).

CHARLES J. SYKES, *THE END OF PRIVACY* (St. Martin's Press 1st ed. ed. 1999).

Christopher Slobogin, *Transaction surveillance by the government*, 75 MISS. LJ 139(2005).

Christopher Slobogin, *Transaction surveillance by the government*, 75 MISS. LJ 139(2005).

Daniel J Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737(2017).

Daniel J Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737(2017).

Daniel J Solove, *A taxonomy of privacy*, 154 U. PA. L. REV. 477(2005).

Daniel J Solove, *A taxonomy of privacy*, 154 U. PA. L. REV. 477(2005).

Daniel J Solove, *I've got nothing to hide and other misunderstandings of privacy*, 44 SAN DIEGO L. REV. 745(2007).

Daniel J Solove, *I've got nothing to hide and other misunderstandings of privacy*, 44 SAN DIEGO L. REV. 745(2007).

DANIEL J SOLOVE, *UNDERSTANDING PRIVACY* (Harvard University Press. 2008).

David Wright, et al., *Questioning surveillance*, 31 COMPUTER LAW & SECURITY REVIEW 280(2015).

David Wright, et al., *Questioning surveillance*, 31 COMPUTER LAW & SECURITY REVIEW 280(2015).

Diego Garcia Ricci, *The Contribution of International Human Rights Law to the Protection of Privacy: The Case of Mexico* (2017) University of Toronto).

Diego Garcia Ricci, *The Contribution of International Human Rights Law to the Protection of Privacy: The Case of Mexico* (2017) University of Toronto).

Edward J Bloustein, *Privacy as an aspect of human dignity: An answer to Dean Prosser*, 39 NYUL REV. (1964).

Eric Goldman, *Data Mining and Attention Consumption*, in *PRIVACY AND TECHNOLOGIES OF IDENTITY* (Daniela Stan Raciuc Katherine J. Strandburg ed. 2006).

Eric Goldman, *Search Engine Bias and the Demise of Search Engine Utopianism*, 8 YALE J. L. & TECH. 188(2006).

Eva-Maria Trüdinger & Leonie C Steckermeier, *Trusting and controlling? Political trust*,

information and acceptance of surveillance policies: The case of Germany, 34 GOVERNMENT INFORMATION QUARTERLY 421(2017).

Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance. (2018).

James Q Whitman, *The two western cultures of privacy: Dignity versus liberty*, 113 YALE LJ 1151(2003).

James Q Whitman, *The two western cultures of privacy: Dignity versus liberty*, 113 YALE LJ 1151(2003).

Jeffrey Brown, *How Much Is Too Much: The Application of the De Minimis Doctrine to the Fourth Amendment*, 82 MISS. LJ (2013).

Jeffrey H Reiman, *Privacy, Intimacy, and Personhood*, PHILOSOPHY & PUBLIC AFFAIRS 26(1976).

Jeffrey H Reiman, *Privacy, Intimacy, and Personhood*, PHILOSOPHY & PUBLIC AFFAIRS 26(1976).

JEFFREY L VAGLE, *BEING WATCHED: LEGAL CHALLENGES TO GOVERNMENT SURVEILLANCE* (NYU Press. 2017).

José Van Dijck, *Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology*, 12 SURVEILLANCE & SOCIETY 197(2014).

Judith DeCew, *Privacy* In Stanford Encyclopedia of Philosophy (Stanford, CA Metaphysics Research Lab, Stanford University Spring 2015 ed. 2015).

Julie E Cohen, *What privacy is for*, 126 HARV. L. REV. (2012).

Louis D. Brandeis Samuel D. Warren, *The Right to Privacy*, HARVARD LAW REVIEW 193(1890).

Louis D. Brandeis Samuel D. Warren, *The Right to Privacy*, HARVARD LAW REVIEW 193(1890).

M Ryan Calo, *The Boundaries of Privacy Harm*, 3 IND LJ (2011).

Margot E Kaminski, *Standing After Snowden: Lessons on Privacy Harm from National Security Surveillance Litigation*, 66 DEPAUL L. REV. 413(2016).

Michael Ryan, *Persona Non Data: How Courts in the EU, UK and Canada are Addressing the Issue of Communications Data Surveillance vs. Privacy Rights* (2016).

Michael Ryan, *Persona Non Data: How Courts in the EU, UK and Canada are Addressing the Issue of Communications Data Surveillance vs. Privacy Rights* (2016).

N Pillay, *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*, Human Rights Council. Twenty-Seventh Session. A/HRC/27/37 (2014).

N Pillay, *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*, Human Rights Council. Twenty-Seventh Session. A/HRC/27/37 (2014).

Neil M Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934(2013).

Neil M Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934(2013).

Nili Steinfeld, *Track me, track me not: Support and consent to state and private sector surveillance*, 34 TELEMATICS AND INFORMATICS 1663(2017).

Nili Steinfeld, *Track me, track me not: Support and consent to state and private sector surveillance*, 34 TELEMATICS AND INFORMATICS 1663(2017).

Omer Tene, *A new Harm Matrix for cybersecurity surveillance*, 12 COLO. TECH. LJ 391(2014).

Omer Tene, *A new Harm Matrix for cybersecurity surveillance*, 12 COLO. TECH. LJ 391(2014).

Paul M Schwartz & Karl-Nikolaus Peifer, *Prosser's "Privacy" and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?*, 98 CALIFORNIA LAW REVIEW 1925(2010).

R.L. David Hughes, *Two Concepts of Privacy*, 31 COMPUTER LAW & SECURITY REVIEW 527(2015).

Richard A. Posner, *Our Domestic Intelligence Crisis* at <http://www.washingtonpost.com/wp-dyn/content/article/2005/12/20/AR2005122001053.html>.

Richard A. Posner, *Our Domestic Intelligence Crisis* at <http://www.washingtonpost.com/wp-dyn/content/article/2005/12/20/AR2005122001053.html>.

Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245(2008).

Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245(2008).

Robert C Post, *Three Concepts of Privacy*, 89 GEO. LJ 2087(2001).

Robert C Post, *Three Concepts of Privacy*, 89 GEO. LJ 2087(2001).

Roger Clarke, *Information technology and dataveillance*, 31 COMMUNICATIONS OF THE ACM (1988).

Saleh Sharari & Raed SA Faqir, *Protection of Individual Privacy under the Continental and Anglo-Saxon Systems: Legal and Criminal Aspects*, 5 BEIJING L. REV. 184(2014).

Seth F Kreimer, *Spooky Action at a Distance: Intangible Injury in Fact in the Information Age*, 18 U. PA. J. CONST. L. 745(2016).

William L. Prosser, *Privacy*, 48 CAL. L. REV. 383(1960).

William L. Prosser, *Privacy*, 48 CAL. L. REV. 383(1960).

Table of Cases

US Supreme Court

ACLU v. Clapper 14-42 (2d Cir. 2015)
ACLU v. NSA, 493 F.3d 644 (6th Cir. 2007).
Baggett v. Bullitt, 377 U. S. 360 (1964)
Baird v. State Bar of Arizona, 401 U. S. 1 (1971)
Carpenter v. United States, 585 U.S. ____ (2018)
Clapper v. Amnesty International USA, 568 U.S. 398 (2013)
Doe I v. Individuals, 561 F Supp. 2d 249, 257
Doe v. Chao, 540 US 614 (2003)
Fed. Aviation Admin v. Cooper, 132 S. Ct. 1441, 1441 (2012)
In Re: Nickleodeon Consumer Privacy Litig., No. 15-1441 (3d Cir. 2016).
Katz v. United States, 389 U.S. 347 (1967)
Keyishian v. Board of Regents, 385 U. S. 589 (1967)
Klayman v. Obama, 957 F. Supp. 2d 1 (2013)
Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010)
Laird v. Tatum, 408 U.S. 1 (1972)
Lamont v. Postmaster General, 381 U. S. 301 (1965)
Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)
Perlin v. Time Inc., No. 2:2016cv10635 - Document 27 (E.D. Mich. 2017)
Smith v. Maryland, 442 U.S. 735 (1979)
Spokeo, Inc. v. Robins, 578 U.S. ____ (2016)
United States v. Bailey, 628 F.2d 938, 940 (6th Cir. 1980)
United States v. Dubrofsky, 581 F.2d 208, 211 (9th Cir. 1978)
United States v. Jones, 132 S. Ct. 945 (2012)
United States v. Knotts, 460 U.S. 276 (1983)
United States v. Miller, 425 U.S. 435 (1976)
United States v. Moore, 562 F.2d 106, 112 (1st Cir. 1977)
Wikimedia Foundation v. NSA/CSS, No. 15-2560 (4th Cir. 2017)

European Court of Human Rights

Ben Faiza v. France, Application no. 31446/12, 8 February 2018

Big Brother Watch and Others v. The United Kingdom, Applications nos. 58170/13, 62322/14 and 24960/15, 13 September 2018

Breyer v. Germany, Application no. 50001/12

Burden v. the United Kingdom [GC], no. 13378/05, ECHR 2008

Catt v. the UK, Application No. 43514/15, 24 January 2019

Centrum för Rättvisa v. Sweden, Application no. 35252/08, 19 June 2018

Colon v. the Netherlands, Application no. 49458/06, 15 May 2012

Dudgeon v. the United Kingdom, application no. 7525/76, 22 October 1981

Evans v. The United Kingdom [GC], no. 6339/05, 10 April 2007

Georgian Labour Party v. Georgia, no. 9103/04, ECHR 2008

Hilton v. The United Kingdom, Application no. 12015/86, 06 July 1988

Johnston and Others v. Ireland, Series A no. 112, 18 December 1986

Kennedy v. The United Kingdom, No. 26839/05, 18 August 2010

Klass and Others v. Germany, no. 5029/71, 6 September 1978

Leander v. Sweden, no. 9248/81, 26 March 1987

Liberty and others v. the United Kingdom, Application no. 58243/00, 01 July 2008

Marckx v. Belgium, Series A no. 31, 13 June 1979

Michaud v. France, Application no. 12323/33, 06 December 2012

Norris v. Ireland, Series A no. 142, 26 October 1988

Odièvre v. France [GC], no. 42326/98, 13 February 2003

Roman Zakharov v. Russia, no. 47143, 4 December 2015

Rotaru v. Romania, no. 28341/95, 4 May 2000

SARL du Parc d'Activités de Blotzheim v. France, no. 72377/01, 11 July 2006

Szabó and Vissy v. Hungary, no. 37138/14, 12 January 2016

Vallianatos and Others v. Greece [GC], nos. 29381/09 and 32684/09, ECHR 2013

Weber and Saravia v. Germany, Application no. 54934/00, 29 June 2006

The Court of Justice of the European Union

Joint Cases C-293/12 and C-594/12 Digital Rights Ireland and Others, 8 April 2014

Joint Cases Tele2 Sverige AB v Post-och teletyrelsen and Secretary of State for the Home Department v Tom Watson and Others, C-203/15 and C-698/15, 21 December 2016

Maximillian Schrems v Data Protection Commissioner, C-362/14, 6 October 2015