# Privacy's Algorithmic Turn: An Intellectual History

Maria Paula Angel Arango

A dissertation
submitted in partial fulfillment of the
requirements for the degree of

Doctor of Philosophy

University of Washington
2024

Reading Committee:
Ryan Calo, Chair
Megan Finn
Meg Leta Jones
José Antonio Lucero

Program Authorized to Offer Degree:
Law

University of Washington

## Abstract

Privacy's Algorithmic Turn: An Intellectual History

Maria Paula Angel Arango

Chair of Supervisory Committee:

Ryan Calo

Law

Between 1990 and 2020, the concept of information privacy in American privacy law scholarship experienced an "algorithmic turn," gradually expanding to encompass a new set of privacy harms, as well as a different kit of legal tools. This dissertation traces, in detail, the intellectual history of this sociotechnical phenomenon. Taking the scholarly work produced around the Privacy Law Scholars Conference (PLSC) as well as earlier scholarship that preceded and inspired it as my primary object of study, I conducted document analysis of 574 law review articles written between 1990 and 2020, as well as fifteen oral history interviews with a purposely drawn representative sample of privacy law scholars. In my analysis, I take a Ground Theory approach and draw from the methodological framework of Intellectual History, following the discursive contextual approach proposed by intellectual historian David A. Hollinger.

In this dissertation I tell a history of how, over the past thirty years, the community of privacy scholars that has developed around PLSC transitioned from focusing primarily on autonomy-based

harms to raising a vast array of harms that share the following three characteristics: being *objective*, originating from the *actual processing phase* of the data cycle, and having *architectural* effects. In this process, scholars shifted twice from states of regulatory innovation and flux to those of relative convergence regarding the preferred tools to protect information privacy. Thus, while between 2000 and 2007 scholars almost unanimously supported the legal implementation of the Fair Information Practices ("FIPs") principles in order to *empower individuals*, by the end of the 2010s several of them seemed to be coalescing around a hands-on set of substantive requirements, duties, and prohibitions intended to *take power away from corporations*.

In addition, building on Science & Technology Studies (STS) literature on "imaginaries" as well as on interdisciplinary scholarship where this concept has been applied to legal endeavors, I propose the theoretical concept of "techno-legal imaginaries" and apply it to the case of the American privacy law scholars here examined. I suggest that the transformation of the scholars' techno-legal imaginaries over the period of time covered by this study can provide us with some insight into the evolution of the tools proposed by scholars to protect information privacy.

Back in the late 1990s and early 2000s, many American privacy law scholars aimed for Information Privacy law to contribute to a pluralist, free, and democratic society that promoted liberty, autonomy, and self-determination. Within that normative framework, procedural standards that gave individuals control over their personal information, such as the FIPs, stood out as appropriate. Over the years, however, scholars' techno-legal imaginaries have radically changed. Several scholars now expect Information Privacy law to promote a socially just society that besides protecting individuals' autonomy, defends the vulnerable and marginalized, protects individuals from data extraction and its consequent power imbalances, and holds corporations accountable. The most recent batch of hands-on tools makes sense within these normative commitments.

This research builds upon the Legal Construction of Technology method, to present privacy's algorithmic turn as a complex sociotechnical phenomenon, placing it within a broader context where technological, social, legal, and—as I hope to demonstrate here—cognitive elements interact and become entangled.

# Table of contents

## Acknowledgments

I would like to express my deepest gratitude to those who have supported and contributed to the completion of this dissertation. Their mentorship, feedback, support, love, and encouragement have been fundamental throughout this journey.

First and foremost, I would like to express my profound gratitude to my advisor, Professor Ryan Calo, for believing in me from the very first day I contacted him. Throughout this process, his feedback, mentorship, and constant support have been invaluable. I would also like to thank him for the numerous opportunities he has offered me. My gratitude for his generosity is beyond words.

I would also like to express my sincere appreciation to my committee members, Professors Megan Finn, Meg Leta Jones, and Tony Lucero. Their thorough feedback has been instrumental in shaping this research project and making it what it is today. The academic and emotional mentoring I have received from them has also enhanced my Ph.D. experience, making me feel supported throughout the entire process.

Furthermore, I would like to express my deepest love and gratitude to my husband, Sebastián, who has been by my side all along the way. Thank you for discussing every decision with me, celebrating my successes, and supporting me through the tough times. With love and understanding, he endured my early mornings and the many weekends I had to work. I could not have done this without him.

In addition, I would like to express my gratitude to my parents and sister for their unwavering support and understanding during these five years. Their love and encouragement have been a

constant source of strength and motivation. They have taken my dreams as their own and felt my successes and disappointments even deeper than I have. I am extremely fortunate to have them in my life.

I would also like to extend my appreciation to the staff members at the University of Washington Law School and the Tech Policy Lab for their continuous administrative support. I am particularly grateful to Alex Bolton, La Sheena Taft, and Devon Pimentelli, for their generous assistance in supporting my journey.

Lastly, I would like to express my deepest appreciation to the fifteen scholars who generously shared their time, histories, memories, and visions of the future with me. Their contributions have been incalculable and are an integral part of this research.

This dissertation would not have been possible without the support, guidance, contributions, and love of many individuals. I will always be grateful for the innumerable opportunities I have had throughout this journey, as well as for the knowledge and unforgettable experiences I gained.

# List of Tables and Figures

# INTRODUCTION

## A. Research problem

Among American legal scholars, there is a group of them—the privacy law scholars—who devote considerable time and energy to researching, analyzing, and advocating for stronger information privacy protections in the Digital Age. Their scholarship contributes to the ongoing conversation surrounding technology law and policy in the United States, and plays a significant role in shaping public debates and policymaking around these issues. Additionally, their teaching influences the intellectual development of future privacy law practitioners, which includes those who will go on to become regulators, policymakers, in-house counsels, or law firm attorneys in the field of Privacy law.

During the last thirty years (1990-2020), American privacy law scholars have written extensively about emerging technologies. From personal computers and networks to social media platforms, Big Data, algorithmic decision-making systems, and Artificial Intelligence ("AI"), over the years scholars have examined the sociotechnical legal problems posed by these technologies, as well as different ways in which the American legal system should respond to them.

Throughout this period, the concept of information privacy in American privacy law scholarship has experienced an "algorithmic turn"[1] (Angel, 2024). As algorithms have become increasingly prevalent in contemporary society, the concept of information privacy has gradually expanded, to encompass a new set of privacy harms, as well as a different kit of legal tools. To put it simply, privacy's algorithmic turn can be described as a combination of the following two main

[1] This term is inspired by the concept of "computational turn" described by Mireille Hildebrandt & Katja De Vries (2013), and builds on the concept of "algorithmic turn" previously used by Lilian Edwards and Michael Veale (2017), Ifeoma Ajunwa (2020), and Woodrow Hartzog (2021).

features: (1) a change in what is typically regarded as *privacy harm*, and (2) a transformation of the *tools proposed for protecting privacy*.

In a recent article (Angel, 2024), I have presented concrete examples (and outliers) of each of these two features of privacy's algorithmic turn, as well as discussed some possible drivers and implications of this new development in American privacy law scholarship. This dissertation serves a different but related purpose. Here, I consider the following two research questions: (1) How did privacy's algorithmic turn actually happen? and (2) What can American privacy law scholars' aspirations, expectations, and visions about the future further tell us about this turn?

Building on legal scholarship on the Legal Construction of Technology, Science & Technology Studies ("STS") literature on "imaginaries," and interdisciplinary scholarship where the concept of "imaginaries" has been applied to legal endeavors, I propose the concept of "techno-legal imaginaries" to answer the second research question. Defined as the *visions of a given legal community about the desirable futures that could be achieved through the regulation of technology*, this new theoretical term serves as an analytical construct to detach privacy's algorithmic turn from the algorithmic technologies that emerged between 1990 and 2020 and place it within a broader context where technological, social, legal, and—as I hope to demonstrate here—cognitive elements interact and become entangled.

Thus, the purpose of this research project is twofold. First, it traces, in detail, the intellectual history of privacy's algorithmic turn over a timespan of thirty years. Second, it proposes the transformation of American privacy scholars' visions about the desirable futures that could be achieved through Information Privacy law, as one of the possible reasons why the scholars' proposed tools to protect information privacy may have changed over time.

To this end, I conducted document analysis of 574 law review articles written between 1990 and 2020. Taking the scholarly work produced around the Privacy Law Scholars Conference ("PLSC") as my main object of study, I drew this sample of articles from: (i) articles that were workshopped at PLSC between 2008 and 2020; and (ii) law review articles published between 1990 and 2007 and that had been cited in one or more of the selected PLSC articles. In addition, as a triangulation point on background, I conducted fifteen oral history interviews with a purposely drawn representative sample of privacy law scholars. In my analysis, I take a Ground Theory approach and draw from the methodological framework of Intellectual History, following the discursive contextual approach proposed by David A. Hollinger (1985).

Although not the only one, PLSC is an essential event in the field of Information Privacy law in the United States. Self-described as "the premier academic conference of privacy, law, and technology scholars, researchers, and practitioners in the world" (*Privacy Law Scholars Conference,* n.d.), it was founded in 2008 by leading law scholars Daniel Solove and Chris Jay Hoofnagle and takes place annually, following a paper workshop and commentator/discussant-led format. As a result of its particular characteristics and guiding principles, the community of scholars that has developed *around* PLSC is ideally suited to be described as a "community of discourse" (Hollinger, 1985), making it a suitable focus for the intellectual history presented here.

Two caveats are appropriate at this point. Firstly, this research project does not attempt to provide *the* intellectual history of American privacy law scholarship. Rather, it tells *a* story about the evolution of the concept of information privacy used by a determined group of scholars in a specific sample of law review articles written between 1990 and 2020.

Second, this dissertation does not assume that the transformation in American privacy law scholars' techno-legal imaginaries was the *principal* or *only possible driver* of privacy's

algorithmic turn. By advancing this research project from an STS perspective, I firmly contend that privacy's algorithmic turn is a sociotechnical phenomenon (Bijker, 1994; Hughes, 1994; Jasanoff, 2004; Latour, 2005; MacKenzie & Wajcman, 1985),[2] and as such, is the result of the complex and multi-way relationship between social, technical, legal, and cognitive factors.

As the intellectual history offered here will evidence in detail, in the framework of numerous technological developments, a frenzied legal system, and an American society that almost until the end of the studied period appeared—*in the eyes of scholars*—ambivalent about the value of information privacy, between 1990 and 2020 scholars' conception of information privacy experiences two main transformations. Through indiscernible reformulations of traditional harms, proposals of new harms, and re-bounce of sparsely mentioned harms, scholars gradually transitioned from primarily focusing on autonomy-based harms, to raising a vast array of different harms. As diverse as these harms—algorithmic discrimination, procedural injustice, online manipulation, diminished exposure to differing perspectives, and subordination/oppression—would look like, they would often share the following three characteristics: being *objective*, originating from the *actual processing phase* of the data cycle, and having *architectural* effects.

In the process, scholars shifted twice from states of regulatory innovation and flux to those of relative convergence regarding the preferred techniques to protect information privacy. After a

[2] Although my work has been majorly influenced by literature from the field of Science & Technology Studies ("STS"), the sociotechnical perspective has also been adopted in other disciplines such as Communication & Media Studies (Gillespie et al., 2013) and Information Systems Studies ("ISS") (Lee, 2021; Sawyer & Jarrahi, 2014). Even though the following description was specifically crafted by Steve Sawyer & Mohammad Hossein Jarrahi (2014) for the case of ISS, its content reflects the general perspective I adopt here:

> The sociotechnical approach *eschews simplifying rationales that seek a single or dominant cause of change*. Instead, sociotechnical approaches *foreground both the complexity and the uncertainty involved in the process of technologically involved change*. In contrast to socially or technologically deterministic views, sociotechnical approaches require a detailed understanding of dynamic organizational processes and the occurrence of events over time in addition to knowledge about the intention of actors (situated rationality) and the features of technologies. (2014, p. 5-4).

first period of flux (1990-1999), when scholars seemed to agree about the harms posed by the technologies and practices of the epoch but were uncertain about what the best tool would be to address them, scholars finally arrived at a first phase of cohesion and agreement (2000-2007). During those years, scholars almost unanimously supported the binding implementation of the Fair Information Practices ("FIPs") principles, trusting in the power of procedural standards to *empower individuals*. Yet, the community's disillusionment with these principles' ability to address the newly identified harms shattered this stability within the intellectual community. After a second period of flux, by the end of 2010s scholars seemed to be entering a new phase of convergence, but this time around a batch of hands-on tools intended to *take power away from corporations*.

As this dissertation also expects to demonstrate, by understanding the scholars' techno-legal imaginaries and their transformation over time, we are better able to comprehend why a large group of American privacy law scholars ended up abandoning the FIPs-based legislative approach strongly advocated at the turn of the twenty-first century in favor of a set of substantive requirements, duties, and prohibitions. As will be seen, when thinking about what Information Privacy law should look like back in the late 1990s and early 2000s, many of the American privacy law scholars here studied aimed for a pluralist, free, democratic society that promoted liberty, autonomy, and self-determination. Yet, by the end of the 2010s—and even today, a significant portion of American privacy law scholars envision a society that besides caring about individuals' autonomy, also cares about social equality, justice, and fairness. In that sense, they expect Information Privacy law to defend the vulnerable and marginalized, protect individuals against data extraction and its consequent power asymmetries, and hold corporate power accountable.

To be clear, this dissertation is *not* arguing that in the last thirty years American privacy law scholars have contradicted themselves. Rather, what the provided intellectual history aspires to offer is the story of how the ideas about information privacy of a portion of American privacy law scholars have changed and evolved over time. As Jack Balkin properly puts it, "[f]or only through constant rethinking, in the face of changed circumstances, can we recall and rediscover what our deepest commitments truly are. What appears to be change is actually continuity; what appears to be revision is actually the deepest form of remembrance" (2004, p. 53). As a matter of fact, if ideas did not evolve, they would not be worthy of consideration in intellectual histories.

## B. Literature review

This dissertation principally looks to contribute to the literature about the history of privacy (in all its different variants). This body of literature is vast, including contributions from several academic disciplines such as Law, History, Sociology, Philosophy, and Journalism, and even from practitioners in the Privacy field. Within this body of literature, authors have usually taken one of three approaches: (i) a legal history of privacy; (ii) a social and/or cultural history of this concept; and to a lesser extent, (iii) an intellectual history of privacy.

### 1. Legal history of privacy

There is a first body of literature —legal history of privacy— (Allen, 2005; Bennett & Raab, 2006; Bennett & Raab, 2020; Bowers, 2006; DeCew, 1997; Despoja, 2007; Diggelmann & Cleis, 2014: Errera, 2011; Fernandez, 2016; González Fuster, 2014; Gormley, 1992; Lengwiler, 2004; Martin, 2014; Richards & Solove, 2007; Solove, 2006c; Twomey, 2018; Ziegler, 2018) that has tended to address what Sara E. Igo has described as "privacy's technical, juridical career" (Igo, 2018, p. 7).

Looking to explain the emergence and development of the *right to privacy* in a given legal system, these authors have mostly focused their historical explorations on precedent and policy, usually highlighting landmark court cases and the issuance of privacy statutes, such as the enunciation of privacy as a constitutional right in *Griswold v. Connecticut* or the Privacy Act of 1974.

Within this group of authors, most of them have focused their attention on the legal history of privacy **in the United States**. For example, in 1992 Law scholar Ken Gormley (1992) published a historical examination of Privacy law in the United States, which covered from Warren and Brandeis's seminal piece up through 1991. In this law review article, professor Gormley walks readers through the twentieth century, identifying and describing triggering technological advances or historical forces, consequent landmark court cases that have introduced new developments in American Privacy law, and scholarly criticism of the Supreme Court's decisions. According to Gormley, during the one hundred years after the emergence of the right to privacy scholars have been unable to agree upon a one-size-fits-all definition of legal privacy, because in its practical evolution it actually consists of the following five distinct species: (i) Tort Privacy; (ii) Fourth Amendment Privacy; (iii) First Amendment Privacy; (iv) Fundamental-decision Privacy; and (v) state Constitutional Privacy. Notwithstanding their differences—the author argues—these species are heavily interrelated as a matter of history, "owing their origins to the same soil" (p. 1357).

Similarly, in one of the chapters of her book *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, Philosopher Judith Wagner DeCew (1997) discusses the history of privacy protection in American law, by drawing from several court cases in which the right to privacy has been protected either under Tort or Constitutional law ("two-pronged development of privacy protection" (DeCew, p. 2)). In DeCew's view, despite seeming like separate interests, these two

sets of privacy cases, which she refers to as the "tort interest in privacy" and the "constitutional right to privacy" (DeCew, p. 25), have a common foundation.

Another example of legal history of the right to privacy in America is *A Brief History of Information Privacy Law*, from Law scholar Daniel Solove. Published in 2006, this article addresses the origins and growth of the law of Information Privacy in the United States. Spanning from the first days of Colonial America and up through the data security breaches of 2005, Solove describes the social and technological developments, court cases, influential scholarship pieces, and federal statutes that have given rise to the American Information Privacy law.

However, within this first body of literature also exist pieces of scholarship that have addressed the legal history of privacy **in other parts of the world**. For instance, Political Scientists Colin J. Bennett and Charles Raab have published two pieces (a book (2006) and much later an article (2020)) tracing the evolution of the governance of privacy from a global perspective. historian Martin Lengwiler (2004), in turn, examines the recent history (since the 1970s) of privacy legislation in the European context in general, and in Switzerland in particular. Specifically, the author describes how the legal concept of privacy in Europe has been redefined over the past decades, from an individualistic to a social concept. In a similar fashion, Law scholar Gloria González Fuster (2014) traces the emergence of personal data protection as a fundamental right in the European Union. Similarly, Argentinean Law scholar Marianela Fernandez (2016) addresses the history of the legal protection of privacy in the Western Civilization, covering Ancient Greece, the arrival of Christianity, the Middle Age, Modernity, and Postmodernity. Likewise, Law professors Oliver Diggelmann & Maria Nicole Cleis (2014) explore how the right to privacy became an international human right in the years after World War II, when the human rights system was devised. Finally, there are two relevant pieces from politician and advocate Natasha Stott

Despoja (2007) and French Conseiller d' Etat Roger Errera (2011), who addresses the legal history of privacy law in Australia and France, respectively.

## 2. Social and/or cultural history of privacy

On the other hand, a second and larger body of literature—social and/or cultural history of privacy— (Barbas, 2015; Cappello, 2019; Clearwater & Hughes, 2013; Cohen, 2017; Davies, 1998; Flaherty, 1972; Friedman, 2007; Garrow, 1994; Igo, 2015; Igo, 2018; Kennedy & Alderman, 1997; Keulen & Kroeze, 2018; Lane, 2009; Lepore, 2013; Marshall & Thomas, 2017; Moore, 1984; Nelson, 2002; Palmer, 2011; Richardson, 2017; Rosen, 2001; Rosenberg, 1969; Rule et al., 1980; Seipp, 1978; Sylvester & Lohr, 2005; Vincent, 2016; Webb, 2007) has focused on studying the development of the *concept of privacy*, as a broader term. Like in the first body of literature, this group of authors tends to underscore the importance of landmark court cases and statutory developments in the history of the concept. However, their sources of information go usually further, exploring historical events, opinion polls of laypeople and amateurs, public records, news sources, and other scholars' publications, which shed light on the value and significance that this concept has acquired (or lost) over time in politics and social life in general.

Among this second group of authors, the vast majority are focused on the social and/or cultural history of privacy **in the United States**. One of the most recent and therefore famous accounts is *The Known Citizen: A History of Privacy in Modern America*, by historian Sara E. Igo (2018).[3] Covering the twentieth century, from the era of the instantaneous photograph to the early

[3] Even though Igo's work is classified here as part of the social and/cultural histoy of privacy, it is important to highlight that Igo herself describes her methodology as "free-range intellectual history," which "entails foraging, for both thinkers and texts, in pastures at some remove from the traditional precincts of intellectual history" (Igo, 2016, p. 324), and which is useful for studying historical ideas that sneak out of intellectual, disciplinary, and institutional spheres to become "publicly claimed" and "popularly shaped" (Kloppenberg et al., 2016, p. 12).

years of the age of Big Data, Igo offers "a wide-angle view of privacy as Americans have argued and imagined it" (2018, p. 5). Thus, by paying attention to privacy's significance as a cultural sensibility and public value, Professor Igo examines privacy's appearances in the U.S. public sphere, seeking to trace how "citizens' understandings of and feelings about privacy have evolved over time" (2018, p. 7). In this way, Igo argues that although it became more insistent as the century advanced and as novel information technologies appeared, the "problem of the known citizen" (i.e., "Who should know us and how?—along with its corollary: What might be altered by other's possession of that knowledge?" (2018, p. 350)) has always been the same. In that sense, although it is true that information technologies' capacities have become more sophisticated over the years, "[a] sense that Americans are known too well by government and corporate entities alike is not unprecedented. It was a discovery of the 1890s and then again of the 1930s and the 1960s" (2018, p. 357).

A year later, historian Lawrence Cappello (2019) published a similar overview of the social and/or cultural history of privacy in America, "from the Gilded Age to the internet age" (Cappello, 2019, p. 3). Yet, instead of using chronological order, Cappello uses a thematic approach to address the following five privacy debates that have come up in the legal, social, and cultural realms and which have captured the attention of the American public: (i) privacy and the proper limits of a free press, driven by modern photojournalism; (ii) privacy versus national security, propelled by the many military conflicts of the twentieth century; (iii) privacy and physical surveillance technologies, boosted by government intrusions on civil liberties; (iv) privacy and Big Data (large scale data collection), caused by the rise of the welfare state, the wars on poverty and crime, and the commercialized data collection; and (v) privacy and reproductive rights, forced by new understandings of gender and the body, and which ended up in the constitutionality of the right in

1965. Cappello explains how, in all these debates, which usually took place between privacy advocates and the proponents of legitimate countervailing public interests, Americans met the different threats to privacy with a sense of ambivalence. As a result, "American understandings of privacy grew increasingly complicated over the twentieth century, and much harder to keep track of, because they were continuously being refashioned to meet new threats" (2019, p. 4).

The social and/or cultural accounts of privacy in the United States, however, have a much older pedigree. In fact, back in 1973 historian David H. Flaherty (1972) published the book *Privacy in Colonial New England 1630-1776*, which emerged from his Ph.D. dissertation. There, Flaherty explores the existence of the concept of personal privacy in colonial New England, from its first settlements to the eve of the American Revolution. Thus, through the analysis of family, courtroom, and church experiences of the colonial community, Flaherty examines the influence of the Puritans in the development of "a full-blown recognition of the need for personal privacy" (1972, p. 3).

Relatedly, in his book *Liberty and sexuality: The right to privacy and the making of Roe v. Wade*, historian David J. Garrow (1994) describes the legal and political struggles that led to the protection of a woman's constitutional right to choose abortion in Roe v. Wade (1973), and which started back in 1940 with Connecticut's struggle for the legalization of birth control. Thus, beginning with the earlier battles against statutes that criminalized birth control, Garrow follows the effects of Griswold v. Connecticut and the evolution of sexual privacy in general up through 1993. In doing so, he especially focuses on the story of activists, plaintiffs, and attorneys who fought for and filed America's first sexuality rights cases, as well as in the discussions that took place inside the United States Supreme Court.

Also focusing on judicial decisions, in 1997 Law scholars Ellen Alderman and Caroline Kennedy (1997) told the stories of ordinary people who struggled to protect their right to privacy in American courts. Similar to Cappello, rather than following a chronological order, the authors group historical privacy case law as follows, according to the different interests that are constantly trying to override this right: (i) privacy v. law enforcement; (ii) privacy and yourself; (iii) privacy v. the press; (iv) privacy v. the voyeur; (v) privacy in the workplace; and (vi) privacy and information. In each case, they explore the story behind, trying to understand both the facts and the human assumptions about privacy that finally gave way to the judicial decisions there described. According to the authors, "as much as we cherish our privacy, it does not always triumph. There are many intrusions which cause great personal pain but are not legally actionable" (1997, p. xv).

In a more ambitious way, legal scholar Frederick S. Lane (2009) tells the 400-year history of the right to privacy in America and the grave threats to its continued existence. According to the author, "the history of America *is* the history of the right to privacy" (2009, p. 1) and "[i]n ways both large and small, the formation of this country was a ringing declaration of the importance of personal privacy" (2009, p. 3). Beginning with the privacy of postal communications in colonial America and covering up through the USA PATRIOT Act of 2001, Lane shows how, over time, the questions of privacy in American society have evolved from "[i]s my home secure against governmental invasion?" and "[h]ave my letters been opened?" to "how can we protect our personal information and individual privacy in a world in which we are rapidly becoming prolific self-publishers, a world where copying is essentially free and data can live forever in a constantly expanding universe of hard drive space?" (p. 262-263).

In this body of literature about the social/cultural history of privacy in the United States, special attention should also be paid to works that trace the history of technologies and practices that have affected privacy. While none of these histories are specifically concerned with privacy, the influence of those technologies and practices on its faith makes them in many ways histories of privacy. Among others, the technologies and practices covered by these works include mass amateur photography (Jenkins, 1975; Mensel, 1991; Newhall, 1949; Oliver, 2007), consumer credit reporting (Lauer, 2010), retail data mining (Lauer, 2012), the Internet (Hafner & Lyon, 1998; Harris, 2014; McCullough, 2018), "cookies" (Jones, 2020; Jones, 2024), the Big Data revolution (Jones, 2015), the "commercial privacy industry" (Draper, 2015), as well as broader sociotechnical phenomena such as "[t]he Googlization of everything" (Vaidyanathan, 2011), "the commercial development of technologies of surveillance" (West, 2017, p. 21), Silicon Valley (O'Mara, 2019), and "surveillance capitalism" (Zuboff, 2019).

Even though a minority, there are still other authors within the body of literature reviewed in this second Sub-Section that have addressed the social and/or cultural history of privacy **in other parts of the world,** such as the United Kingdom, the West, or the Ancient World. For example, historians David Vincent (2016) and Deborah Cohen (2017), and Law scholars Daniel Marshall & Terry Thomas (2017) and Megan Richardson (2017) have all advanced social and/or cultural histories of privacy in the United Kingdom. Interestingly, among them, historians have focused their studies on the development of the concept of privacy within reduced units of analysis, such as the domestic domain or the family.

## 3. Intellectual history of privacy

The third and last body of literature—intellectual history of privacy—(Glancy, 1979; Leebron, 1991; Richards & Solove, 2010) is much more reduced.[4] Primarely, these efforts have been focused to date on investigating the formation, structure, and impact of the concepts proposed by the authors of canonical works about privacy in America.[5]

For instance, in 1979, Law scholar Dorothy J. Glancy published an article that sought to comprehend the original concept of the right to privacy, by putting in historical perspective Warren and Brandeis's original conception of the right. Thus, in an attempt to understand why these authors ended up proposing a legal theory for enforcing the right to privacy, Glancy explores who its inventors were and how their epoch (the late nineteenth century) looked like. According to Glancy, the intensity and complexity of life, the advances in technology, the intensified newspaper

[4] Here, I will refer exclusively to scholarly pieces where the intellectual history of privacy is the main event. However, it is important to acknowledge that intellectual summaries of privacy do occur in other works. In particular, many scholars have offered brief recounts of privacy scholarship in order to further expand on them or to distinguish their own lens by reference to prior understandings. See, for example, Anita Allen's (2000) recount of the privacy-control paradigm described by Professor Paul M. Schwartz; Paul M. Schwartz & William Michael Treanor's exposition of the theoretical work inside and outside of the legal academy that has pointed to a "new privacy" (2003); Adam Moore's recapitulation of the different accounts of privacy (2008); Woodrow Hartzog's discussion of the role of confidentiality in scholarship (2014); Seda Gürses's & Joris van Hoboken's (2017, p. 2-3) categorization of the three different approaches taken by privacy scholarship; and Ignacio N. Cofone & Adriana Z. Robertson's recount of the normative conceptions privacy (2018).

[5] There have been, though, two *attempts* to advance intellectual histories of broader communities of privacy thinkers. In 2015, Law professors Robert Sprague and Kevin Grauberger, and Data Scientist Nicole Barberis workshopped at PLSC a draft of a paper titled *One Hundred Twenty Years of U.S. Privacy Law Scholarship: A Latent Semantic Analysis* (2015). Although finally never published as an article, in this piece—available online—the authors used probabilistic topic modeling "to reveal the evolution of fundamental U.S. privacy law concepts expressed in the legal literature published from 1890 through 2013" (2015, p. 2). According to their analysis, "privacy law in the United States comports most closely with the Georgia Supreme Court's 1905 description of privacy from the seminal case Pavesich v. New England Life Insurance Company: 'the right of a person to be secure from invasion by the [government or] public into matters of a private nature'" (2015, p. 3).
The second attempt was made by Law scholars Meg Leta Jones and Karen Levy, and Reference Librarian Ellen Kaufman. At PLSC 2018, these scholars workshopped a draft of a paper titled *Methods to Our Madness: An Interdisciplinary Reflection on 10 Years of Privacy Scholarship* (2018), which intended to map and trace the evolution of the different research methods used in the privacy scholarship discussed at PLSC over the years. As will be seen in the Research Methods section of this dissertation, although this draft was never published and is not publicly available, thanks to the generosity of its authors the database constructed for its purpose was one of the basic inputs for the document analysis advanced in the present dissertation.

enterprise ("newspaperization" (1979, p. 8)), the long-standing assumption on the part of social, political, and legal commentators that there was a clear line of demarcation between the private and the public, the long tradition of American individualism, and the need to protect the individual from the "constituted authority" of the government, were among the major causes that set the stage for the invention of this new legal concept.

Similarly, but from the perspective of Tort theory, in 1991 Law scholar David W. Leebron (1991) looked to trace the conceptual basis of the tort right of privacy in America, its theoretical and historical pedigree, and its resulting destiny. For doing so, he "explores the theory of tort law implicit in the Warren and Brandeis article, its relation to the intellectual developments in the law at the time, and its subsequent influence on the law" (Leebron, 1991, p. 770). Therefore, in his article Leebron addresses the intellectual landscape of tort law in the United States prior to the Warren and Brandeis article, the origins of this famous article, and the conceptual approach to Tort law (and the common law) on which it is based, its immediate and long term impact (in particular its influence on Constitutional law), and the nature of the theoretical disputes in which it became embedded. According to the author, part of the current vulnerability of Warren and Brandeis's article and proposed right to privacy lies in our failure to identify and address its underlying theory. In particular, over time we have missed that "they did not identify a new tort, but rather a new right that ought to be protected by tort law. That new right, in turn, was derived from an old right, perhaps a natural right, namely the right to be let alone" (1991, p. 807). In that sense—he argues, as long as invasion of privacy is viewed as an intentional tort rather than as a constitutional right, it is condemned to lose the battle when faced with constitutional challenges.

Almost 20 years later, Law scholars Neil M. Richards and Daniel J. Solove (2010) conducted a critical assessment of William Prosser's legacy to the American law of privacy, in

Tort law as well as more generally. According to them, Prosser's legacy is a mixed one. On the one hand, he shaped the privacy torts into their current form, giving them the order and visibility that only a scholar of his influence could have done. On the other hand, he "bears at least some responsibility for the failure of the privacy torts to evolve in response to the technological and cultural developments of the last fifty years" (Richards & Solove, 2010, p. 1889).

***

To be clear, the works that are part of this third body of literature are not the only ones that have alluded to early, landmark privacy scholarship. Almost every work about the legal history and the social and/or cultural history of privacy highlights Warren and Brandeis's famous 1890 law review article *The Right to Privacy* as an authoritative piece. Equally, William Prosser's Tort Privacy scholarship, and in particular his 1960 article *Privacy*, has often been cited as one of the milestones in both the legal and social/cultural history of privacy in the United States (Palmer, 2011; Richards & Solove, 2010). As pointed out by Neil M. Richards and Daniel J. Solove in 2010, "[w]hereas Warren and Brandeis planted the germinal seed for tort privacy, Prosser systematized and organized the law, giving it an order and legitimacy that it had previously lacked" (2010, p. 1888). Similarly, *Privacy and Freedom* by Alan Westin (1967) has also been repeatedly characterized by this literature as a path-breaking book (Clearwater & Hughes, 2013; Lengwiler, 2004; Rule et al., 1980), by becoming "the framework for the future field of informational privacy (…) [as well as] the conceptual background upon which many of the U.S. privacy laws of the seventies were built" (Clearwater & Hughes, 2013, p. 899). Even, Arthur R. Miller's 1971 book *The Assault on Privacy* has been identified as exercising an important source of influence over subsequent discussion and legislation on protecting privacy from computer technology (Rule et al., 1980).

Besides, in the legal and social/cultural accounts of the history of privacy, it is also common to see a reference to the reactions that Law scholars, in general, have had to important court cases or legislative developments. For example, in his book Garrow (1994) pays special attention to the academic reactions that Law scholars had to each of the court cases addressed there, and which were expressed in a variety of academic publications and op-eds. In a similar way, within his article Gormley (1992) includes scholarly criticism of the Supreme Court's decisions.

Nevertheless, there seems to be little, or almost none published literature that purposely addresses the role of law scholars as a community—rather than as outstanding individuals—in the history of privacy. In the same way, there is a lack of literature that intentionally studies what has happened to the scholars' "thinking" (Igo, 2018, p. 11) about privacy, or how the concept of privacy has been transformed throughout the privacy scholarship. Thus, even if law review articles have been a common source of information for the aforementioned historical accounts, Law scholarship has rarely been the main object of study of published pieces.

This omission in the literature is of particular relevance, given the significant role that law scholarship has played in American Privacy law, both through direct and indirect means.

As of *direct* means of influence, at many points in time privacy scholars have had remarkable impact in privacy public policy in the United States. If thinking about earlier scholarship, it was already mentioned how Warren & Brandeis's famous article *The Right to Privacy* (1890) as well as Prosser's *Privacy* (1960) played a major role in the birth and further development of Privacy law in America. Relatedly, after publishing his article *The Assault on Privacy* (1971), Law scholar Arthur R. Miller was appointed in 1973 to serve as part of the Advisory Committee on Automated Personal Data Systems, which recommendations, included in the report "Records, Computers, and the Rights of Citizens" (1973) issued by the United States

Department of Health Education and Welfare (HEW), were later mirrored in the Privacy Act of 1974.

Moreover, thanks to the oral history interviews conducted for this project I could collect tens of other examples of additional and more recent situations where scholar's ideas have ultimately impacted regulation.[6] This, usually by means of "Amicus Briefs or legislative testimonies, op-eds, public policy statements, white papers, FTC comments (…)" (N. M. Richards, oral history interview, April 14, 2023).

In fact, many of the interviewed scholars showed themselves proud of the "regular, sustained, cross-pollination" that over the years has existed between privacy scholars and legal practitioners,[7] and which, in their view, is not "as common in other areas of law as in Privacy Law" (N. M. Richards, oral history interview, April 14, 2023). As Daniel Solove would clearly state:

> the general sense in academia is that practitioners don't care about what academics do, and that academics don't really talk much to the practitioners, and there's this, they're siloed. *But in privacy they're not*. And *I found just wonderful interest among practitioners, and people are listening, regulators and policymakers and folks in-house and external counsel*. (D. J. Solove, oral history interview, February 26, 2023)

[6] Scholar Priscilla Regan, for example, was hired at the Office of Technology Assessment (OTA) to do a study on civil liberties and electronic surveillance requested by a Senate and a House committee, which report was later the basis for the passage of the Electronic Communications Privacy Act. Similarly, Anita Allen was for seven years a member of Barack Obama's Bioethics Commission, and as a result, her "ideas about privacy are very much visible in some of the reports that that body issued" (A. L. Allen, oral history interview, March 30, 2023). Likewise, Neil Richards was retained by the Data Protection Commissioner (DPC) of Ireland (the winning party in the case) as independent expert witness in Schrems v. Data Protection Commissioner. Woodrow Hartzog, in turn, was invited to testify in DC as a consequence of the publication of the paper *The FTC and The New Common Law of Privacy*, which he co-authored with Daniel Solove. And even if not in direct contact with an agency, according to Chris Hoofnagle's and Paul Ohm's own accounts, while Hoofnagle's 2003 article *Big Brothers, Little Helpers* "put on the map the problem" of the public sector getting its data from the private sector (C. J. Hoofnagle, oral history interview, September 8, 2023), Ohm's UCLA Law Review article *Broken Promises of Privacy* "introduced the legal world—and not just legal scholars, practitioners gobbled up that article—to the problem [of the failure of anonymization], and also pushed them really hard on the solution" (P. Ohm, oral history interview, September 22, 2023).

[7] Throughout this dissertation, the term "legal practitioners" refers to those who, as opposed to academics/scholars, *practice* law as regulators, policymakers, in-house counsels, or attorneys for law firms.

Hence, in contrast to other fields of law, the close relationship between American privacy law scholars and other stakeholders in the privacy field has enabled them to expand their ideas beyond the confines of law review articles and put them into action.

When it comes to *indirect* means of influence, there are at least two other ways in which Privacy law scholarship continuously impacts Privacy law in America. First, as regular members of their Advisory boards, scholars are frequently consulting with advocacy groups such as EPIC and the Center for Democracy and Technology (CDT), whose main mission is in turn to influence policy. Second, through the Information Privacy Law courses they are teaching nowadays at US universities, as well as the textbooks a few of them have created for this purpose (e.g., Anita Allen, Daniel Solove & Paul Schwartz, and William McGeveran) and which their colleagues use in their own courses, the American Privacy law scholars here studied are constantly transmitting their ideas and approaches to JD students who might later become practitioners, public servants, legislators, or even judges. As eloquently described by Andrew Selbst in his oral history interview,

> [t]he stuff that gets taught in privacy classes, right? People who took privacy classes, again, which have only been a mainstay of legal education for maybe 15 years, or maybe even less than that. But *some of those people are in, like, they're all reading things that, you know, people in our community published, in those classes. And then now they're going to like AG's offices, they're going to these places where… or law firms thinking about privacy, where they have these ideas about privacy that came from academia in a lot of ways*. (A. D. Selbst, oral history interview, October 26, 2023)

Consequently, although sometimes overlooked in the face of more direct means of influence in public policy, Information Privacy Law courses offered at universities are another powerful means through which American privacy law scholars spread their ideas and shape the privacy field.

In light of these different examples of American privacy law scholarship's direct and indirect influence on Privacy law in America, the gap in the literature mentioned above seems

problematic. To put it simply, this inattention might be making American society lose sight of other "Warrens," "Brandeises," "Prossers," "Westins," or "Millers" who, either individually or collectively, may be: (i) finding the current state of the law and the existing conceptions of privacy unsuitable for a post-algorithmic time period; (ii) proposing persuasive alternatives that can propel disruptive changes in the very nature and conception of privacy; and (iii) devising and transmitting legal rationales that courts, federal or state legislatures, or legal practitioners will eventually employ in drafting both regulation and self-regulatory interventions. Filling this gap, therefore, is precisely the goal of this dissertation.

Finally, it is also interesting to note how these different accounts of the history of privacy have tended to stop short with the Big Data era (around 2014). As will be seen in Chapter V of this dissertation, since the advent of Big Data, privacy has had to grapple with many other algorithmic-based sociotechnical systems, being social media platforms, the Internet of Things, algorithmic decision-making systems, and Artificial Intelligence among the most disruptive. Therefore, another reason why the conduction of this research is novel and hopefully significant is because, unlike previous efforts by others, it also intends to cover privacy's interaction with these novel technologies and practices.

## C. Methodological framework

Although the pursuit of intellectual histories in Law is not new,[8] the vast majority [9] of the works of this type within this discipline has very few explicit methodological pronouncements that permit the reader to gain a deeper understanding of how their authors proceeded in tracking human thought.

In an effort to avoid these omissions, in this research I explicitly drew from the field of Intellectual History to inform my methodological framework. Although "intellectual historians can claim today no widespread agreement about how to conduct their work, and they often seem to lack the will to argue out the alternatives" (McMahon & Moyn, 2014, p. 4), it can be said that in terms of methodology their field has mainly followed two different trends: an internal and an external or contextualist approach.

Unlike the internal approach,[10] which focuses on traditions of thought, the contextualist approach looks to place ideas in context, drawing on a "variety of methods associated with the turn

[8] In addition to intellectual historical accounts of the right to privacy mentioned in the Literature Review section, intellectual histories have also been proposed for, among other concepts, the legal concepts of freedom of contract and regulation (Micklitz, 2015); freedom of movement (McAdam, 2011); juvenile court (Feld, 2016); prior acquittal sentencing (Murray, 2010); the criminal trial jury (Cockburn & Green, 1988); unjust enrichment (Harvard Law Review, 2020); judicial empathy (Fissell, 2016); judicial engagement (Tushnet, 2011); judicial activism (C. Green, 2008); Tort law (White, 1980; Hackney, 2014); Comparative Tax law (Brooks, 2020); European Private law (Hondius, 2010); German Administrative law (Meinel, 2007); International law as a research field (Lange, 2012); and Law and Economics (Priest, 2020).

[9] Edward White's intellectual history of Tort law (1980) can be highlighted as an exception. In the introduction of his piece White clearly states: "This book has sought to combine four perspectives: one from intellectual history, somewhat modified for my own purposes; one from scholarship on the sociology of knowledge; one from scholarship on the phenomenon of professionalization in late nineteenth- and early twentieth-century America; and one from the recurrent concerns of tort law during its history as a discrete field." (p. xxiv). In addition, he later claims: "I view the influence of these ideas as a sociological phenomenon, linked not to the inherent soundness of the ideas but to the institutional context in which they have appeared. In this sense my approach to intellectual history resembles that of the sociologist of knowledge" (p. xxv).
Kim Brooks's work on the intellectual history of comparative Tax law (2020) can also be named as an exception. In his piece, Brooks explicitly points out: "Comparative tax law has an intellectual history, told in this article using the social history of ideas tradition and by embracing the global turn in intellectual history studies" (p. 652).

[10] Looks for traditions of thought, following ideas across temporal frontiers and tracing them "in terms of an inner dynamic, or familiar logic" (Kelley, 2005, p. 156), with disregard of the distinctive contexts in which those ideas appeared or were applied.

to discourse, culture, and language" (Wickberg, 2018, p. 306). Thus, authors that are part of this trend have focused their attention on understanding how ideas have been shaped by different types of contexts. According to the authors who are part of this approach, "for any given idea we can only understand the meaning of that idea if we reconstruct the unique sphere of meanings to which it once belonged" (Gordon, 2014, p. 32).

Since the main subject matter of the present historical study is the *arguments* of scholars around information privacy, for the purpose of this study I have followed a contextualist approach known as the **discursive context of thought**. This approach, which "became normative [in the field if Intellectual History] by the late 1980s, and remains broadly influential today" (Burgin, 2016, p. 354), holds as its "simple methodological postulate that 'arguments are social acts'" (Hollinger, 1985, p. ix).

Proposed by David A. Hollinger (1985), this historiographical tradition studies *the* intellectual *conversations* to which ideas are contributed. More specifically, it is concerned with "the performance of minds in [the] discourse" of intellectuals[11] (Hollinger, 1985, p. 131). Thus, taking "discourse" as the communicative context within which ideas should be understood, this approach considers that "*discourse* and *the communities formed around it* are 'central subjects' as authentic as are ideas and the texts in which ideas are embedded" (Hollinger, 1985, p. 134). For the purpose of this study, it is worth briefly discussing each of these two central subjects.

[11] "In our historiographical tradition, then, the 'discourse of intellectuals' is identified chiefly by the extent to which participants draw upon and bring into precise focus the theoretical knowledge, literary and religious traditions, and other cultural resources that historians know to have been accessible to the most well-informed members of a given society at a given historical moment" (Hollinger, 1985, p. 146).

## 1. Discourse

When explaining the role of *discourse* within this historiographical tradition, Hollinger would point out:

> By identifying "discourse" as a basic subject matter of inquiry I intend several implications. Discourse is a social as well as an intellectual activity; it entails *interaction between minds*, and it revolves around *something possessed in common*. Participants in any given discourse are bound to *share certain values, beliefs, perceptions, and concepts—"ideas,"* as these potentially distinctive phenomena are called for short—*but the most concrete and functional elements shared, surely, are questions.* (…) questions are at the active heart of the discourse. Questions are the point of contact between minds, *where agreements are consolidated and where differences are acknowledged and dealt with*; questions are the dynamisms whereby membership in a community of discourse is established, renewed, and sometimes terminated. (1985, p. 132)

Thus, within this approach "ideas are viewed in their capacity as answers to *questions* shared with other persons" (Hollinger, 1985, p. 132). According to Hollinger, a historical account of discourse should begin by identifying the extent to which the writers of a given group of texts share questions. For doing so, it should necessarily explore whether a given person, through whatever they wrote, *intended* to speak to a given question. Nevertheless, instead of focusing on "the complete recovery of all the intentions behind a work," or on "the rigorous determination of the author's hierarchy of priorities" (1985, p. 143), historians following this tradition are specially interested in understanding how texts "functioned in the designated community of discourse" (1985, p. 144).

## 2. Communities of discourse

From Hollinger's description of discourse, one can also deduce that *the communities formed around discourse* share both (i) certain ideas, understood as values, beliefs, perceptions, and concepts; and (v) questions. In addition, while surveying three well-known works of intellectual

history as examples, Hollinger would provide the following additional characteristics of a community of discourse:

> It will scarcely have gone unnoticed that the examples I am using address, in each case, *a discourse carried on predominantly in verbal form* among *disputants who were essentially peers*, *who were cognizant of each other's views*, and *who shared both a language and what we could loosely call, (...) a national culture*. (…) The notion of a community of discourse need not be given so restricted a denotion, but I begin with works of this sort because so many studies of intellectual history do, in fact, operate within these perimeters. (1985, p. 137).

Accordingly, if the most restrictive approach is adopted, the "communities of discourse" that Hollinger proposes to study are composed of disputants who: (i) are essentially peers; (ii) are cognizant of each other's views; and (iii) share a language and a national culture. In addition, (iv) the interaction among its members is usually carried on predominantly in verbal form.

As explained by Hollinger (1985), the term "community of discourse" can be applied to "communities with varying degrees of commitment to the ideal of rationality" (Hollinger, 1985, p. 141). As such, the term should not be used solely to refer to a group of men and women of words whose chief business is to logically and rationally argue. Yet, "it is in relation to studies of this kind that the word 'discourse' makes the clearest intuitive sense" (1985, p. 140).

***

Therefore, although not explicitly articulated by Hollinger as so, a revision of his work appears to suggest that, when conducting a **study of the discourse of intellectuals**, historians should look to identify, at least: (i) the boundaries of the "community of discourse" under study; (ii) the shared questions involved in the conversation; (iii) each text's function in the discourse; (iv) the evolving constitution of the questions supposedly involved in the conversation; (v) the succession of

conflicts, disputes, discussions, and arguments that take place among the community members;[12] and (vi) the salient perceptions, commitments, values, and attitudes that are shown by the participants.

As will be seen in Chapter I of this dissertation, the community of scholars whose work I study here lends itself well to be characterized as a "community of discourse" (element (i)). Likewise, in the process of conducting this research project, identifying the questions shared by scholars as well as their evolution, the articles' functions in the discourse, and the succession of disputes, discussions, and arguments held among the participants of this discourse (elements (ii) to (v)) turned to be key for constructing the intellectual history presented in Chapters II to V. Finally, understanding the scholars' salient perceptions, commitments, values, and attitudes (element (vi)) proved extremely helpful for tracking the transformation of techno-legal imaginaries discussed in Chapter VI.

## D. Research methods

As announced in the Introduction, this dissertation looks to answer the following two research questions: (1) How did "privacy's algorithmic turn" actually happen? And, (2) What can American privacy law scholars' aspirations, expectations, and visions about the future further tell us about this turn? For doing so, I conducted document analysis of 574 law review articles written between 1990 and 2020. In addition, as a triangulation point on background, I also drew on fifteen oral history interviews conducted with a purposely drawn representative sample of privacy law

[12] According to Hollinger, the life of the mind should be depicted as a *life*, rather than as a set of discrete units of thought or artifacts of intellect. In that sense, even if at this point of the methodology the historian of discourse should study ideas, she should do so by giving them the same relevance as events have in other historical accounts. According to Hollinger, "an idea contributed to a discourse is no less an 'event' (and no less trivial or momentous, in itself) than a bullet fired in a war or the invention of a machine" (Hollinger, 1985, p. 149).

scholars. The data collected was analyzed from a "Grounded Theory" perspective, for which I primarily followed the inductive coding approach known as "constant comparative method," while also incorporating an additional step of deductive coding.

## 1. Data gathering practices

### 1.1 Document analysis

For this dissertation, I conducted document analysis of 574 law review articles written between 1990 and 2020. Given the importance of the Privacy Law Scholars Conference (PLSC) for the field of privacy law in America, I used the scholarly work produced around this academic event as my primary source of data. Specifically, I drew this sample of articles from the following two sources: (i) papers workshopped at PLSC between 2008 and 2020 and which ended up being published, either as an article, a draft (e.g., on SSRN), or a book chapter (hereinafter referred to as "PLSC articles"), and (ii) law review articles published between 1990 and 2007 and cited in at least one of the aforementioned PLSC articles (hereinafter referred to as "pre-PLSC articles").

There were two reasons for including the latter set of articles (pre-PLSC articles) as part of this study's sample. In the first place, by covering only the period during which PLSC has existed (2008-2020), I would have failed to capture the progressive changes in privacy harms and proposed tools that compose privacy's algorithmic turn. Furthermore, covering these previous years also seeks to acknowledge that the field of privacy law scholarship in America did not begin with the formation of PLSC in 2008. In fact, several of the articles workshopped at PLSC were written by scholars who have been writing about privacy since the early 1990s (or even earlier, as in the case, for example, of Anita Allen, Paul Schwartz, and Pricilla Regan). As a result, by reviewing earlier

scholarship cited in the PLSC articles, I intended to recognize scholars whose work influenced and inspired subsequent research in the field.

To identify the first set of articles (PLSC articles), I built on previous work done by Law scholars Meg Leta Jones and Karen Levy, and Reference Librarian Ellen Kaufman, for a project titled *Methods to Our Madness: An Interdisciplinary Reflection on 10 Years of Privacy Scholarship*. Although this project was never finalized nor its findings published, the data collected for its purpose was compiled by these scholars in a spreadsheet that tracks and characterizes all the papers presented at PLSC from 2008 and up to 2017. For the three remaining years of the conference (2018-2020), I drew from the conference's previous agendas—which were all available online—to conduct my own compilation and characterization work in order to complete the database (hereinafter referred to as "the PLSC database built for this project"). As a result, I arrived at an initial number of 735 PLSC papers.

In turn, in order to identify the pre-PLSC articles I used the lists of references cited to in the PLSC articles. In order to recognize an adequate size of this sample, I aimed to reach a point of saturation (Saunders et al., 2017), where no additional articles were being identified and sources began to repeat. As a result, I arrived at an initial number of 1086 pre-PLSC articles.

I then filtered both sets of articles (PLSC and pre-PLSC) to exclude: (1) papers that had not been published or could not be accessed online;[13] and (2) articles that did not directly concern information privacy. For this second filter, I began by removing articles that, based on their titles, did not strictly relate to *privacy*, namely those focusing primarily on (i) the First Amendment, (ii) the Fourth Amendment, (iii) the risks to Intellectual Property posed by privacy, (iv) Internet jurisdiction, and (v) Cybersecurity. As a next step, I utilized Anita Allen's (2000) classification of

[13] Even when available, I also excluded drafts of papers which explicitly stated "do not cite."

the different meanings of privacy[14] to further exclude articles that were not about *information* privacy, but instead referred to decisional privacy, proprietary privacy (including the right of publicity), and physical privacy (including articles related to government surveillance and the Fourth Amendment).

As a result, I ended up with a final sample of 574 law review articles (**Table 1**), of which 283 (49.3%) were published before PLSC's foundation in 2008, while 291 (50.7%) correspond to PLSC articles. Notably, despite being discussed at PLSC sometime between 2008 and 2020, 38 articles (6.6%) from this second group were only published between 2021 and 2023. Having however been workshopped at PLSC during the established timeframe, they were still included as part of the sample.

| | **Year of publication** | **Number of articles** |
|---|---|---|
| **Pre-PLSC** | 1990-1999 | 101 |
| | 2000-2007 | 182 |
| **PLSC** | 2008-2013 | 89 |
| | 2014-2020 | 164 |
| | 2021-2023 | 38 |
| | **TOTAL** | **574** |

**Table 1. Annual distribution of articles analyzed for this research project**

### 1.2 Oral history interviews

Besides document analysis, this research also draws on fifteen oral history interviews conducted from November 2022 to November 2023 with a purposely drawn representative sample of

[14] According to Allen, "[t]he actual contemporary usage of 'privacy' in the United States is particularly broad. 'Privacy' can mean informational privacy, but also physical, informational (sic), and proprietary privacy" (2000, p. 866).

American privacy legal scholars whose works I had previously reviewed (hereinafter referred to as "interviewees,""narrators," or "participants"). Although not the primary research method for this dissertation, these oral history interviews were used as a triangulation point on background, (i) filling in details about the history of PLSC that I could not acquire elsewhere, and (ii) providing confirmation of elements of scholars' techno-legal imaginaries as identified through the document analysis.

As defined by Lynn Abrams, "oral history is the act of recording the speech of people with something interesting to say and then analyzing *their memories of the past*" (2016, p. 1). Thus, in contrast to other forms of data collection that use interviews, oral histories are based in memories and particularly interested in engaging with the past.

On the surface, these characteristics appear to be contrary to the two purposes for which I included oral history interviews as a triangulation point in my research. First, given the frailties associated with memory, relying solely on the accounts of interviewees could result in inaccurate or biased versions of the history of PLSC. In fact, in order to address this potential flaw, whenever possible I cross-checked the accounts of my narrators with those of other interviewees, as well as with documentary sources found online and on the website of PLSC.

Nevertheless, what drove me to select this method among others was the fact that oral histories "tell us not just what people did, but what they wanted to do, what they believed they were doing, and what they now think they did" (Portelli, 2015, p. 52). Hence, as will be seen in Chapter I, the excerpts from the transcripts of the oral history interviews there included provide insight into not only the history of PLSC and the community that developed *around* it, but also what its co-founders and recurring participants *expect* them to be (or to have been). Therefore, when addressing Chapter I, I want readers to be mindful about the fact that in these oral history

interviews "the past is remembered, reworked, and reconstructed by people in the present" (Abrams, 2016, p. 8), and in that sense, what we might see there is the combination of facts and the narrators' subjectivity.

Second, the fact that oral history researchers are particularly interested in engaging with the past also seems contrary to my objective of exploring American privacy law scholars' techno-legal imaginaries, which are by nature forecast-oriented. Yet, I chose the oral history method consciously, as a strategy to build the rapport and trust necessary for scholars to feel comfortable daydreaming and talking about the future. As Anna Sheftel and Stacey Zembrzycki explain, more than other forms of data collection that use interviews, oral history researchers "work to build trust and share authority so that we may truly collaborate with our interviewees and understand their experiences" (2010, p. 192).

As I was able to verify it myself across the different oral history exercises, as scholars progressed through the different phases of their scholarship, it turned natural for them to think about their desirable futures. Likewise, giving interviewees the opportunity to reflect on their journey as scholars and professors allowed each of them to reveal their "self," "the autonomous and self-contained individual who possesses a rich and complex inner life or consciousness" (Abrams, 2016, p. 33). The fact that during their oral history interviews two of the participants joked about feeling in therapy or receiving free counseling (Karen Levy, oral history interview, November 17, 2023; Paul Ohm, oral history interview, September 22, 2023) talks about the candid, vulnerable, and even cathartic character of many of their answers, which—as will be seen in Chapter VI—could be considered by many as brutally honest.

In total, I contacted a pool of 20 possible interviewees, following up a week later in case of missing in action. For drawing the sample, I took into account (i) the scholar's role in the

"algorithmic turn," as I was starting to identify it in the reviewed documents;[15] (ii) my initial understanding of their role[16] within the PLSC community or privacy scholarship at large; and (iii) the names of scholars suggested by interviewees themselves. In addition, in my initial pool I aimed as much as possible to have equal representation between genders. I finally conducted oral history interviews with 15 scholars (**Table 2**), while 5 excused themselves or did not respond to my emails.

| Scholar |
|---|
| Priscilla Regan |
| Anita Allen |
| Paul Schwartz |
| Julie Cohen |
| Michael Froomkin |
| Pauline Kim |
| Daniel Solove |
| Chris Hoofnagle |
| Neil Richards |
| Paul Ohm |
| Tal Zarsky |
| Woodrow Hartzog |
| Ari Waldman |
| Karen Levy |
| Andrew Selbst |

**Table 2. Interviewed scholars**

Each participant signed an informed consent prior to the interview (**Appendix A**), which explained the purpose of the oral history exercise, what would happen to the information provided by them, and who they could reach out to for more information about this research project. The

[15] My assumptions about their role in "privacy's algorithmic turn" may have changed over time. In addition, as the research project advanced, I decided to focus on the trends that I was seeing in the "community of discourse" rather than in the scholarship of specific authors.

[16] Based on my own experience attending PLSC for the last three years (2020-2023), the data provided on the conference's official website, and the information provided to me by other interviewees.

oral history interviews were conducted (and recorded) over Zoom or Microsoft Teams, based on an initial interview guide (**Appendix B**), which was shared with interviewees in advance. It is important to note, however, that as my different hypotheses started to emerge from the data and develop into theories (see Section 2 of this Chapter—Qualitative analytic approach), the list of topics addressed, as well as the questions posed evolved over time. Likewise, the specifics of each interview were adapted based on a preparatory review of each interviewee's professional website and published work.

Every oral history interview was transcribed with the help of Zoom and Microsoft Teams's transcription tools. After a first draft of each transcript was completed, I sent the transcript to each interviewee, thanking them again for their participation and inviting them to review the document and make sure I had got their meaning down accurately. In addition, this offered the narrators the possibility to consider whether they were still comfortable with the oral histories they had co-created, and whether there was additional information they wished to add. I encouraged them, however, not to try to formalize their speech or make it like a written biography, so that the transcript could retain the conversational quality of the spoken interview.

As announced in the informed consent document (**Appendix A**), I had initially planned for the final transcript of each complete oral history, along with some video clips from the interviews (if applicable), to be deposited in The Internet Archive (archive.org), a non-profit digital library of cultural artifacts in digital form. In this way, researchers, historians, scholars, people with print disabilities, and the general public would be able to freely access them online. Nonetheless, given that during the conduct of the interviews the Large Language Models' ("LLMs") hype exploded in society, one of the participants' off-the-record observation about the risk that these transcripts may be scraped and fed into ChatGPT or other LLMs' training data prompted me to reconsider my

original decision. As of the completion of this dissertation, the decision to deposit the oral histories in The Internet Archive has been suspended, while I explore other archival options that provide password-protected access to the material.

Aside for some exceptions,[17] so much historical information about PLSC and the community that has developed *around* it exists only in the conference co-founders' and participants' memories and not in the written record. Therefore, regardless of where these oral histories end up being deposited, I hope them to contribute to the institutional memory of the community whose scholarly work I study here.

## 2. Qualitative analytic approach

As it usually happens, both the identified research problem and the two research questions posed for this dissertation ended up dictating the qualitative analysis approach for this project. Given that my research problem and questions are focused on a *social process*—the transformation of a concept in the minds of American privacy law scholars over time, and that I wanted the end result of this research to be a set of hypotheses (*theories*) on (1) the evolution of the concept of information privacy, as well as on (2) one of its possible drivers, I opted for addressing the sample of articles as well as the oral history interviews' transcripts using "Grounded Theory" analysis (Glaser & Strauss, 1967).

Grounded Theory was proposed in 1967 by sociologists Barney Glaser and Anselm Strauss. In contrast to logico-deductive theory analysis, grounded theory analysis does not recur to external, pre-existing theories to make sense of the data collected. Instead, the theories used to

[17] As Paul Ohm would reference in his oral history interview, at PLSC's 10-year anniversary the conference Program Committee prepared bound book for PLSC co-founders Daniel Solove and Chris Jay Hoofnagle with "every single abstract ever written" during those first ten years. (P. Ohm, oral history interview, September 22, 2023)

explain and interpret the data are inductively developed from the data of social research. For this reason, grounded theory analysis is understood as "the discovery of theory from data" (Glasser & Strauss, 1967, p. 1). According to Glasser & Strauss,

> The interrelated jobs of theory in sociology are: (1) to enable prediction and *explanation of behavior*; (2) to be useful in theoretical advance in sociology; (3) to be usable in practical applications-prediction and *explanation should be able to give the practitioner understanding and some control of situations*; (4) to *provide a perspective on behavior*-a stance to be taken toward data; and (5) to guide and provide a style for research on particular areas of behavior. (1967, p. 3).

In the present case, the purpose of interrogating the sample of articles and the oral history interviews' transcripts through qualitative analysis is to provide a perspective on the transformation of the concept of information privacy in a portion of American privacy law scholarship, enable a possible explanation of that sociotechnical phenomenon, and even, give American privacy law scholars an understanding of the situation and some control over it. As I hope to evidence throughout this document, the data collected for this project allowed me to expand on the theory of privacy's algorithmic turn proposed in prior work (Angel, 2024), as well as suggest a theory of the transformation of scholars' techno-legal imaginaries as a possible driver of one of the features of that turn.

Based on Glasser & Strauss's original account of Grounded Theory (1967), three characteristics can be highlighted about the two theories expanded/proposed in this dissertation. First, instead of being logically deduced theories based on ungrounded assumptions and common sense, these two theories are intimately linked to the data here reviewed, and aim to help explain and interpret it. Second, these two theories do not aim to be perfect products, but rather are presented as "an ever-developing entity" (Glasser & Strauss, 1967, p. 32). In that sense, they are introduced here with the assumption that they will keep developing in the future. Finally, when

generating them, my job as a researcher has not been "to provide a perfect description of an area, but to develop a theory that accounts *for much of* the relevant behavior" (Glasser & Strauss, 1967, p. 30), namely, the transformation of American privacy law scholars' conception of information privacy.

In order to discover theory, classical Grounded Theory relies on an inductive coding approach[18] that Glasser & Strauss coined as the "constant comparative method." According to these authors, constant comparison

> [i]s an inductive method of theory development. To make theoretical sense of so much diversity in his data, the analyst is forced to develop ideas on a level of generality higher in conceptual abstraction than the qualitative material being analyzed. He is forced to bring out underlying uniformities and diversities, and to use more abstract concepts to account for differences in the data. (Glasser & Strauss, 1967, p. 114).

As will be seen in Section 3, for this study I primarily followed the constant comparative method, while also incorporating an additional step of deductive coding.

## 3. Coding techniques

As announced, for this research project I primarily used inductive coding (constant comparative method) in conjunction with an additional deductive coding phase.

### 3.1. Constant comparative method

As described by Glasser & Strauss (1967) and many other scholars who have written about this method since then (Silverman & Paterson, 2014), the constant comparative method follows four stages/phases: open coding, focused coding, delimiting the theory, and writing theory.

[18] Qualitative coding "involves sorting data into categories for further analysis and theory building" (Silverman & Paterson, p. 29). In that sense, "[c]oding moves in a stepwise fashion progressively from unsorted data to the development of more refined categories, themes, and concepts" (Hahn, 2008, p. 5).

### 3.1.1. Open coding

"During open coding," Robert Mark Silverman & Kelly Paterson explain, "each line of data is read and *codes* are assigned to all relevant segments" (2014, p. 29).

Thus, with the aid of the computer-assisted qualitative data analysis software (CAQDAS) Atlas.ti, I began the analysis of the data collected by reading through the data meticulously and identifying multiple emerging open codes. Mostly descriptive, these codes were based on: (i) *in vivo* codes (taken from the specific excerpts) (e.g., FIPs; discrimination; fiduciary duties); (ii) my own derived terms (e.g., FTC work; actions taken in the European Union); and (iii) conceptual phrases derived from privacy literature I was familiar with in advance (e.g., "the privacy paradox;" "law of the horse"). While doing this, I used Atlas.i memos to record my ideas and observations about the possible interactions and relationships that I was seeing between the emerging codes.

### 3.1.2. Focused coding

As a second phase, focused coding "involves the synthesis of codes identified during the open coding process. The goal of focused coding is to take discrete codes from the open coding process and organize them into overarching *categories* that can be used in subsequent analysis" (Silverman & Paterson, 2014, p. 29).

For this phase, I started comparing the open codes mentioned above to find similarities and differences. Based on these comparisons, I used Atlas.ti's code groups and merging codes tools to cluster the codes into a narrower set of broader categories. To the extent possible, I attempted to make these categories as representative and comprehensive as possible, selecting terms that were now conceptual, rather than descriptive. For example, I realized that codes such as "threat to

autonomy" or "discrimination" could be clustered under the category of "harms." Similarly, I concluded that for the purpose of coding, codes such as "co-regulation" and "collaborative governance" could be merged into one code, which could in turn be included under the category of "proposed tools." As a result, this second round of coding yielded 22 broad categories of codes (**Appendix C**).

### 3.1.3. Delimiting theory

Instead of another coding phase, this stage entails the conceptual exploration of relationships among the previously identified categories. In order to start delimiting a theory (or theories), the researcher can, for example, "create diagrams that visually represent relationships identified in a study. Diagrams assist researchers in identifying relationships between conceptual categories identified with focused coding" (Silverman & Paterson, 2014, p. 38).

In the case of this study, the creation of diagrams was a constant, iterative process, that helped me put in paper the relationships I was starting to see among some of the codes. Besides, during this phase I further divided the proposed categories into the following three themes, depending on whether they would help me to answer each of my two research questions or to characterize PLSC as a "community of discourse": Intellectual History ("IH") (for categories used to answer research question (1)), Techno-legal Imaginaries ("TI") (for categories used to answer research question (2)), and Privacy Law Scholars Conference ("PLSC") (for categories used to characterize PLSC as a "community of discourse").

### 3.1.4. Writing theory

During this fourth phase the researcher is expected to use the coded data, the series of memos, and the created diagrams to write the theory (or theories) that has discovered from the data. As explained by Glasser and Strauss, in a constant comparative method the identified categories "become the major themes [(section titles)] of the theory later presented in papers or books" (1967, p. 113). Similarly, the "[d]iagrams (…) can also provide researchers with a roadmap for developing a narrative describing the results from a qualitative study" (Silverman & Paterson, 2014, p. 38).

In this case, if the structure of each chapter described in the Roadmap section of this Introduction is compared to the codebook of categories of this study (**Appendix C**), the reader will indeed notice how the structure of all the chapters that follow was indeed largely shaped by several of the identified categories.

In that sense, this four-phases ground-up process not only lent structure to my understanding of the different trends present in the data and therefore, in the scholarship under review. Furthermore, it also allowed me to "delimit" and finally "write" (Glasser & Strauss, 1967) the two theories that I either expand on (privacy's algorithmic turn – see Chapters II to V) or propose (the transformation of scholars' techno-legal imaginaries as a possible driver of the shift in scholars' proposed legal tools to protect information privacy – see Chapters VI) in this dissertation.

## 3.2. Additional deductive coding step

While the previous two coding phases (open and focal coding) were conducted using inductive coding (Naeem & Ozuem, 2022), the final step of my coding process—and which was not part of the constant comparative method—was rather deductive.

My goal for this final phase was to further analyze the data by using the lens of Intellectual History. Having an established set of categories that had resulted from the application of the constant comparative method, I proceeded to code the ATLAS.ti reports generated for each "IH-" and "TI-" category (12 in total), based on the five elements[19] that, according to my interpretation of David Hollinger's work, a historian should consider when conducting a study of the discourse of intellectuals: shared questions, evolution of questions, article's role, conflicts/disputes/discussions, and salient perceptions/commitments/values/attitudes. As a result of this top-down approach, I was able to identify key elements—typical of a study of the discourse of intellectuals —that, although not influential on the structure of Chapters II to V, should be highlighted whenever appropriate throughout the intellectual history there discussed.

Overall, the whole three coding phases (open, focused, and deductive) followed during the analysis yielded hundreds of relevant excerpts, which are cited (sometimes at length) throughout this dissertation in order to support the proposed theories, claims, and findings.

***

Before concluding, three important caveats should be noted with regards to the structure followed in Chapters II to V (corresponding to the intellectual history). Firstly, it is important to note that in these chapters the content of Section A ("Context") is presented through the lens of the privacy law scholars here reviewed. In other words, in all of these chapters, Section A describes the technologies/practices, societal attitudes, and legal systems of the covered epoch *as viewed by these authors*. Consequently, although the accounts there registered may sometimes be inaccurate or incomplete, or the scholars believed things would occur but have not, my role in collecting and synthesizing their views has not been to correct or judge them.

[19] Excluding the "the boundaries of the 'community of discourse'" element, which had been previously identified through the category "community."

As a second point, the structure of those four chapters (II to V) intends to generate comparison among them. By using uniform rubrics under which data and discussion are grouped, the outline followed in Chapters II to V looks to enable the reader to trace how the properties of each of the proposed categories (e.g., societal attitudes; identified harms) have changed throughout the four covered time periods (1990-1999; 2000-2007; 2008-2014; 2015-2020). For making these comparisons more evident, however, I have been intentional about including explicit cross-references and comparative insights within the four chapters.

Finally, it is also worth noting that the structure followed in Chapters II to V has a purely analytical function. By breaking down the scholars' written accounts into different categories or constituent domains, this structure brings order to the discourse advanced by the intellectual community here studied. This compartmentalization, however, should not be interpreted as a denial of the sociotechnical character of the phenomenon under study. Specifically, it does not attempt to negate the dynamic and complex relationships that exist between these different technical (technologies/practices), social (societal attitudes), and legal (legal systems) domains, or the multiple ways in which these domains co-produce the scholars' conceptions of information privacy. In fact, by separating them, I hope to make more evident their different interactions and entanglements.

Additionally, I would also like to clarify the purpose for which I use some means of emphasis in these four chapters and throughout the document. Unless otherwise stated in the text, the italics used in excerpts from articles and oral history interviews should be understood as mine, added to emphasize the importance of certain words or sentences for the point being made in the narrated intellectual history. Bold, in turn, is used in this dissertation to emphasize open codes that despite not getting to be mentioned as sub-headings, still deserve the readers' attention.

## E. Theoretical framework

In his 2011 article titled *The Drone as Privacy Catalyst*, Ryan Calo wrote: "One might reasonably wonder whether we will ever have another Warren and Brandeis moment, *whether any technology will dramatize the need to rethink the very nature of privacy law*" (2011, p. 30). Even though Calo was referring to the drone, as I developed this research project, I began to believe that algorithms—those complex sets of rules supporting many of the sociotechnical systems that emerged between 1990 and 2020—might be that catalyzing technology. At first glance, it seemed reasonable to think that the transition from personal computers and the Internet to algorithmic decision-making systems and AI had animated the transformation of the concept of information privacy that I was beginning to see in American privacy law scholarship.

I rapidly realized, however, that adopting this hypothesis would lead me into the path of technological exceptionalism. This perspective attributes tech law & policy change to "something about a technology or its use that is 'exceptional'" (Crootof & Ard, 2021, p. 348). In that sense, it follows a linear relationship in which "a new technology is presented to society and the law must move quickly to respond to the disorder technology creates" (Jones, 2018, p. 102-103).

Over the years, a number of legal scholars have begun to criticize this approach to law and technological change.[20] In 2015, for instance, Jack Balkin wrote against technological exceptionalism in the following terms:

> I do not think it is helpful to speak in terms of "essential qualities" of a new technology that we can then apply to law. On the contrary, *we should try not to think about characteristics of technology as if these features were independent of how people use technology in their lives and in their social relations with others*. Because the use of technology in social life evolves, and because people continually find new ways to employ technology for good or for ill, it may be unhelpful to freeze certain features of use at a particular moment and label them "essential." (2015, p. 45)

[20] Another example comes from Rebecca Crootof & BJ Ard, who have also pointed out how "the exceptionalist approach fosters siloed and potentially incomplete analyses, masks the repetitive nature of the underlying questions, and thereby results in the regular reinvention of the regulatory wheel" (2021, p. 349).

Thus, Balkin argues that, rather than focusing on technologies' "essential" characteristics, when thinking about "technology and law's encounter with innovation" (2015, p. 46), one should have in mind the multiple ways in which (i) technology uses and (ii) the social relations that employ those technologies affect how people (including lawyers) come to think about them.

A similar critical approach to technological exceptionalism can be found in Margot Kaminski's scholarship. In Kaminski's view,

> In reality, the picture is far more complex. *The law can itself drive technological development*; (…). To the extent new technology (or really, the social practice of a new technology) disrupts the law, it does so because of how it encounters existing features of the law, both doctrinal and theoretical. *The law, in constructing—that is, building the meaning of—new technological developments and their social uses, takes a central part in its own disruption*. Conceiving of technology as some outside force that acts upon the law can lead to a technology-centric approach in which one tries to identify what features of a particular technology are legally disruptive. *This kind of disruption narrative gets it wrong. A particular feature of a particular technology disrupts the law only because the law has been structured—doctrinally and theoretically—in a way that makes that feature relevant. The disruptive effects (if any) of a technology become manifest when they encounter, interface with, and are given particular meaning within the law*. (2017, p. 590-591).

In that sense, Kaminski argues that technology should not be considered the driving force of law. Rather, she emphasizes "the importance of legal context in the disruption story—and the relative unimportance of particular features of the technology itself" (2017, p. 590-591).

Joining Balkin and Kaminski, in a 2018 article Meg Leta Jones also invited cyberlaw scholars to consider "the way in which technologies, practices, and social arrangements are constructed within certain legal contexts" (2018, p. 105). For her, "[w]hether a technological advancement matters, whether it is novel or innovative, depends heavily on a cultural landscape. Technological exceptionalism disregards this aspect of innovation and assumes newness based on technological essentialism" (2018, p. 133).

Thus, looking to change the approach, Jones formally linked the field of Law & Technology with STS, and particularly, with the STS perspective often referred to as the Social Construction of Technology ("SCOT"),[21] to propose a method coined by her as the "Legal Construction of Technology" ("LCT") or "techno-legal construction." According to her, "[t]he legal construction of technology focuses on law as a cultural corner of societies with its own customs and rituals, players and roles, institutions and relationships, and rules and power—and how this cultural corner makes sense of a technology, technological system, or technological concept" (2018, p. 133).

More recently, Kaminski & Jones (2024) joined forces to expound upon the Legal Construction of Technology method and apply it to the case of AI speech.[22]According to these scholars, "[t]he method examines *how the law makes sense of technology*, querying the *objects*, *values,* and *institutions* involved in such sensemaking" (2024, p.1215). Expanding on the latter, they would further contend: "Law makes sense of, and indeed shapes, technology and its trajectories through legal tools and *institutions*. These tools and institutions are designed to advance particular *values*, and are aimed at particular *people, behavior, or things* (2024, p.1217). Interestingly, with this added emphasis on values, institutions, and objects, in this article Kaminski

[21] Initially proposed by Trevor J. Pinch & Wiebe E. Bijker (1984), SCOT is a theoretical and methodological endeavor which attempts to describe the construction of technical artefacts through the eyes of "relevant social groups." According to Pinch & Bijker (1984), the interactions among the members of a social group and between these groups, which are structured by a given "technological frame," can give different meanings to the same artefact, commonly referred to as "interpretive flexibility." In turn—they say, this interpretative flexibility evidences that the "stabilization" of an artefact, "is a social process, and hence subject to choices, interests, and value judgments-in short, to politics" (Bijker, 1997, p. 281).

[22] In 2022, Kaminski had already returned to the topic, supporting the idea of the "legal construction of technology" by once again arguing that "the law dynamically *constructs* technology into its own systems of meaning—just as it constructs many other things" (2022, p. 893). Nevertheless, in this piece she would also recognize that "sociotechnical changes can afford new opportunities for contestation over legal rules and principles" (2022, p. 895), being that a case in which technology does disrupt the law.

& Jones extended Jones's initial proposed link between Law & Technology and SCOT, to the co-production perspective[23] also nested in STS (2024, p. 1217, footnote 11).

As Sheila Jasanoff—author of the STS concept of co-production—has herself explained when criticizing SCOT, the problem with sticking to the Social Constructivist approach is that "the discourse of social construction tends to inhibit *the symmetrical probing of the constitutive elements of both society and science* that forms the essence of the S&TS research agenda" (2004b, p. 19-20). In contrast, Jasanoff argues, "[t]he term co-production reflects this self-conscious desire to avoid both social and technoscientific determinism in S&TS accounts of the world" (2004b, p. 20). Thus, by extending the link to co-production, Kaminski & Jones comfortably contend in this article that "[l]aw and technology are each aspects of, and deeply embedded in, society. As such, they co-construct each other, in the context of deeply political systems that channel or constrain political power" (Kaminski & Jones, 2024, p.1216).[24]

[23] Sheila Jasanoff proposed the idiom of "co-production" to describe what previous STS authors and social scientists had already been recognizing in their research, with greater and lesser self-consciousness. According to Jasanoff,

> "co-production is shorthand for the proposition that the ways in which we know and represent the world (both nature and society) are inseparable from the ways in which we choose to live in it. Knowledge and its material embodiments are at once products of social work and constitutive of forms of social life; society cannot function without knowledge any more than knowledge can exist without appropriate social supports. *Scientific knowledge, in particular, is not a transcendent mirror of reality. It both embeds and is embedded in social practices, identities, norms, conventions, discourses, instruments and institutions – in short, in all the building blocks of what we term the social. The same can be said even more forcefully of technology*." (2004a, pp. 2-3).

In that sense, the aim of co-production, as a theoretical tool, "is to make available resources for thinking systematically about the processes of sense-making through which human beings come to grips with worlds in which science and technology have become permanent fixtures" (Jasanoff, 2004b, p. 38).

[24] To be clear, at various points throughout her original 2018 article Jones had already emphasized the idea that, a variety of factors—apart from technology—influence "the interpretations American law has made in theory, doctrine, analogical reasoning, or overarching policies" (2018, p. 107). According to Jones, "technology does not drive history and it does not drive law. *It is only part of the story*. New technologies have become a part in social settings made of existing *technologies, uses and users, norms* and *aspirations*" (2018, p. 115). When it came to the concrete conceptualization of the "Legal Construction of Technology," however, its initial theoretical roots—SCOT, its name itself, and its prior description seemed to limit its original scope. This, by prioritizing the one-way arrow of influence of law over technology, namely, the idea that technology is socially constructed by law, and therefore, that technological novelty depends on the legal context where it is being evaluated.

In this dissertation I intend to build upon Kaminski & Jones's new conceptualization of the Legal Construction of Technology method (now nested in co-production), in which both technology and law are socially constructed and co-produce each other. In particular, this study uses the STS concept of "imaginaries," as an instrument of co-production, to account for the cognitive elements—the scholars' visions of desirable future that could be achieved through the regulation of technology—that might be intervening the already dialectical and multidirectional relationship that exists between the American privacy law scholars' conceptions of information privacy and the sociotechnical changes occurred during the years reviewed.

For doing so, I use different elements from the STS literature on "imaginaries," and from interdisciplinary scholarship that applies this theoretical concept to the law, to propose the concept of "techno-legal imaginaries." By placing privacy's algorithmic turn within a broader context where technological, social, legal, and—as I hope to demonstrate here—cognitive elements interact and become entangled, the concept of "techno-legal imaginaries" serves as an analytical construct to detach the studied turn from the algorithmic technologies and understand it instead as a complex sociotechnical phenomenon.

According to Kaminski & Jones,

> *The law* plays as much of a role as technology does: it *embeds values*, crafts institutions, and even sets up its own fault lines that later may crack. *This method emphasizes that the law is worthy of deeper scrutiny*; its *values and theories*, objects of regulation, and institutions all contribute to how technology is brought into contact with, and made meaningful within, the law. (2024, p.1217).

Against this framework, it is also my hope that the concept of "techno-legal imaginaries" can more generally serve as a tool within the Legal Construction of Technology method, to scrutinize and bring to light the *values and normative commitments embedded* in the regulatory proposals of legal actors engaged in technology regulation.

This Section proceeds as follows. My first step will be to examine in detail the STS literature on "imaginaries." Although I am particularly interested in exploring the concept of techno-legal imaginaries proposed by Sheila Jasanoff & Sang-Hyun Kim (2009), as well as the concepts of expectations, promises, and visions suggested by the sociology of expectations, I precede this Section with a brief review of their theoretical precursors: prior social and political theories that have proposed different forms of collective imagination. In Section 2, in turn, I will examine some examples of how the concept of imaginaries has been applied by interdisciplinary scholars to legal endeavors. Finally, I will introduce the concept of "techno-legal imaginaries," as a novel and distinct theoretical construct that takes elements from the terms and uses mentioned above.

## 1. STS literature on imaginaries

During the last few decades, the concept of "imaginaries" has been widely adopted in the STS field, developing into innumerable variants (McNeil et al., 2016). Generally understood as "patterns of thought that have an influence on wider social processes" (McNeil et al., 2016, p. 438), imaginaries are assumed to contain the "aspirational and normative dimensions of social order" (Jasanoff, 2015a, p. 5) that the members of a given community operate on.

Like the STS concept of "imagined affordances," which "bring[s] back into the scholarly conversation the importance of imagination, non-rational thought, and perception for describing the process of the formation of technological affordances" (Nagy & Neff, 2015, p. 7), the theoretical concept of "imaginaries" likewise contributes to opening STS to "the study of social and psychological investments and future visions linked to specific technoscientific developments" (McNeil et al., 2016, 457). Additionally, it allows science and technology to be

associated not only with facts and artifacts, but also with storytelling, imaging, and imagining (McNeil et al., 2016). In that sense, studying "imaginaries" offers "new ways to investigate the relationships among science, technology, and society" (McNeil et al., 2016, 435).

For the purpose of this research, I am particularly interested in exploring the variants of the concept of "imaginaries" proposed by the literature of "sociotechnical imaginaries" and the "sociology of expectations." However, it seems important to recognize that the pedigree of the concept of imaginaries stretches back to prior social, political, and cultural theorists' efforts to theorize the collective imagination. Therefore, before digging into the aforementioned bodies of literature, I will explore briefly their theoretical precursors.

### 1.1 Theoretical precursors: Social, political, and cultural theories on collective imagination

As said, although nowadays widely used as an STS analytical tool, the pedigree of the concept of "imaginaries" stretches back to earlier efforts from social, political, and cultural theorists to make sense of the collective imagination. Here I present some of them as examples of these prior endeavors.

In 1983, for instance, Benedict Anderson proposed the idea of an **"imagined political community."** In particular, Anderson defines the nation as "an imagined political community" (Anderson, 1983, p. 6), describing it as a *construct of minds that come together through shared practices of narrating, recollecting, and forgetting*. In that way, he says, nationality turns out to be a cultural artefact that commands profound legitimacy.

Another example can be drawn from the work of George Marcus (1995) and his colleagues. Writing in 1995, these authors would develop the concept of **"technoscientific imaginaries**." In

their book *Technoscientific Imaginaries: Conversations, Profiles, and Memoirs,* they use this concept to describe the predicaments of scientists about the future possibilities that could be achieved through technoscientific innovation. In the Introduction of the book, those imaginaries are described by Marcus as "structures of contingency," used by scientists "to understand the present by borrowing from a cautiously imagined emergent future [(constrained by the very present conditions of their scientific work)], filled with volatility, and uncertainty, but in which faith in practices of technoscience became even more complexly and interestingly constructed in new locations of doing science" (Marcus, 1995, p. 4). Importantly, the imaginaries that Marcus and his colleagues refer to are exclusively *related* to the *future possibilities* of the various kinds of science that scientists portraited in the book do. In that sense, they correspond to scientists caught in social changes of government or of industry, "who no longer are doing science as usual" (Marcus, 1995, p. 3).

Twenty years ago, Charles Taylor (2004) offered the concept of **"social imaginary,"** which can be defined as "the ways in which people imagine their social existence, how they fit together with others, how things go on between them and their fellows, the expectations that are normally met, and *the deeper normative notions and images that underlie these expectations*" (Taylor, 2002, p. 106). They are shared by large groups of people, make possible common practices, and offer a widely shared sense of legitimacy about how lives should be ordered. According to Taylor, these social imaginaries are determined by a given moral order, which not only "tells us something about how we ought to live together in society" (Taylor, 2004, p. 3), but also "stresses the rights and obligations we have as individuals in regard to each other, even prior to or outside of the political bond" (Taylor, 2004, p. 4). As a result, social imaginaries are composed of a common understanding, which is both factual and normative. In that sense, "we

have a sense of how things usually go, but this is interwoven with an idea of how they ought to go, of what missteps would invalidate the practice" (Taylor, 2002, p. 106).

Finally, in 2012 Yaron Ezrahi coined the term **"imagined democracies,"** to refer to political realities which are "actually created by the largely unconscious public's own recursive performative political imagination" (Ezrahi, 2012, p. 2). In that sense, Ezhari argues that democracy depends on rituals, verbal and figurative representations, and nonmaterial elements performed by numerous individuals and groups in order to exist. In other words, widely believed "political imaginaries," composed of metaphoric and both cognitive and emotional elements, are necessary to perform and sustain democracy. According to Ezrahi, "[p]olitical imaginaries, for our purpose, refers to fictions, metaphors, ideas, images, or conceptions that *acquire the power to regulate and shape political behavior and institutions in a particular society*" (Ezrahi, 2012, p. 3). As a result, they not only generate performative scripts that orient behavior and pattern institutions, but also produce behavior that, in turn, affirms them.

Except for Marcus's concept of "technoscientific imaginaries," none of these theoretical efforts explicitly links the concept of "imaginaries" to technology-related contexts. Even so, it is still pertinent to discuss them here, since they allow me to flag several key aspects of the concept. In particular, a review of the theoretical precursors described above sheds light on (i) the nature of "imaginaries" as the *constructs of mind*, which come together through *shared narratives* (more evident in Anderson's concept); (ii) their usual relation with *the future* and with *future possibilities* (more evident in Marcus's concept); (iii) the ways they are usually underlain by deeper *normative notions and commitments* (more evident in Taylor's concept); and (iv) their *performative character*, that is, the way they are brought into being and have an influence on wider social processes (more evident in Ezrahi's concept).

As will be seen in Sub-section 1.4, however, element (ii)—usual relation with the future—has not always been the case when the concept has been applied by legal scholars as an analytical tool to interpret legal endeavors.

### 1.2 Sociotechnical imaginaries

Initially proposed by Sheila Jasanoff & Sang-Hyun Kim (2009) for nation-specific scientific and/or technological projects,[25] but later developed by Jasanoff (2015a) with a more general scope, sociotechnical imaginaries are "collectively held, institutionally stabilized, and publicly performed visions of desirable futures, animated by shared understandings of forms of social life and social order attainable through, and supportive of, advances in science and technology" (Jasanoff, 2015a, p. 4). Jasanoff has further described them as "a continually rearticulated awareness of order in social life (…) and a resulting commitment to that order's coherence and continuity" (Jasanoff, 2015a, p. 26). Unlike their original formulation (Jasanoff & Kim, 2009), sociotechnical imaginaries are not exclusively limited to nation-states or top-down initiatives, and can also be collectively articulated and advanced from a bottom-up perspective by different types of organized groups, including professional societies.

Jasanoff adds that "these imaginaries are at once products of and instruments of the coproduction of science, technology, and society in modernity" (Jasanoff, 2015a, p. 19), and that they are both temporally situated and culturally particular. Also, despite being grounded on positive visions of social progress, sociotechnical imaginaries inevitably correlate with shared fears of harms that might arise from technology or from the failure to innovate.

[25] "We define national sociotechnical imaginaries as 'collectively imagined forms of social life and social order reflected in the design and fulfillment of nation-specific scientific and/or technological projects.' Imaginaries, in this sense, at once describe attainable futures and prescribe futures that states believe ought to be attained." (Jasanoff & Kim, 2009, p. 120)

Jasanoff identifies the following four phases in the construction of sociotechnical imaginaries: origins, embedding, resistance, and extension.[26] Throughout this process, sociotechnical imaginaries originate either in the minds of single individuals or among like-minded activists, professionals, or policy-makers; are encoded into cultures, institutions, and material technologies; and can even "gain traction, acquire strength, and cross scales, for example, by persisting through time or by overcoming geopolitical boundaries" (Jasanoff, 2015b, p. 323). As a result, during those phases, the sociotechnical imaginaries can either "get built into the hard edifices of matter and praxis" (Jasanoff, 2015b, p. 323) or be confronted with resistant imaginaries that can end up disabling thoroughgoing social transformations.

Besides building on various of the social, political, and cultural theoretical efforts mentioned above, in order to construct their own concept Jasanoff & Kim also drew upon the STS works that examine the nature of the "sociotechnical." Within this category, in Chapter 1 of *Dreamscapes of Modernity* Jasanoff (2015a) highlights the Actor-Network Theory (ANT) as a systematic mode of inquiry into the connections between technology and society. Proposed by Bruno Latour (1984, 1987, 1992, 1996, 1999, 1999b, 2004, 2005, 2009, 2010), Michel Callon (1980, 1986, 1990) and John Law (1992, 1994, 2006, 2009), this theoretical and methodological approach extends the word actor—or actant[27]—to non-human entities, and understands that "the social" also incorporates the natural and the material. Based on these theoretical assumptions, ANT traces associations ("networks") between human and non-human agents, seeking to make visible

[26] Interestingly, these 4 phases slightly resemble the four components of the social construction of technology (SCOT) proposed by Trevor J. Pinch & Wiebe E. Bijker (1984), namely: relevant social groups, interpretive flexibility, closure, and stabilization.

[27] According to Latour (2009), "[s]ince the word 'agent' in the case of nonhumans is uncommon, a better term, as we have seen, is actant" (p. 15).

the resulting joint production of actors and artifacts, which is usually opaque due to a process of "blackboxing" (Latour, 2009, p. 17).

Despite the analytical virtues of this approach for making evident the "sociotechnical" connections, Jasanoff does not agree with ANT's treatment of power and normativity. In particular, she considers ANT too promiscuous in attributing power to every single possible actor, risking both falling into a kind of moral nihilism and establishing a troubling normative equivalence between nonhuman and human agents. According to Jasanoff, although it is true that "imagination's skilled implementation requires putting in play the intricate networks whose construction has been the stuff of so much STS analysis" (Jasanoff, 2015a, p. 17), it should also be acknowledged that imagination, as a crucial reservoir of power and action, is exclusive for human agents and institutions.

Thus, by proposing the concept of "sociotechnical imaginaries," Jasanoff & Kim expect to "(…) occupy the blank space between two important literatures, the construction of imaginaries in political and cultural theory and of sociotechnical systems in STS (e.g., Bijker, 1997; Bijker et al., 1987)" (Jasanoff, 2015a, p. 5). In that way, while still focusing the STS researchers' attention on "the centrality of science and technology in the making and stabilization of collectives" (Jasanoff, 2015a, p. 5), the proposed theoretical concept particularly stimulates their interest in the ways in which the *collective beliefs about science and technology* contribute to that process of making and stabilization.

As a result, and unlike the prior approaches it builds on, the concept of sociotechnical imaginaries offers the possibility of explaining discrepant responses to new and emerging technologies. Also, it allows us to understand both durability and change in people's expectations of how things are and how they should be when it comes to science and technology. In third place,

"by allowing for competition among different visions of futures, the framework of sociotechnical imaginaries restores some of the indeterminacy of history and avoids the determinism built into grand narratives of scientific progress" (Jasanoff, 2015a, p. 23). And finally, by keeping its focus on human actors as well as on their collectively enacted hopes and expectations, it allows researchers to refocus their attention on human actors as their main object of study.

As will be seen in Sub-Section 1.4, this latter advantage provided by "sociotechnical imaginaries"—the ability to redirect the STS researcher's attention from the artifacts back to human actors—is particularly desirable for legal scholars who view law and technological change through the technological exceptionalism approach referred above.

### 1.3 The sociology of expectations

As a sub-field in both STS and sociology, the sociology of expectations study future expectations, promises, and visions related to technology and innovation. According to Kornelia Konrad & Knud Böhle, it can be defined as "a field that is concerned with the *performative role of expectations in science and technology*, and the question *how such expectations are shaped and dynamically evolve over time*" (2019, p. 103). Thus, although not always employing the concept of "imaginaries" but using instead other terms such as "visions" or "expectations," the scholars that make part of this sub-field are equally interested in the relationship between patterns of thought about the future and technology.

As seen in Konrad & Böhle's definition, for the sociology of expectations one of the most important characteristics of these future-oriented visions is the "performative character" mentioned earlier (see Sub-section 1.1). As Lukas Schlogl, Elias Weiss, and Barbara Prainsack aptly explain, visions and promises are never purely descriptive. "As the growing body of the

sociology of expectations shows (Brown et al., 2016), visions of the future create realities in that *they affect the availability of funding, shape policy agendas or public perceptions*" (2021, 309). Similarly, Konrad and and others of her co-authors point out:

> A key concern of STS treatments of expectations, visions, and imaginaries has been to investigate the performativity of future representations. These studies show how future-oriented discourses, practices, and materialities *shape the way society makes sense of science and technology, adjust how actors create strategies, and contribute to the shaping of technologies, as well as the development of entire technology fields*. (Konrad et al., 2016, 468)

In fact, it is precisely this performative character of future expectations which has led some scholars to often refer to them as practices of *imagineering* (Suitner 2015), that is, the processes of simultaneously imagining and engineering reality.

In second place, the sociology of expectations considers that these future-oriented understandings can exist at a wide variety of levels in society. In the view of Mads Borup, Nik Brown, Kornelia Konrad & Harro Van Lente, "expectations are foundational in the coordination of *different actor communities and groups (horizontal co-ordination) and also mediate between different scales or levels of organization (micro, meso, and macro—vertical co-ordination)*" (2006, p. 286). In that sense, and unlike sociotechnical imaginaries, these visions of the future can exist "also at the *meso level* of sectors and innovation networks, and at the *micro-level* within engineering and research groups and in the work of the single scientist or engineer" (2006, p. 286).

Finally, in order to study these future-oriented visions, the field privileges the use of anticipatory practices, which can be defined as "the particular ways by which these expectations are produced and spread within and across the different arenas, such as scientific publications, roadmaps, or consultancy reports" (Alvial-Palavicino & Konrad, 2018, 193). According to some of the authors working in this space, though, it is key to take into account that "[t]hese practices

show different kinds of performativity" (Alvial-Palavicino & Konrad, 2018, 200). In any case, all of them include "narrative infrastructuring work" (Sepehr & Felt, 2023), which allows researchers to explore the narratives and the normative commitments of the communities in charge of crafting them.

## 2. Interdisciplinary literature that applies imaginaries to the law

Whether based on STS literature or not, an increasing number of scholars have applied the concept of "imaginaries" (or related approaches) to legal endeavors. This, in order to make evident how the law interacts and becomes entangled with cognitive factors. The body of literature that addresses the possible interactions between law and imagination includes work from legal scholars Jack Balkin & Reva B. Siegel (2006), legal scholar Kieran Tranter (2011), STS scholars Kjetil Rommetveit & Niels van Dijk (2022), philosopher Daniel Susser (2022), and legal scholar Margot Kaminski (2022), among others.[28]

The work of these authors can be roughly divided into two. The first group is composed by scholars who employ the concept of "imaginaries" (or related expressions) to talk about imagined scenarios that underpin or are behind a regulatory approach or intervention (which may or may not be related to technology). Thus, those scenarios are either a set of problems/cases that need legal intervention, or a set of assumptions about reality (the legal reasoning behind an intervention).

Balkin & Siegel (2006) can be cited as an example of this first group. As early as 2006, these authors proposed the concept of **"imagined regulatory scene."** They use this term to describe "a set of background understandings about the paradigmatic cases, practices, and areas of social life to which [legal principles] (…) properly apply" (2006, p. 928). In that sense, they

[28] Ryan Calo, for example, studies how robots play an interesting role as the subjects of judicial imagination (Calo, 2016).

suggest that, when proposing a given legal principle, legal actors imagine a "paradigmatic set of problems" (p. 931) that have to be regulated by the law. According to these legal scholars, "a legal principle is given coherence by its regulatory scene," which also "offers a sense of security about how that principle should operate in practice" (p. 931).

Sixteen years later, Margot Kaminski (2022) built on Balkin & Siegel's concept to explore, in turn, how the social use of technology can change or disrupt the law's imagined regulatory scene. "[E]ach law or policy conversation takes place around *an understood imagined setting*, with technology, or the lack thereof, often playing a central role," Kaminski would argue. "When the social adoption of technology alters the forces in one of these imagined scenes, it can upset the policy balance and undermine the goals of a particular regulation or regime" (2022, p. 886).

Relatedly, Rommetveit & van Dijk (2022) have recently talked about **the "techno-regulatory imaginary"** of privacy by design that drives the actions of the policymakers behind the European Union's General Data Protection Regulation ("GDPR"). In the view of these authors, this "techno-regulatory imaginary" "prescribes that for data processing to be legitimate, it must include protections of rights and values as designed and in-built: in technologies, in organizations, and in digital futures and agendas" (2022, p. 856). Therefore—they argue, it includes a vision of law and technology as interchangeable instruments to achieve privacy regulatory goals and is at the base of techno-regulation.

It is important to note that in these three previous examples, the proposed imaginary scenarios cover current or past social practices. In other words, they are states of affairs (a set of problems or paradigmatic cases; a legal reasoning or train of thought) whose elements already exist somewhere in the *present* or *past*. In contrast, the second group of scholars comprises scholars

who use the term "imaginaries" (or related expressions) in a very similar manner to STS, in order to describe possible—desirable or undesirable—*futures* that technology may bring about.[29]

Although not talking concretely about imaginaries, Australian legal scholar Kieran Tranter (2011) can be seen as a member of this second group. In 2011, Tranter wrote about **the projection of technological futures by Law & Technology scholars**. According to Tranter, science fiction is the speculative jurisdiction of legal writing, where scholars usually have access to concerning conceptions of technological futures that need law. "The nexus between legal scholarship on technology and science fiction," he argues, "is in the inherent speculation by lawyers of technological futures that orientate and legitimate the project of law and technology" (2011, p. 817).

In a similar way, philosopher Daniel Susser (2022) has recently addressed the **"sociotechnical imaginaries" of privacy and surveillance scholars**. Explicitly drawing on Jasanoff and Kim's concept of "sociotechnical imaginaries," Susser contends that besides critiquing the existing data-driven order and highlighting its possible harms, these scholars should also offer alternatives, "new substantive ideas about what data-driven technologies could do and mean." (2022, p. 300). Therefore, in contrast to Tranter, the future scenarios Susser talks about are desirable.

As these different examples show, it is interesting to see that in opposition to STS, where all uses of the concept of "imaginaries" refer to imagined *futures*, in interdisciplinary scholarship here reviewed only a portion of the uses are future oriented. As well, it is important to note that, among those efforts that do use the concept with reference to the future, none allude to the futures

[29] A similar distinction was done by Margot Kaminski (2022) in *Technological "Disruption" Of The Law's Imagined Scene: Some Lessons From Lex Informatica,* to distinguish the concept of "imagined regulatory scene" from the concept of "sociotechnical imaginaries" used in STS.

that could be achieved through the tool that legal actors are most familiar with, namely, rulemaking. In other words, none of these imaginaries covers the future scenarios that could be achieved not through technology, but *through the regulation of it.*

## 3. My proposed concept: Techno-legal imaginaries

As advanced in the Introduction, in this dissertation I propose the concept of "techno-legal imaginaries." I define "techno-legal imaginaries" as the *visions of a given legal community about the desirable futures that could be achieved through the regulation of technology*. By proposing this concept, my intention is to build upon the theoretical constructs mentioned above, bring different elements of them together, and ultimately fill the gaps left by them (or if using Jasanoff's wording, "occupy the blank space between" them (Jasanoff, 2015a, p. 5)).

As all concepts related to the collective imagination here reviewed, the techno-legal imaginaries proposed in this dissertation are the constructs of the mind of a given community, which come together through shared narratives, are usually underlain by deeper normative notions and commitments, and have a performative power. Nevertheless, the distinctive nature of the techno-legal imaginaries concept resides in the fact that it: (i) specifically applies to *legal actors*; (ii) addresses *future* imaginaries *in relation to technology*; and (iii) makes emphasis on the special role that *regulation* (understood in the broadest way, through law, social norms, the market, and architecture (Reidenberg, 1997; Lessig, 1999)) plays in achieving those futures.

As in George E. Marcus's "technoscientific imaginaries," the techno-legal imaginaries here proposed are foresights of a specific group of society (i.e., scientists/legal actors) about the future possibilities of their work (i.e., scientific/legal) in relation to technology. Likewise, as it happens in the case of Marcus's concept, the concept of techno-legal imaginaries also denotes an evident

faith of their holders in the potential of their corresponding work activity. Thus, while scientists holding "technoscientific imaginaries" trust in the potential of science to achieve future scientific production in new locations of doing science, legal actors holding techno-legal imaginaries have faith in the potential of rulemaking to reach their desirable futures.

Similar to Sheila Jasanoff and Sang-Hyun Kim's concept of "sociotechnical imaginaries" (and therefore in contrast to the concepts of "imagined regulatory scene" and "techno-regulatory imaginary" reviewed earlier), the techno-legal imaginaries are also future oriented, being mainly composed of visions of desired future realities. Additionally, same as "sociotechnical imaginaries" are, they are temporally situated and culturally particular. In that sense, the techno-legal imaginaries tend to be different among different social groups, evolve over time, and can be compared and contrasted among different legal communities.

Yet, unlike the "sociotechnical imaginaries," techno-legal imaginaries are not particularly animated by "shared understandings of forms of social life and social order attainable *through*, and supportive of, *advances in science and technology*" (Jasanoff, 2015a, p. 4). Rather, they are underlaid by shared understandings of forms of social life and social order attainable *through the regulation of technology*. Thus, even though technology keeps playing a central role in these imaginaries—since the regulation we are referring to here is exclusively about tech, the affordances offered by *rule-making activities*—either through formal law, social norms, the market, or architecture—are what is considered fundamental by the holder of the imaginary—the legal actor—to reach the future ideal scenarios. In fact, this especial emphasis on regulation as the main vehicle for archiving the desired futures also makes techno-legal imaginaries different from the approaches to imaginaries in the law proposed by both Kieran Tranter (2011) and Daniel Susser

(2022). Unlike techno-legal imaginaries, in those two cases legal actors are assumed to have visions about certain futures that *technologies*—not legal regulation— might bring about.

Additionally, also in contrast to "sociotechnical imaginaries," techno-legal imaginaries are not always "collectively held, institutionally stabilized, and publicly performed" (Jasanoff, 2015a, p. 4). Therefore, even though they can, they are not necessarily involved in practices of state-making or national governance of innovation processes. For that reason, it can be said that the techno-legal imaginaries are closer to the future-oriented representations proposed by the sociology of expectation, in that they not only play a central role in mobilizing resources at the *macro level*, in national policy through regulation and research patronage, but can also emerge at the *micro and meso level*. In practice, that means that in order to be recognized as such, techno-legal imaginaries do not necessarily need to occupy a dominant position for policy purposes, but simply exist in the minds of individual legal actors or the members of a given legal community.

Finally, and also similar to the future-oriented representations addressed by the sociology of expectations, techno-legal imaginaries are mostly identified in "anticipatory practices." As explained by Carla Alvial-Palavicino & Kornelia Konrad, "anticipatory practices are the way in which expectations about the future, as *material and discourse elements* are circulated and spread throughout different social groups" (2018, p. 194). For instance, law review articles are the main anticipatory practices reviewed in this dissertation. Yet, white papers or policy documents produced by policymakers can also be common anticipatory practices of techno-legal imaginaries.

***

Built in this way, the concept of techno-legal imaginaries—understood once again as *the visions of a given legal community about the desirable futures that could be achieved through the*

*regulation of technology*—emerges as a useful analytical tool to study the endeavors of legal communities involved in the tech policy sphere.

First, if one assumes that every proposed regulation of technology is underpinned by one or more of these visions of desirable future, one can expect to reach a better comprehension of those proposed regulations by understanding their underlaying techno-legal imaginaries. How so? As announced earlier, same as all the concepts related to the collective imagination (as well as all the the other types of imaginaries) here reviewed, techno-legal imaginaries are "*normatively loaded visions* not only of what should be done 'in the world' but also how it should be undertaken and why" (Smith, 2009, p. 462). In that sense, an exploration of the techno-legal imaginary that supports a given proposed regulation of technology can shed light on the values, normative notions, and ideological commitments with which the holders of the imaginary—and proponents of the regulatory intervention—are working.

In practice, understanding an underlying techno-legal imaginary can be useful not only to understand and evaluate a given regulatory proposal around technology, but also to compare regulatory approaches, based on their underpinning visions of desirable future. Additionally, when examined over time—as it is the case in this dissertation (see Chapter VI), techno-legal imaginaries allow researchers to interpret changes in legal reasoning.

Second, and at a more theoretical level, studying the techno-legal imaginaries of particular legal communities offers a possible avenue to investigate one of the possible ways in which the relationship between technology and law is not unidirectional, but rather complex and intertwined with *cognitive* factors. The concept of "techno-legal imaginaries" thus emerges as an effective tool for pursuing the renewed mission Kaminski & Jones (2024) have recently assigned to the Legal Construction of Technology method.

## F. Contribution

The dissertation makes a contribution to both the fields of Law & Technology and Science & Technology Studies ("STS").

Four contributions to the Law & Technology field deserve special attention. By providing a comprehensive intellectual history of a significant sample of American privacy law scholarship, this research provides Law & Technology with a comprehensive view of where the community of scholars here reviewed has been and where it is headed. Specifically, it provides the sub-field of Information Privacy Law with an opportunity to reflect on its journey and possible future directions.

Second, and on a theoretical level, this dissertation develops and expands on the concept of "privacy's algorithmic turn" proposed in prior work (Angel, 2034), providing details of how the turn actually occurred. By tracing in detail how each of the two features of privacy's algorithmic turn occurred, this document allows the field to better understand the different phases that led to the recent widening of the concept of information privacy in a significant portion of American privacy law scholarship.

In third place, by integrating Intellectual History and STS into its methodological and theoretical frameworks, this dissertation adopts an interdisciplinary approach that methodologically enriches the field of Law & Technology in two ways. By drawing on Intellectual History, it provides methodological rigor to an endeavor that is often pursued in the field of Law without a clear methodology. Additionally, by bringing certain cognitive factors into the picture through the concept of "techno-legal imaginaries," this dissertation sophisticates and makes more complex the relationship that may exist between historical sociotechnical changes and the scholars' evolving approaches to Information Privacy. In that way, it sidesteps the technological

exceptionalism perspective often seen in the Law & Technology field (Kaminski, 2017; Jones, 2018).

Finally, and in relation to this last point, this dissertation joins previous efforts in legal scholarship (Jones, 2018; Kaminski & Jones, 2024) to tie the field of Law & Technology to the field of STS. In particular, it offers the Legal Construction of Technology method a tool to scrutinize and bring to light the values and normative commitments embedded in the regulatory proposals of legal actors engaged in the tech policy sphere.

When it comes to Science & Technology Studies, this research project expects to contribute to this field in the following two ways. First, this research project does not only introduce a new theoretical concept of "techno-legal imaginaries", but also provides a case study of it, by examining the case of American privacy law scholars. Secondly, this dissertation continues a quest begun fifteen years ago by Sheila Jasanoff & Sang-Hyun Kim (2015)—and now successfully carried on by the sociology of expectations—of finding new places for imagination in STS literature.

## G. Limitations

The study has, however, certain limitations. To begin with, there are many reasons why the trends and patterns identified both in the intellectual history offered here as well as in Chapter VI cannot be generalized to the whole American privacy law scholarship or the American privacy law field, in general. First, if compared to the massive number of law review articles published every year on the topic of information privacy in the United States, the sample of articles here reviewed is very small. Second, given the encapsulated nature of the community whose work I selected to study (see Chapter I), my sample of articles is also not representative of the diversity of views that exist about information privacy in the American privacy law scholarship field at large. Having said

that, given the significant role of PLSC within the Information Privacy Law field in America (see Chapter I.C), recognizing these trends is still worthwhile.

Furthermore, by highlighting certain trends in the reviewed scholarship and failing to identify others, this dissertation runs the risk of reifying the most popular accounts of information privacy (which may not necessarily be the soundest). To reduce this risk—and the consequent limitation—I endeavored to include in the offered intellectual history approaches that, although unpopular or infrequent within the sample of articles here reviewed, were nonetheless proposed. Also, to avoid placing some approaches under a more positive light, I refrained from weighing the different proposals or providing normative positions about them. However, this limitation may still exist to some extent.

Lastly, I would like to reflect for a moment on my positionality in relation to this research. First, I am aware that my perspective as *a foreign legal scholar* may have influenced the history that I present in this document. On the one hand, my background as a legal researcher from a jurisdiction with a different legal culture has allowed me to compare and contextualize the evolution of privacy law scholarship in America with my own experiences in my home country. In practice, this may have led me to emphasize changes and transformations in the scholars' desirable futures and conceptions of information privacy that would have gone unnoticed or seemed natural for an American legal researcher. On the other hand, it can be sometimes challenging for "outsiders" like me, as a lawyer trained in another jurisdiction, to fully understand the historical and cultural context in which the American privacy law scholarship here reviewed has evolved.

Second, my current identity as *a junior privacy law scholar in America* may have also impacted the development and final result of this research. To begin with, I acknowledge that my

application of the proposed research methods might have been influenced—both positively and negatively—by: (i) the fact that I am by-now a member of the community of scholars whose work I study here; and (ii) the fact that many of my interviewees (who are also the authors of several of the reviewed articles) are also prominent figures in this community, with whom there may be a power relationship. While this "insider" position provided me with a familiarity with the field and the Privacy Law Scholars Conference, and relatively easy access to my interviewees, it may have also unconsciously influenced how I conducted the oral history interviews and/or inhibited my ability to take a more critical stance when analyzing the data. This, specially taking into account that, unlike other historical studies where there is a break between the present and the past, this research project addresses the history of "very recent past" that is "not dead yet" (Romano, 2012, p. 27) and therefore, my "subjects of study" and interviewees "can indeed talk back" (Leahy, 2021, p. 1).

In third and last place, I am also aware that having presented a draft of my article *Privacy's Algorithmic Turn* at PLSC 2023 and a related draft at We Robot 2023 conference as well as at a Boston University Law Review conference may have influenced the responses of three interviewees—Paul Ohm, Pauline Kim, and Andrew Selbst—who attended at least one of these conferences and whose interviews were conducted after these events. As pointed out by Paul Ohm himself during the interview, "[i]t's funny, because you're now doing interviews after your draft is out in the world, and so there's a little bit of a, this is less of a pristine environment for you" (P. Ohm, oral history interview, September 22, 2023). Yet, I hope to have partly mitigated this limitation by treating the oral history interviews as a triangulation point on background.

## H. A roadmap

This dissertation proceeds as follows. In Chapter I, I present a comprehensive—though probably imperfect—picture of the Privacy Law Scholars Conference ("PLSC"). For this purpose, I examine its origins, development, and renowned discussion format. Likewise, to gain a deeper understanding of the community of scholars that has developed *around* PLSC, I explore the conference's guiding principles as well as the elements that make this community a suitable subject for study under the concept of "community of discourse" proposed by David Hollinger (1985). To conclude this Chapter, I briefly discuss the relevance of the conference for the field of American Information Privacy law.

Next, in Chapters II through V, I present the intellectual history of privacy's algorithmic turn. Thus, in each of these chapters, I introduce the reader to the sociotechnical and techno-legal context of each period covered (1990-1999; 2000-2007; 2008-2014; 2015-2020), *as viewed through the lenses of the scholars here examined*. The chapters present information regarding the most relevant information technologies and practices of the era, the societal attitudes that surrounded these technologies and practices, and the different ways in which the existing legal system responded to them (both in the United States and, if applicable, in the European Union). Following this, I present the harms that scholars writing during those respective years considered most important, as well as the legal tools they would propose to protect information privacy during that period. Lastly, I conclude each chapter with a set of reflections and conclusions that will hopefully help the reader understand how privacy's algorithmic turn gradually developed over the four decades covered.

The purpose of Chapter VI is to demonstrate that the transformation of scholars' techno-legal imaginaries over the period of time covered by this study (1990-2020) provides us with an

insight to better understand the second feature of privacy's algorithmic turn, namely, the transformation of the tools proposed by the scholars to protect information privacy. Therefore, I begin by describing the techno-legal imaginary that may have influenced the scholar's preference for a FIPs-based legislative approach between 1990 and 2007. In the following section, I describe the one that might be underlying the batch of hands-on tools proposed by a considerable group of scholars by the end of the 2015-2020 period. In both cases, I discuss (1) the narratives that bring each imaginary together, as well as (2) the desirable future that American privacy law scholars expect Information Privacy law to achieve in each case.

In the Conclusion I wrap up the dissertation and propose a tentative agenda for future research.

## I. The Privacy Law Scholars Conference: A Community of Discourse

As announced in the Introduction, in this research project I trace, in detail, the evolution of the concept of information privacy in a sample of papers published by the community of scholars that has developed *around* the Privacy Law Scholars Conference ("PLSC"). PLSC has been taking place in the United States since 2008, annually assembling "a wide array of privacy law scholars and practitioners from around the world to discuss current issues in information privacy law and policy" (*PLSC History – Privacy Law Scholars Conference*, n.d.).

As will be shown in this Chapter, this annual event has fostered an interdisciplinary community of mostly American scholars—although with some participation of international scholars and a decreasing number of practitioners—with a wide range of academic maturity levels. Also, this community possesses all of the characteristics required to be considered a "community of discourse," in the sense proposed by David A. Hollinger (1985). As such, its intellectual work appropriately lends itself to be analyzed through the lens of the study of the discourse of intellectuals suggested by Hollinger (1985).

This Chapter proceeds as follows. First, I will examine the origin, evolution, and format of PLSC, emphasizing its successes (the discussion format it follows) as well as its shortcomings (the invitation-only model it initially followed, which has led to repeated criticism regarding the lack of diversity among its participants). Second, I will study the community of scholars that has developed *around* PLSC, both in terms of its guiding principles and the elements that make it apt to be considered a "community of discourse." Finally, I will close the Chapter by considering the relevance of the conference for the field of Privacy law in America. As will be seen, in spite of the

fact that the field was not born with PLSC, this conference has not only coalesced the field, but also provided its attendees with the conditions for considering themselves a part of it.

## A. The conference

### 1. Origin

PLSC was co-founded in 2008 by Daniel Solove and Chris Jay Hoofnagle, to bring together people working on and writing about similar sets of problems. According to Solove, "we thought there really should be a conference that, you know... At that point there were some scholars, not a lot. But there, there was enough that we thought, 'yeah enough people writing in the area, *it would be great to bring people together*'" (D. J. Solove, oral history interview, February 26, 2023). Similarly, during his oral history interview, co-founder Chris Hoofnagle added:

> Dan and I were interested in *coalescing Privacy Law as a field*. (…) And the other problem that we found was, there was a kind of difficulty in placing scholarship, because privacy, it wasn't clear where Privacy Law existed. When people talk about Tech Law, what they typically mean is Intellectual Property [(IP)]. So, like a Tech Law center, IP, Patent, Trademark, blah, blah, blah. And *we wanted to bust out and say, "there is this new field*, and it's not Cyber Law, and it's not Software Law, and it's not Trademark, Patents, blah, blah, blah. It's this other thing that's important." (…) (oral history interview, September 8, 2023)

Consequently, among other objectives (e.g., the growth potential for this area of law; Solove's desire to identify people teaching Privacy Law (Chris Hoofnagle, oral history interview, September 8, 2023)), the main purpose of bringing together people writing about similar problems was to create a space for Privacy Law to rise as an independent area of law, apart from Intellectual Property. Indeed, when asked about his knowledge of PLSC's origins, Woodrow Hartzog would similarly refer to the need to separate privacy scholarship from Intellectual Property alluded by Hoofnagle. According to Hartzog's own recollection,

> [i]t's my understanding that PLSC happened because the IP, the Intellectual Property scholars community, kicked the privacy people out (*laugh*). They used to go to a conference, I think it was called [Intellectual Property Scholars Conference] IPSC, that had like a privacy track. And the privacy people were happy to have that little track, because there weren't that many of them. (…) But apparently, the story goes, they got kicked out of IPSC because IP was getting so big, they couldn't afford the privacy track anymore. So, Dan and Chris looked around and said: "Well, I guess we'll do a little, sort of workshop, paper workshop." (oral history interview, February 27, 2023)

Initially, PLSC was born "as a *very small invitation-only* workshop" (J. E. Cohen, oral history interview, February 27, 2023). As to its small size, during his oral history interview Solove would attribute it to the fact that very little work on privacy was occurring at that time. According to him,

> [w]hen I started the Privacy Law Scholars Conference [(PLSC)], in the early, in the mid aughts, we had 12 papers. *I struggled to find papers, we actually, Chris [Hoofnagle] and I had to solicit people to do the papers.* We didn't have, you know, we asked for submissions. We got like maybe one or two people, actually, sent something in. No one knew about the conference, and I reached out to anybody who, you know, had something somewhat related, and said, "please, you know, do your paper here." Different now, where, yeah, we got, there's like a gazillion submissions to the PLSC, and it's much bigger. But at the early days, you know, I just, anyone who is in the vicinity, and has something somewhat related like, "please come in because we need many people." (oral history interview, February 26, 2023)

Regarding the invitation-only model, Solove would justify it based on budget and space constraints, as well as the existence of far fewer online resources than are available today to advertise the event. Moreover, he would once again emphasize the fact that there were very few scholars working on privacy at the time. "[O]ne reason why we had an invitation only was because *I didn't know who would say yes, and who would say no*. And in the early days, *there's only a small group of the core privacy people, so we wanted to make sure they're definitely going*" (D. J. Solove, oral history interview, February 26, 2023), he would explain. It is interesting to note, though, that

Solove did not generally believe this meant that interested people would be prevented from attending the conference if they so desired. In his words,

> anyone who wanted in, would get in. So, a lot of the people would just say, "hey, I've heard about this conference," and we'd let them in. I mean it was, you know, we wanted everybody that we could get. But, you know, they had to hear about us. We just didn't advertise. But there wasn't anyone who you know, came along, and they said, "hey, we want in," and we wouldn't like, let them in, unless they were, you know, unless we ran out of spots or, and sometimes it was practitioners...For any academic they were in. And then for practitioners, you know, we would just want to make sure we didn't give too many spots it would make it a practitioner conference, so we would definitely be cautious about, like, letting in too many of them. So, there are sometimes where we said, "look, we don't have enough spots. We're running tight." So, we turned away a practitioner or two, but we rarely turned away anybody, anyone who wanted it could pretty much get it, and they just had to write to ask. (oral history interview, February 26, 2023)

Over the years, however, this invitation-only model would take a toll on the conference, forcing it to switch to an open format. As much as it ensured the attendance of a specific specialized audience and the consolidation of a "core" circle of scholars (see Section B of this Chapter), it also made the conference a target of criticism based on a lack of diversity in the attendance pool. As we shall see in the following Sub-section, this restrictive model initially adopted led PLSC to miss out on the opportunity to gain valuable insights from individuals from marginalized groups who did not have access to influential academic networks, as well as from more diverse perspectives about privacy.

Finally, a third characteristic of the conference in its beginnings was that attendance was free of charge. Sponsored by the law firm Proskauer Rose, LLP, and the private companies ChoicePoint, AT&T, and IBM, PLSC's first convening was held in June 12-13, 2008 at George Washington University (GW) Law School with 132 participants (*Privacy Law Scholars Conference 2008*, n.d.). There were only 12 papers discussed, which were distributed in the following five tracks: (i) General and Philosophical (the theory track); (ii) Economics and Business

Practices, (iii) Technology and Anonymity; (iv) Social Networking and Media; and (v) Government Surveillance (C. J. Hoofnagle, oral history interview, September 8, 2023). The event was hosted by the Berkeley Center for Law & Technology and the GW Law School Intellectual Property Law Program, and it was agreed that the conference would be held annually, alternating between GW and UC Berkeley (D. J. Solove, oral history interview, February 26, 2023).

## 2. Evolution

In June 2024, PLSC will turn 16 years old. Over these years, several changes have taken place within the conference. Fundamentally, the size of the conference increased significantly. In its version #15, PLSC 2023 hosted 225 participants to discuss 78 papers (*PLSC 2023 – Privacy Law Scholars Conference*, n.d.). As explained by Julie Cohen in her oral history interview,

> it gradually broadened out, you know, to include more and more and more people, because people heard that it was great, and asked to be invited, and people asked to have, you know, other people invited. And then, ultimately, we transitioned the organization to kind of a more sustainable and defensible structure *for a big professional and academic conference*. (oral history interview, February 27, 2023)

Notably, this growth was not without resistance. As explained by Daniel Solove during his interview,

> every year we had this *tension* where some people would say "if it gets too big, if it gets to like 200 more, if we have 200 people, it used to be smaller, and we had a lot more time with everybody, and now it's so big, and *it's getting impersonal*." On the other hand, we didn't want to cap it so that it would, you cap it too much, because then *we want the field to grow*. But we always had this worry that if it got too big, what if it got to be 300 people, 400 people, 500 people, you know, *is it going to lose its intimacy*? And is it going to lose that, you know... And there's only so many breakout rooms, so we don't want, you know, if we have 100 people in a session, you can't have a conversation with 100 people. (oral history interview, February 26, 2023)

Thus, as the years progressed, a tension developed between promoting the growth of the field and maintaining the conference's intimate nature. In fact, this loss of intimacy worry was similarly reflected as a criticism in one of the other oral history interviews held for this project. Asked what he enjoyed most about the conference, Michael Froomkin stated:

> I loved it *in its early days, when it was small* and, you know, you could... It was, it started out as a single-track conference. And then it went into a double-track conference. Even that was manageable. You could sort of read most of the papers, you could get your arms around it. Now it's, last time I went it was a six track, it was, you know, it's like going to a big circus, you don't know where to look. There's too much going on, you know...Every time there's three things I'd like to go to. So, *I loved it best when it was smaller*. On the other hand, the advantage of the bigger size is much more inclusion. That's a virtue, and it's a trade-off. (oral history interview, September 21, 2023)

In any case, as a result of this growth, several other changes followed. First, a Program and Planning Committee (PPC) was created. As narrated by Solove, "eventually, we had so many abstracts, and just so much that we had to, you know, 'okay, we can't do this ourselves.' We created a committee to help us select papers" (oral history interview, February 26, 2023). According to the PLSC Charter, the PPC is composed of a minimum of 7 people and a maximum of 15 people, and "shall be responsible for selecting the Host Institutions for the PLSC, soliciting and selecting papers to be workshopped at the PLSC, managing participation at the PLSC, developing and adopting a code of conduct for the PLSC, and making all other strategic decisions relating to the PLSC" (*PLSC Charter – Privacy Law Scholars Conference*, n.d.).

Second, besides getting more sponsors and setting different attendance fees for different categories of participants, the conference' organizers decided to place an open call for new host institutions—besides GW and UC Berkeley—that could offer more breakout rooms as well as a big conference room (*PLSC Charter – Privacy Law Scholars Conference*, n.d.; D. J. Solove, oral history interview, February 26, 2023). Consequently, since 2021 the conference has been held at

Georgetown University (2021) (although, due to the COVID-19 pandemic, PLSC 2021 was finally held 100% virtual), Northeastern University (2022), and the University of Colorado (2023) (*PLSC History – Privacy Law Scholars Conference*, n.d.).

A third noteworthy change was partly the consequence of a clash in the emerging community, which seemed to explode at PLSC 2019 and initially revolved around one of the conference's sponsors—the technology company Palentir. In a letter that became public a day before the 2019 conference, a group of scholars called on the conference's convening committee and Berkeley Law School to drop Palantir as a PLSC sponsor. According to the language of the missive,

> We appreciate that the PLSC planning committee released a sponsorship agreement policy [—signed in October 2018 by Chris Jay Hoofnagle & Daniel J. Solove, as co-chairs of the conference, and the by then members of the PLSC PPC (*PLSC Sponsorship Statement – Privacy Law Scholars Conference*, n.d.)—], and we know that corporate sponsorships present complex questions that may not be easily resolved. We also understand the need to secure funding. PLSC's policy makes clear that sponsors don't influence the programming or content. But even without direct influence, *we are deeply concerned that Palantir's sponsorship of a leading academic conference on privacy helps the company polish its image, and thus undermines efforts to resist militarized surveillance against migrants and marginalized communities*. (*Scholars Tell UC Berkeley: Cut Ties with Palantir*, 2019)

Referring to this schism, during his oral history interview Paul Ohm would describe it in the following terms:

> So, it was, it was the year, it was at Berkeley before the pandemic. And it was, you know, four or five people, so Alvaro Bedoya and Laura Moy, my colleagues, were two of them, but they were not alone at all. And there was leafleting that happened at one of the breaks and there was all this recrimination throughout the entire conference. And yeah, it was a super, super difficult, and sad, and distracting conference. Umm... And I think that probably there might have been some agitation the year before. And as I recall, *a lot of this was channeled not originally through a diversity lens, but through the Palantir funding complains. But that sparked and grew and became, had a life of its own*. And then eventually, became embraced by certain *members of the inner circle* and the Program Committee. So started as *an external critique*, but quickly got adopted by some of the *internal players* as well. (oral history interview, September 22, 2023)

Before discussing the consequences of this schism on the evolution of the conference, two points should be noted about this quote. To begin with, although the internal division within PLSC initially revolved around the conference's funding sources, it later evolved to include complaints concerning the lack of diversity among its participants. Further, Ohm's account also illustrates a characteristic of the emerging community that will be discussed later on in this Chapter, and which revolves around an implied stratification that exists between internal/inner circle and external actors, with Alvaro Bedoya and Laura Moy included by Ohm in the latter group.

As a result of the described conflict, in 2021, PLSC moved for the first time to an open format, where not only an open call for submission of abstracts of papers is widely circulated every year, but anyone can attend/register without an invitation. Likewise, the current PLSC Charter also requires the PPC to make special efforts to encourage individuals from underrepresented groups to participate in the conference, and as part of the conference foundation principles includes: "The PLSC welcomes participants of all races, ethnicities, nationalities, genders, gender identities, sexual orientations, and religions, and it encourages submitted papers that engage with issues of systemic and/or structural bias and inequality" (*PLSC Charter – Privacy Law Scholars Conference*, n.d.). Lastly, starting on 2021 submitted abstracts are blind reviewed by the PPC, although "the final selection of papers [still] need not be blind" (*PLSC Charter – Privacy Law Scholars Conference*, n.d.). When referring to this latter change, during his oral history interview Paul Ohm would express:

> (…) we went from not blind to blind, you know, assessment of abstracts; and what that has meant is, it used to be PLSC was Neil [Richards]'s paper, Woody [Hartzog]'s paper, Dan [Solove]'s paper, Orin [Kerr]'s paper, Paul [Schwartz]'s paper and that doesn't work anymore; and like famous senior scholars now get boxed out and they get really mad. And that's just one of the prices we've paid with this, what I think was a really welcome intervention to reform the conference (…). (oral history interview, September 22, 2023)

Finally, as part of this last batch of changes that took effect in 2021, Ari Ezra Waldman was elected as the PLSC Chair for the next three years, as Daniel Solove and Chris Hoofnagle decided to step down from the direction of the conference. In Solove's words, "eventually, we had, you know, after, I think, it was about 13 or 14 years, we stepped aside, and other people run it" (oral history interview, February 26, 2023). Similarly, during his interview Hoofnagle expressed:

> I decided that it would be important for me to kind of get out of the way. I ran the, I ran the event for a long-time and... Too long, and you know, what happens with institutions: People who start things are often not the right person to maintain them. And so, Ari Waldman, who's brilliant, sensitive, accomplished, wonderful, and like... He wanted to do it, and he's doing it and taking it in different directions. And I've decided to stay away so that he can, he can do what he wants to do. (oral history interview, September 8, 2023)

In fact, a clear portion of Ari Waldman's mission as the new Chair has been to promote a diverse and inclusive scholarly community. As described by Waldman himself,

> [t]here are certain things that we've been working on, and while I've been the chair, during the time that I've been its chair, there are a lot of things that we're working on to make PLSC better. For example, *make it more accessible, make it more diverse*. Make sure it's open and accessible to a lot of people who didn't really think PLSC was for them in the past, because it used to be invite only, and it used to be relatively restrictive. But we've done a lot of good work with the present committee in, um, *committing PLSC to an anti-subordination agenda*. And now that we've done that, I think it's even better. (oral history interview, November 30, 2022)

Despite these changes and commitments, remains of criticism about the conference's lack of diversity—in terms of race, gender, and different viewpoints— were still identified in some of the oral history interviews conducted for this research project. According to Anita Allen, for example,

> in the last few years I've been consulting with *some younger scholars of color*, who believe that the conference is often, is like an *old boys' network* to them, and they feel like...And I know that there's been a big effort to try—through Ari [Waldman] and others—to try to get the conference to be more inclusive. And, you know, I think, that

> Ari Waldman is doing a great job and so forth. *But it needs to be a space where everybody feels welcome, and everybody's privacy issues feel welcome*. I mean, it's not acceptable to marginalize the *privacy concerns of people of color or disabled people*, or you know, whatever. It is just no longer acceptable, and I think that *they need to select papers that reflect the diversity of the community*. And I think they're trying, they're doing that better than they did ten years ago, to be sure. (oral history interview, March 30, 2002)

Although from a different perspective—viewpoints diversity, during her interview Pauline Kim would relatedly point out:

> So, and I'll say this, I think, it's maybe one limitation of PLSC. *PLSC tends to get people who are fairly like-minded in terms of normative goals*, even though we may differ a lot in terms of how is the best way to get there, how to conceptualize a problem or how to read a particular case, or how to define a particular challenge. We don't... I know *there are people out there who think about data and privacy very, very differently*, right? Like, "it should be all commercializable, it should be all commodifiable," right? And *there are a lot of techno-optimists out in the world,* who would say about my work and many others that we're just sort of, you know, raising alarms or missing how this is going to be the best of all possible worlds. *And we do miss that a little bit in PLSC*, I think that we... It probably might be a more rigorous environment, I mean, it is pretty rigorous environment, but *it might be a little bit more...rigorous in a challenging way if we had more of those views*. (oral history interview, November 30, 2023)

Despite not necessarily representative, these pieces of criticism are still valuable. They suggest that despite the great number of changes implemented in the last few years, PLSC still has work to do in diversifying its pool of attendees. And while several efforts have been done to specially address the race and gender issues raised by Anita Allen in her quote, a lesser amount of attention appears to have been paid to integrating into the community participants who view privacy in manners at odds with the PLSC's apparent shared normative goals and undeniably positive views about privacy.

### 3. Format

Since its inception, PLSC was designed to "provide support for *in-progress* scholarship" (*Call for Abstracts: Privacy Law Scholars Conference 2024*, n.d.). Accordingly, the format followed during the conference differs significantly from that usually used to discuss camera-ready papers at other "more conventional" (J. E. Cohen, oral history interview, February 27, 2023) academic conferences. At PLSC there are no published proceedings, no panels, and the discussions are conducted in a paper workshop format. As regularly described in the conference's agendas between 2014 and 2020,

> At PLSC, papers workshops are led by a "commenter" who facilitates a discussion among participants on an author's paper. Authors are encouraged to participate in "listening" mode. There are no panels or talking head events at PLSC.
> All participants are expected to read and be prepared to discuss one paper per session (…), and thus PLSC requires significant preparation. We recommended (sic) that participants devote 1.5 to 2 days of reading to prepare prior to the conference. (*2018 Privacy Law Scholars Conference (PLSC2018)*, n.d.)

Similarly, since 2021 the conference's calls for abstracts state:

> PLSC is a *paper workshop conference*. It offers no opportunity or obligation to publish. The goal is to provide support for in-progress scholarship related to information privacy law. (…) *We follow a format in which a discussant, rather than the author, introduces and leads a discussion on a paper. There are no panels or talking heads; attendees read papers in advance and offer constructive feedback as full participants in the workshop*. (*Call for Abstracts: Privacy Law Scholars Conference 2024*, n.d.)

Thus, instead of the papers' authors, the paper and the attendees are the primary protagonists in this format. Moderated by a discussant who briefly introduces and criticizes the paper, participants attending the session are expected to provide feedback and comments to the author based on their previous reading of a provided draft. According to Daniel Solove, this

methodology was derived from elements of other conferences[30] which, based on his own experience, he liked as well as those which he found annoying:

> One thing I hated about a lot of conferences was: you travel all this way, you go there, and then people would just spend most of the time just summarizing their papers. And then there was time for like one question, and that was it. And, I thought, "what's the point of everyone getting together if, you know, it's just reading comprehension," like, okay, someone's just, you know, doing the cliff notes of their papers. "*I want to talk to people. I want to engage with them*. I don't want to just, you know, I can read their papers on my own time, but the whole point is to talk to people and have a discussion." So that was one thing that made me just, yeah, a little bit annoyed at conferences, *the lost opportunities*. And so that's one reason why we have the rule, like, you read the papers in advance, you come, and it's expected that you read the papers in advance, we're not going to spend much time summarizing things.
> And then, another thing was that *we wanted many breaks*, so that it's not like, like a lot of conferences I go to, that it's like, you know, 5 minutes between sessions and you don't have enough time to really talk to people in the hallways, and that's where some of the best conversations happen. So, we wanted to have good break time between the sessions, *so people could really talk to each other*.
> And then, *the other thing we wanted was a kind of seminar style*, where people would have discussions rather than just be talked at. You know, sitting passively for a whole day and just hearing people talk at you is just less fun than if you're really engaged in a conversation. We wanted to say, "okay, let's make the whole of that like this, and let's be pretty rigorous about it."
> And then, the other thing that I learned, it was a conference that we had at Seaton Hall. And one of the really interesting and fun things that we did—it was a retreat, and I don't know who came up with the idea, but it was a brilliant idea, and *the idea is that you wouldn't present our own papers*. To prevent someone to do that we have someone else present the paper and do a little critique of it, but summarize it, and then the author can do a very short response. And the idea was to try to, you know, someone else seeing your paper and presenting it, you could learn, like what things they see are the important things in the paper. Because a lot of times, you know, people don't really know what their real, most important point is, close to it. So, I thought that was a great idea. (…)
> But anyway, we, you know, implemented that, like "hey! authors do not present their own work. We want to keep it super short, and then *we really want the discussion to flow*." And that was the, those were the basic principles. (oral history interview, February 26, 2023)

During his oral history interview, Chris Hoofnagle would corroborate these basic principles. According to him,

[30] The commentator model mentioned above, for example, seems to have been adopted from the University of Oxford.

> [w]ell, Dan was brilliant. Because he said, "this is our event, so we could make it however we want." And so, what we did is *we created very long breaks*, like the breaks would be 30 to 45 minutes long; the afternoon would essentially be off, so you'd be done by like 2'clock. And we also didn't do things like pollute the lunch with a keynote. So, the result was, is that *it created a huge amount of networking*. There was just time to just talk.
> And the other thing is, *we had no panels*, and this was totally key. No panels. The author shows up with a paper. The paper is presented by what we called a "commenter." I don't, I don't know why, that's just the word we used. And as a result, there were no talking heads, and we avoided the problem of an author just yapping for an hour. And it turns out that *people loved this format* because, see, authors loved it, because they could listen to careful readers understand what their paper says. And then the participants loved it because they got to speak (*laugh*). (oral history interview, September 8, 2023)

Therefore, the idea of the co-founders was to adopt a format that would provide attendees with formal (workshop sessions) and informal (breaks) spaces for in-depth discussion about the papers as well as ample networking opportunities. And according to some testimonies collected during my oral history interviews, it seems to have successfully worked. Among my other thirteen interviewees, six praised these community norms during their oral histories (Ari Waldman, Julie Cohen, Woodrow Hartzog, Priscilla Regan, Andrew Selbst, and Pauline Kim).

First, some of them would highlight what this methodology has done for the community. Hartzog, for example, would describe this idea as "kind of mad and brilliant, and it works to incredible effects to help build the community" (oral history interview, February 27, 2023). Relatedly, Selbst would express:

> [O]ne thing I think that model has done, right? First of all, everybody takes the scholarship really seriously, but it's *a collaborative* model. And so, you're all in there with draft papers and so you're not in there to shoot each other down. You're in there to improve each other's work. I think *the result of that is the Privacy law community is actually really tight knit and like this is not all assholes* (*laugh*). Everybody's friendly, and gets along, (…). (oral history interview, October 26, 2023)

Second, interviewees would also underscore what this format has offered them individually as scholars, both when presenting a paper and when attending a session as

participants. For Priscilla Regan, for instance, "[i]n terms of being able to get feedback and have a real discussion of the ideas that you've raised in the paper, is absolutely wonderful. It's a fantastic format" ( oral history interview, September 18, 2023). Similarly, Pauline Kim would assert:

> At PLSC, because they've developed a strong norm of reading, of the audience reading and engaging, *it makes it very valuable as a place to present*. And then also, as just as a participant, because you know you have to read (*laugh*), you do read, and then the sessions are that much more engaging because you've all read the same thing, and you can sort of hear other people's takes on the paper. In that sense I just feel like *I learn a lot more, it asks more of me, but therefore I invest more and then I get more out of it.* (oral history interview, November 30, 2023)

In addition, some of these interviewees—including PLSC co-founder Chris Hoofnagle (oral history interview, September 8, 2023)—would cite as evidence of the model's success the fact that it has been copied or "totally stolen" (A. D. Selbst, oral history interview, October 26, 2023) by other conferences in the field. For Cohen, "almost everything now is kind of derivative of PLSC in some way. PLSC really reshaped the field. So, there's a thing that's actually called 'PLSC Europe,' that happens every once in a while, where they've adopted the PLSC model" (oral history interview, February 27, 2023). In Hartzog's view, in turn, "I don't know how standard that was in the legal scholarly academy before PLSC did it, but it certainly has become popular afterwards. We Robot [Conference] was based on this, for example, and a couple of others" (oral history interview, February 27, 2023).

Thus, just as the invitation-only model adopted at the beginning of PLSC could have adversely impacted the development of the conference in terms of diversity, its characteristic discussion format—also adopted since PLSC's inception—has helped the conference stand out and be very highly regarded by many of its attendees.

## B. The community

### 1. Guiding principles

Albeit probably implicitly, the organization of PLSC has also been guided by a set of principles. Based on Daniel Solove's account, "the recipe for the conference" included "established scholars doing papers (…), junior scholars doing papers (…), people from around the world, (…) practitioners and academics" (oral history interview, February 26, 2023). Put another way, the conference's founders wanted "to have it be *interdisciplinary*," "to make sure that the conference would be, you know, *open to the junior folks*," "to make it open to all sorts of fields, and also *internationally*," and finally, to "make sure that there were *people from practice* involved" (D. J. Solove, oral history interview, February 26, 2023).

While outside of this research's primary objectives, some of the accounts from the interviewed scholars, in addition to the evidence collected through the PLSC database built for this project, corroborated, to some degree, the *existence* of each of these principles nearly 16 years after the conference was founded.

#### 1.1. Interdisciplinarity

In terms of interdisciplinarity, during his interview Andrew Selbst would express: "(…) PLSC still, well, *it's not just Law*, right? It takes in people from Engineering, you have some people who are maybe lawyers, but not in Law Departments basically too. And then you people like yourself, right? There are STS folks, *so it's somewhat interdisciplinary*" (oral history interview, October 26, 2023). Similarly, Solove himself would confirm that, over the years, "we had some great people in *Computer Science* attend and *Sociology* and *Economics*. Alessandro Acquisti was an early participant, and just doing some really interesting things that are really eye opening and helpful in

developing our scholarship" (oral history interview, February 26, 2023). Likewise, when describing what he calls as PLSC's "inner circle," Paul Ohm would refer to the "interdisciplinary group" (oral history interview, September 22, 2023), including in there as examples scholars Helen Nissenbaum and Alessandro Acquisti, whose fields of work are Philosophy and Behavioral Economics, respectively.

Based on the PLSC database built for this project, other non-legal scholars who have also regularly attended PLSC[31] include, among others, Priscilla M. Regan (Political Science) (included as part of the sample of interviewees), Lorrie Cranor (Engineering and Public Policy), Mark MacCarthy (Economics), Colin J. Bennett (Political Science), danah boyd (Computer Science, STS, and Information Studies), Kirsten Martin (Business), Seda Gurses (Engineering), Solon Barocas (Communications), Madelyn R. Sanfilippo (Information Science), Alice Marwick (Communications), and Sebastian Benthall (Engineering).

### 1.2. Openness to junior scholars

As said, PLSC co-founders saw the conference as an opportunity to "encourage junior scholars to get into the field and get mentorship" (Daniel Solove, oral history interview, February 26, 2023). According to Daniel Solove,

> (…) would definitely put a thumb on the scale of a junior scholar, didn't mean they automatically got the paper accepted, but it did mean that *we would, you know, try, you know, hard to give them a spot* even if their paper, you know, needed a little bit of work, or it wasn't quite as strong as, you know, some more established scholars. (oral history interview, February 26, 2023)

Although not fully supported—since a separate research project would have to be conducted for this purpose, anecdotal testimony from three interviewees can shed some light on the actual

[31] All of them workshopped three or more papers at the conference between 2008 and 2020.

opportunities given in the conference to once, junior scholars. For Karen Levy, who was a postdoctoral fellow at both NYU's Information Law Institute and the Data and Society Research Institute when she presented her first paper at PLSC in 2014, PLSC has significantly contributed to her career as an academic. As expressed by Levy during her oral history,

> [PLSC] (…) feels like my home conference, is the conference I'm most excited to go to every year, I'm on the organizing committee, it's very close to my heart. I really like the style of it. *I like that I feel like it's welcoming to junior scholars* and it's welcoming across disciplines. I mean, it has work to do as all institutions do, but I think... Yeah, I feel very... *I owe a lot to that community too. Like I wouldn't, I certainly wouldn't be where I am if not for the guidance of that community.* (oral history interview, November 17, 2023)

Relatedly, in a separate part of the interview she would add:

> (…) *generally speaking, I have found it to be an incredibly supportive and cohesive community for myself personally*, like I have found that it is really, really, *easy to get informal feedback and mentorship* from people. And I just like don't, I'm part of lots of intellectual fields, but this is definitely the feel that stands out to me as being *the most strongly oriented towards like, junior support*. So, I *owe like tons and tons of my own intellectual development to this field*." (K. Levy, oral history interview, November 17, 2023)

Equally, Ari Waldman—who won PLSC's Best Paper Award in both 2017 and 2019 and is nowadays the conference's Chair—workshopped his first paper at PLSC—*Privacy as Trust*—while he was still a Ph.D. candidate in Sociology. According to Waldman's own account,

> (…) it turned out that at that same conference two other scholars, Neil Richards and Woody Hartzog also submitted a paper about privacy and trust. So it was, *but it was a really good opportunity, it was a little scary as a newbie, um, that these more senior scholars are writing about the same thing. But it was a great way to meet them, and they also became, um, my, some of my great best friends in the academy*. (oral history interview, November 30, 2022)

The third anecdotal piece of evidence comes from Woodrow Hartzog, who presented his first PLSC paper in 2009, while still doing his Ph.D. in Mass Communication. When asked whether he feels part of the PLSC community, Hartzog clearly responded:

> Yeah, oh, absolutely. Thanks to the generosity of the people that came before me, *setting an explicit norm of wanting to foster junior scholarship* and wanting to avoid some of the pathologies that are in other areas of legal scholarship, that tend to be very gate-keepy. And *I think that some of the early scholars did a really great job of setting a different norm of inclusivity*. And, as a result, I've always felt like I had a place to discuss ideas and ideas were taken seriously. *Even as a junior scholar, someone who was still very new to the space, and had no real idea what he was doing*. People took the idea seriously and engaged with it, and that meant the world to me. (oral history interview, February 27, 2023)

Cited as examples, these testimonies illustrate how PLSC appears to have established itself as a nurturing environment for junior scholars, providing them with a supportive platform to grow and improve their scholarship. In particular, the conference's commitment to fostering a supportive and collaborative atmosphere, where junior researchers can exchange ideas, seek informal feedback and mentorship, and build professional networks, seems to have been a critical factor in this outcome.

### 1.3. Internationally diverse character

When it comes to PLSC's international component, corroborating the implementation of this guiding principle in practice was also outside of this research's objectives. However, extracts from the oral history interviews conducted can give us some lights on the matter.

In two of the interviews conducted (P. M. Regan, oral history interview, September 18, 2023; N. M. Richards, oral history interview, April 14, 2023), narrators provided specific names of scholars from Europe and Canada attending PLSC: Natali Helberger (Germany), late Ian Kerr (Canada), and Colin Bennett (Canada). Likewise, a superficial review of the PLSC database built for this project yields that the list of international scholars who regularly attend PLSC[32] also includes, among others, Tal Zarsky (Israel), Frederik Zuiderveen Borgesius (the Netherlands),

[32] They workshopped three or more papers at the conference between 2008 and 2020.

Joris Van Hoboken (the Netherlands), Sandra Wachter (UK), Lilian Edwards (UK), Jonathon Penney (Canada), and Ignacio Cofone (Canada).

Perhaps thinking about these names, in his oral history interview Neil Richards described PLSC as "an intellectual home" for, among others,

> *scholars from other countries*, Canada, the Netherlands, the United Kingdom, Ireland. I'm missing a major constituency there. I would say that's probably... Belgium, though many of the Belgian professors are Dutch. There are some German academics, (…). So, it's this annual... convention is the wrong word. But *it is an annual gathering of people from around the world*, who do this. (oral history interview, April 14, 2023)

This "around the word" reach, however, does not seem to be agreed by everyone in the community. When asked about the representativeness of PLSC in comparison to the Privacy law field, during her oral history interview Karen Levy contended:

> The international component of it, I have to admit, I'm just not super, like I have not, International or Comparative Privacy law has not been an area of focus for me. *Some of that work I know is represented at PLSC, although largely it's European and American, right? Like there's a LITTLE bit of work from other parts of the world, but it's pretty minimal.* So, that, certainly, I mean, there's obviously a lot more Privacy law in the world or like people thinking about privacy than is represented at PLSC. And part of that is a geographic focus. (oral history interview, November 17, 2023)

As a result, although it is certainly true that PLSC has attracted many international academics from North America and Europe, this is probably not enough for the conference to be considered an *international* conference. Particularly, there is still an apparent lack of representation of academics from Latin America, Asia, and Africa working on privacy issues in those jurisdictions.

### 1.4. Openness to legal practitioners

Finally, within this research, existing evidence about the conference's openness to people from practice is mixed. On the one hand, when talking about law firm partners Mike Hintze, Kirk Nahra,

and Ed McNicholas—who also teach the Information Privacy Law course at different universities, Neil Richards highlighted:

> [I]nterestingly, Mike and Kirk, and McNicholas, (…), are all members of the PLSC community as well, which I think that, that's an interesting thing that I think is worth talking about at some point. The ways in which practitioners come to our conferences, go out for drinks with us afterwards, we talk about these things, we exchange ideas. (oral history interview, April 14, 2023).

Similarly, during his oral history interview, Paul Schwartz would raise the name of another law firm partner with strong ties to PLSC. According to Schwartz, "Chris Wolf, just for many years, was the 'Dean of privacy practitioners,' as I would refer to him at conferences and events. He would come to academic events, and *bridge events, like the Privacy Law Scholars Conference, where lots of practitioners show up*" (P. M. Schwartz, oral history interview, March 29, 2023).

When it comes to other type of legal practitioners—policymakers and advocates, Andrew Selbst would similarly claim:

> it's been about 15 years since the privacy field was a thing. And for the first five so, the FTC was still talking about notice and choice, right? If you look back and like, you know, *the advocates were also coming to PLSC for those first five years, the public interest organizations*, right? *The government folks were coming*. And so, there's a direct conversation. Like *Julie Brill was there like a hundred times, before she left for Microsoft, when she was a Commissioner*, right? And she would have to defend the FTC, and we'd all be like, "what are you doing, right? Notice and choice makes no sense." And so, I think the conversation certainly, from an FTC perspective, changed how they thought about privacy, they sort of tried to give up on this. (oral history interview, October 26, 2023)

Thus, for Neil Richards, Paul Schwartz, and Andrew Selbst, legal practitioners coming from private practice, advocacy organizations, and public agencies could be considered as regular attendees of the conference. On the other hand, Julie Cohen seems to have a different vision, at least when it comes to the PLSC-policymakers relationship. When talking about other privacy conferences she would regularly attend, during her oral history interview Cohen stated: "PLSC is

definitely better than every single one of those things that I've just listed, because it is organized around the depth and the richness of the *academic* interchange. *If you want to talk to policymakers, it doesn't really have that much to offer*. CPDP in Brussels is by far the better thing to do" (oral history interview, February 27, 2023)

How can these differing visions be reconciled? Looking at what Paul Ohm would say on a related subject might help clarify this disparity of opinions. After being asked to talk about the relationship between advocates and privacy scholars, Ohm responded:

> *I think that answer has changed over time*. I think earlier in my career, one thing I'm, I was most proud of in Information Privacy Law was *the small divide between academics and practice.* And the extent to which we talked to one another and the extent to which we transmitted ideas to one another. And I made the claim repeatedly that there was more transfer than in almost any other legal field. And so, *your question is specifically about advocates, but I would say for all practitioners, they needed scholars and scholars needed practitioners more than in any other area of law.* And it was partly because we didn't have a lot of law and so, our theorizing and abstract organizing is exactly what they needed most. And then at the same time, we needed to know how our theories were being developed into laws. And so, I used to say that all the time. *It's less true today*. (…) (oral history interview, September 22, 2023)

Thus, when it comes to the practitioners' participation in PLSC, it seems like things have changed over time. Whereas in the beginning law firm members, policymakers, and advocates where active members of the PLSC community, as time passed their participation in the conference has decreased. In fact, this can be also traced in the evolution of PLSC's public documents. As stated in the conference's agendas since 2008 and up until 2020,

> the Privacy Law Scholars Conference (PLSC) assembles a wide array of privacy law scholars *and practitioners* from around the world to discuss current issues and *foster greater connections between academia and practice*. PLSC brings together privacy law scholars, privacy scholars from other disciplines (economics, philosophy, political science, computer science), *and practitioners (industry, legal, advocacy, and government)*" (*2020 Privacy Law Scholars Conference (PLSC 2020)*, n.d.).

However, since 2021 the phrasing included in the conference's call for abstracts has experienced slight changes year after year. According to the language of the 2024 Call for papers, "PLSC assembles a wide array of *privacy law scholars, policymakers, and practitioners who engage in scholarship.* Scholars from non-law disciplines (…) are critical participants in this interdisciplinary field" (*Call for Abstracts: Privacy Law Scholars Conference 2024*, n.d.). Likewise, this present state of affairs can also be seen in section 5 of the current PLSC Charter, "Participation in the PLSC." According to its language,

> [t]he PPC shall invite *practitioners and others* to participate *only after* taking into consideration *their commitment to academic values* of open-minded discussion and debate and their ability to contribute to the discussion independently of their employer's or organization's special interests. (*PLSC Charter – Privacy Law Scholars Conference*, n.d.).

Therefore, while scholars of non-law disciplines keep being a key component of the conference, policymakers and practitioners are now welcome *as long as* they engage in scholarship and commit to certain academic values.

***

Hence, based on the evidence collected for this research project—which main objective, as stated, was not to prove the existence of the principles examined, it can be concluded that, over the years, what has developed *around* PLSC is an *interdisciplinary* community of mostly *American scholars* (although joined by *some international participants* and a *decreasing number of practitioners*) with a *wide array of academic maturity levels*. But can this be considered a "community *of discourse*"?

## 2. A community of discourse

As reviewed in the Methodological Framework Section, David Hollinger (1985) points out that, for a community to be considered "of discourse," there should be an interaction between the minds of disputants who: (i) are essentially peers; (ii) are cognizant of each other's views; (iii) share a language and a national culture; (iv) share certain ideas, understood as values, beliefs, perceptions, and concepts; and (v) share questions. Finally, (vi) this interaction is usually carried on predominantly in verbal form.

As I hope to show in this Sub-Section, the community that has developed *around* PLSC clearly exhibits each one of these characteristics. Yet, before examining each of these elements, I would like to try to identify roughly the contours or boundaries of this community.

Interestingly, while the boundaries of the community that has developed *around* PLSC are hard to tell after 16 years of continuous growth, many of the scholars interviewed for this study would refer in passing to PLSC's "core people" (P. T. Kim, oral history interview, November 30, 2023; A. D. Selbst, oral history interview, October 26, 2023; Zarsky, oral history interview, November 22, 2022) or "inner circle" (W. Hartzog, oral history interview, February 27, 2023; P. Ohm, oral history interview, September 22, 2023). In fact, while Tal Zarsky would explicitly describe himself as "not at the core" (oral history interview, November 22, 2022), Ohm would situate himself as "part of the just inner circle from the beginning" (oral history interview, September 22, 2023).

When asked about what he meant by PLSC's "inner circle" and who, apart from himself, he would describe as being part of it, Ohm provided what he would describe as a "rough list" of people ("the almost original group") who, according to his recollection, (i) have been at PLSC from almost the beginning; and (ii) have been regulars (oral history interview, September 22,

2023). When combining this list with Neil Richards's proposed picture of "the field" (oral history interview, April 14, 2023), it became apparent that the alluded "inner circle" is itself composed of various (mostly) generational layers, much like an onion (**Figure 1**).

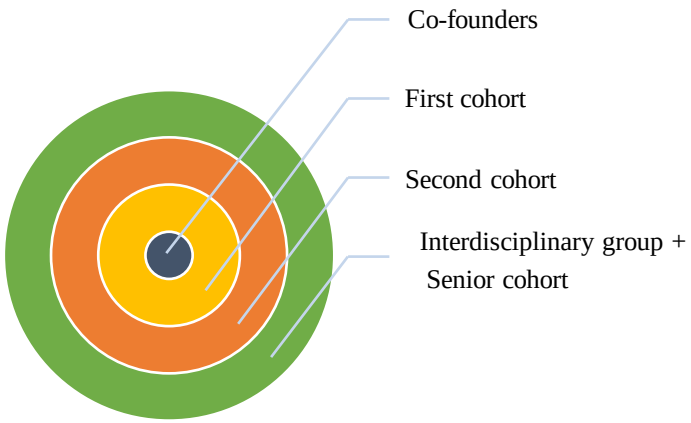


**Figure 1. Privacy's "inner circle"**

Accordingly, if Daniel Solove and Chris Jay Hoofnagle—as the conference's co-founders—are at the center, a first layer of members includes scholars such as Julie Cohen,[33] Neil Richards, Danielle Keats Citron, and Paul Ohm,[34] who were present since the beginning of the conference's foundation. A second, "slightly younger cohort" (Paul Ohm, oral history interview, September 22, 2023), in turn, consists of scholars who, according to Richards' account, were "a couple of years behind, it seemed like, I think we all had tenure when they started" (Neil Richards, oral history

[33] Instead of placing Julie Cohen here, though, Neil Richards would mention her as part of the "earlier wave" that will be described in the next page.
[34] By contrasting Paul Ohm and Neil Richards' s accounts, though, it is unclear whether Ohm should be placed as part of the first or second cohort. While in his quoted description of "the field" Richards mentions Ohm in the same batch as Ryan Calo, Woodrow Hartzog, and Margot Kaminski, in his own account Ohm refers to Richards and Citron as his "contemporaries." However, given that, in contrast to the rest of the scholars included in the second cohort, Ohm is the only one who workshopped a paper at the first PLSC (2008) (where Richards and Citron were also presenting papers), I have decided to include him as part of the first cohort.

interview, April 14, 2023). For this second cohort, the names of Woodrow Hartzog, Ari Waldman, Ryan Calo, Margot Kaminski, and Meg Leta Jones were offered as examples of its participants.

Based on Ohm's account, there is also a third layer—"the interdisciplinary group" (oral history interview, September 22, 2023), whose members includ, for example, non-legal scholars Helen Nissenbaum and Alessandro Acquisti. For his part, Richards would also mention an "earlier wave" of scholars, including Anita Allen, Paul Schwartz, Joel Reidenberg, and Julie Cohen as examples of its members. According to Richards, "they were out there, and then, when the field began to coalesce, *they became the immediate senior figures*, and they... And they, to be clear, they took that mantle on impeccably and spectacularly" (oral history interview, April 14, 2023).

To be sure, the names of the scholars mentioned here as examples for each layer do not represent the totality of scholars within each generational cohort. Also, the fact that PLSC's "inner circle" presumably follows an onion-type structure of generational cohorts does not imply that the full community of scholars that developed *around* PLSC is necessarily structured in this way. Yet, this categorization and the sample of names offered as examples allow me to evaluate the existence of the different elements present in a community of discourse.

### 1.1 Disputants are essentially peers

According to the different generational layers that compose PLSC's "inner circle" (**Figure 1**), it would seem from the outset that the members of the community that developed *around* PLSC are not all peers, in the sense that they are not on equal standing with one another. Rather, the implied generation-based structure of PLSC's "inner circle" appears at first sight to place its participants in a hierarchical structure based on various levels of seniority. In practice, however, this does not seem to be the case.

First, no matter the generational level they presumably pertain to, at countless times the narrators interviewed for this project would use the term “friend” to refer to scholars in apparent higher levels of seniority. Ari Waldman (a scholar mentioned as part of the younger cohort), for example, would refer to Julie Cohen, Danielle Keats Citron, and Neil Richards (scholars mentioned as part of the first cohort) as some of his “great best friends in the academy” (oral history interview, November 30, 2022). Similarly, Daniel Solove (one of PLSC’s co-founders) would refer to Paul Schwartz (a scholar mentioned as part of the senior cohort) as a person with whom he “became a very, very quick friend. And we've worked together for forever now” (oral history interview, February 26, 2023).

Furthermore, the mentorship dynamics that I identified between my list of interviewees and the sample of scholars offered as examples for each generational cohort (**Table 3**) suggest a more complex picture of interactions.

Evidently, many mentorship relationships in this community have followed the traditional the one-way arrow from more senior (mentors) to younger scholars (mentees). Anita Allen (a scholar named as part of the senior cohort), for example, was said to be a mentor to Daniel Solove (one of PLSC’s co-founders), while Paul Schwartz (a scholar mentioned as part of the senior cohort) was mentioned as a mentor by Solove, Neil Richards (a scholar mentioned as part of the first cohort), and Ari Waldman (a scholar mentioned as part of the younger cohort). Solove, in turn, was mentioned as a mentor by various of my interviewees who were classified by Ohm and/or Richards as part of the first or the younger cohort. Finally, all of the names included by Richards and/or Ohm as examples of the first cohort of scholars (Cohen, Richards, Citron, Ohm) were mentioned as mentors by both Woodrow Hartzog and Ari Waldman (scholars mentioned as part of the younger cohort).

Nonetheless, not all mentorship relationships within this community can be described as unidirectional and straightforward. According to the interviews, it is not uncommon for younger scholars to act as mentors for senior ones, or for scholars in the same cohort to mentor one another. Daniel Solove's description of his own situation rightly exemplifies the first possibility:

> there are people who, you know, got in early on, that were also great. You know, I was, *I kind of started out being a mentor to them. But then they really kind of, you know, got to a point where they were, kind of, bring as much advice to me as I brought to them.* And these are people like, you know, [Neil] Richards and Danielle [Citron], and Woodrow Hartzog, he definitely started out as to being a student, not in academia, you know. I was definitely trying to help him, but then it came a point where, you know, *he is someone who I go to for advice*. Chris Hoofnagle as well, who I early on started out with, and who's been tremendously influential. It's a lot of people who I owe a great debt of gratitude to." (D.J. Solove, oral history interview, February 26, 2023).

Thus, although having been in the field for a longer time and therefore being more senior than Richards and Citron (scholars mentioned as part of the first cohort), Solove would consider them as mentors. Similarly, despite having been one of the most important mentors in Hartzog's career[35] (a scholar mentioned as part of the younger cohort), Solove would still consider him as someone he goes to for advice.

An example of the second possibility (mentorship among members of the same cohort), in turn, could be identified in the oral history of Paul Ohm, who considers his cohort peers to be his mentors as well. In the case of Julie Cohen, for instance, Ohm would state: "Now, at this point, I'm so privileged that she's one of my closest friends and faculty colleagues. But *absolutely a role model I've been looking at my whole career*" (oral history interview, September 22, 2023). Similarly, when referring to Neil Richards and Danielle Keats Citron, he would contend: "even, like my contemporaries who just do things better than I do. So, Danielle [Citron], Neil [Richards],

[35] During his oral history interview, Woodrow Hartzog would refer to Daniel Solove in the following terms: "Dan really was an incredible teacher, and then ultimately became *an incredible mentor to me*" (oral history interview, February 27, 2023).

right? *I consider them more friends than mentors, but they mentor me in a way, as well*" (P. Ohm, oral history interview, September 22, 2023)

Among other factors, one of the possible reasons why these complex mentorship relationships developed is that, as some interviewees pointed out, there were not many information privacy mentors during the early years of the conference (and the field). To be sure, throughout the interviews narrators would refer to mentors from other areas of law or jurisdictions. For instance, scholars such as Julie Cohen, Michael Froomkin, and Chris Hoofnagle repeatedly mentioned Law & Technology scholar Pamela Samuelson as a mentor (A. M. Froomkin, oral history interview, September 21, 2023; C. J. Hoofnagle, oral history interview, September 8, 2023; J. E. Cohen, oral history interview, February 27, 2023). In the same way, Daniel Solove and Tal Zarsky[36] would mention Jack Balkin when discussing mentors during their interviews (D. J. Solove, oral history interview, February 26, 2023; T. Zarsky, oral history interview, November 22, 2022). Likewise, according to Paul Schwartz, one of his most influential mentors was the European jurist and pioneer of data protection, Spiros Simitis (P. M. Schwartz, oral history interview, March 29, 2023).

Yet, when asked about her mentors *within* the field, Priscilla Regan—whose career as a privacy scholar began in the early 1980s[37]—responded: "So, who were mentors? I mean, I guess… *We were all kind of figuring it out* at that point. You know, *there wasn't*…" (oral history interview, September 18, 2023). Furthermore, when explicitly referring to Alan Westin—another privacy scholar even more senior than her, she would contend: "So, Alan Westin had *Privacy and Freedom*. That probably, that was really important. Umm, so… And I knew Alan, you know, I knew him from the time I was at [the Office of Technology Assessment] OTA. *I never thought of*

[36] Tal Zarsky would also refer to Ruth Gavison and Eli Noam (T. Zarsky, oral history interview, November 22, 2022).
[37] Priscilla Regan was not explicitly included by Richards as an example of PLSC's "senior cohort." Yet, she was indeed mentioned by Chris Hoofnagle in his interview as an "early person" in the field (oral history interview, September 8, 2023).

*him as a mentor, though, I didn't know that kind of close relationship with them"* (oral history interview, September 18, 2023). Similarly, although Neil Richards would ultimately share his own list of mentors acquired at PLSC, when asked about mentorship relationships during his interview, Richards began his response by stating: "So, directly nobody from Law School, because *the field didn't exist*. (…) But I do think one of the interesting things about our field is *we didn't really have mentors*, at least this [cohort]..." (oral history interview, April 14, 2023).

Consequently, even though it is difficult to prove for certain, this initial relative lack of mentors within the field may have motivated the members of this community, particularly those in the earliest cohorts (seniors, co-founders, and first cohort scholars), to seek unusual mentorship arrangements, regardless of their level of seniority. Whatever the reason, the complex mentoring relationships examined here illustrate that, despite generational cohorts existing within this community, the interactions among the scholars who are part of them appear to be less hierarchical and more like a network of academic friends who treat each other as peers and share a sense of camaraderie.

| Generational cohort | Examples of scholars (1) | Mentioned as a MENTOR by the following interviewees: (2) | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Priscilla Regan | Paul Schwartz | Julie Cohen | Michael Froomkin | Pauline Kim | Daniel Solove | Chris Hoofnagle | Neil Richards | Paul Ohm | Woodrow Hartzog | Ari Waldman | Karen Levy | Andrew Selbst |
| **Senior cohort** | Anita Allen | | | | | | | | | | | | | |
| | Paul Schwartz | | --- | | | | | | | | | | | |
| | Joel Reidenberg | | | | | | | | | | | | | |
| **Founders** | Daniel Solove | | | | | | --- | | | | | | | |
| | Chris Hoofnagle | | | | | | | --- | | | | | | |
| **First cohort** | Julie Cohen | | | --- | | | | | | | | | | |
| | Neil Richards | | | | | | | | --- | | | | | |
| | Danielle Keats Citron | | | | | | | | | | | | | |
| | Paul Ohm | | | | | | | | | --- | | | | |
| **Second cohort** | Woodrow Hartzog | | | | | | | | | | --- | | | |
| | Ari Waldman | | | | | | | | | | | --- | | |
| | Ryan Calo | | | | | | | | | | | | | |
| | Margot Kaminski | | | | | | | | | | | | | |
| | Meg Leta Jones | | | | | | | | | | | | | |
| **Interdisciplinary group** | Helen Nissenbaum | | | | | | | | | | | | | |
| | Alessandro Acquisti | | | | | | | | | | | | | |

**Table 3. Mentorship dynamics identified between my list of interviewees and the list of scholars offered as examples of each generational cohort***

## Notes*

**(1)** According to a combination of Paul Ohm's and Neil Richards's recollection and proposed categorization of cohorts.

**(2)** Although interviewees for this project, Anita Allen and Tal Zarsky were not included in any of the columns, since during their oral history interviews they were explicitly not asked about mentors

### 1.2 Disputants are cognizant of each other's views

Having found that at least PLSC's described "inner circle" is composed by scholars who consider each other as peers, the time has come to explore whether its members—or, even better, all the members of the community of scholars that has developed *around* PLSC—are cognizant of each other's views (element (ii) of a community of discourse). Based on the information collected through the oral history interviews conducted for this study, there are at least two circumstances that would suggest that the scholars here studied have ample knowledge of one another's perspectives.

First, thanks to PLSC itself, the community of scholars that has developed *around* PLSC is in constant conversation. Thus, by annually gathering the community to workshop in-progress scholarship, the conference allows—at least—its regular attendees to get to know what many of the members are working on. In fact, while telling me about other scholars who have influenced his scholarship, Andrew Selbst would point out:

> *my scholarship is very much influenced by what everyone's done at PLSC*. It's really hard to like name specific influences, right? Uh, obviously my co-authors are big influences. But yeah, I mean *the people at PLSC*, again, the same people that have all like the big papers each year. (…). So, *have all influenced, not just my scholarship but my general way of thinking about the field, right? Like I'm exposed to their ideas constantly* (*laugh*). (A. D. Selbst, oral history interview, October 26, 2023)

Second, besides reading each other when preparing for the PLSC sessions, evidence from the interviews also shows how many of the scholars mentioned as examples of PLSC's "inner circle" constantly serve as "informal reviewers" or "interlocutors" to one another as well as to other scholars who joined the conference later (e.g., Karen Levy and Andrew Selbsts). As such, many of the interviewees in this study regularly reach out to them to discuss ideas or request feedback on drafts (**Table 4**).

Interviewees Daniel Solove, Chris Hoofnagle, Neil Richards, Tal Zarsky, and Ari Waldman, for example, included Paul Schwartz among their informal reviewers/interlocutors. In a similar fashion, all of them, plus Woodrow Hartzog, also recognized Daniel Solove as a person they reach out to for feedback or to discuss ideas. Julie Cohen, in turn, stands out as the scholar from the "first cohort" who—according to the consolidation of the interviews' data—is most sought by the interviewees of this study to review a draft or discuss ideas. Regarding the "second cohort," Woodrow Hartzog is seen as an informal reviewer/interlocutor by seven of the fifteen interviewees, while Ryan Calo is similarly seen as such by six of them.

More than a ranking of academics who help others, what these dynamics show is that even when not preparing for or at PLSC, scholars within this community—or at least those within PLSC's "inner circle"—are informally reviewing the work of others on a regular basis, and therefore, permanently getting to know what each other thinks about different topics related to privacy. On this point, the following quote from Woodrow Hartzog seems eloquent:

> So, basically, there is at least three different sets of people that we try to get to review our paper. One would be *the close circle of people that read everything I write*. That would be Dan Solove, Ryan Calo, Neil Richards, Julie Cohen, Ari Waldman, Margot Kaminski, Meg Jones, Paul Ohm, Bill [(William)] McGeveran. *These people that write, not only write in similar spaces, but have become kind of close friends over the years, and confidants, and people that I work with on a lot of different things*. And so, we know that all of us sort of collectively know that, if any of us have a draft we want to read, we'll read them. (…) the nice thing is, sometimes they'll give you the most pointed criticism because they don't have to worry about hurting your feelings (*laugh*) (W. Hartzog, oral history interview, February 27, 2023)

Thus, the community of scholars that has developed *around* PLSC seem to have forged diverse avenues through which their scholarship can be shared formally and informally with others, both on the occasion of PLSC and on a regular basis. In addition to providing scholars with feedback

and the opportunity to bounce ideas off of one another, these constant interactions allow scholars to be cognizant of each other's views.

### 1.3 Verbal interaction among disputants who share a language, a national culture, and ideas

The description of the community of scholars that has developed *around* PLSC provided in Section B.1. of this Chapter yields elements that allow us to confirm the existence of an interaction between the minds of disputants—Privacy law scholars—which meets the characteristics outlined in elements (iii), (iv) and (vi) of a community of discourse, namely: a predominantly verbal interaction and the sharing of a language, a national culture, and a set of ideas.

Given PLSC's nature as a *paper* workshop, the fact that the interaction between the minds of these scholars is usually carried on in verbal form (element (vi)) needs no further substantiation. In particular, it is through their written expression through which these scholars convey most of their scholarly work. Equally, it seems evident by now that the community that has developed *around* PLSC shares a language—English—and a national—American—culture (element (iii)). Thus, even if some of the participants of the conference are indeed international scholars, most of the discussions held at PLSC revolve around the American legal culture and system, and to a lesser extent, about the European Union.

Finally, taking into account Pauline Kim's critic to PLSC's tendency to gather fairly like-minded individuals in terms of normative goals, at this point it seems fair to assert a relative share of values, beliefs, perceptions, and concepts among the PLSC community (element (iv)). As mentioned earlier, this community mainly gathers scholars who agree on the value of privacy and

use their scholarship to emphasize its importance. In fact, while not as a criticism, Paul Ohm would confirm this tendency of the conference during his interview. According to him:

> [t]his is something that I bet someone has said to you: If you come to the Privacy Conference, *it's because you have a pro-privacy viewpoint, we're a very one-sided community*. And so, there's this other interesting cohort of people who have come a lot, but have always been more suspicious of privacy and for that reason, we don't consider them as core (*laugh*). And so, the three that immediately screened in mind at different eras *are Orin [Kerr], Lior Strahilevitz, and Jane Bambauer*, right? Like by other measures, they seem really central, but because they've always been so skeptical of privacy in certain spheres, we've never fully embraced them, right? (oral history interview, September 22, 2023)

Even though this lack of diversity of viewpoints may affect the rigor and richness of the discussions held at PLSC—as pointed out by Pauline Kim herself, in the context of this study it serves as an additional indication that a community of discourse has indeed developed *around* PLSC.

| Generational cohort | Examples of scholars (1) | Mentioned as an INFORMAL REVIEWER/ INTERLOCUTOR by the following interviewees: (2) | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Priscilla Regan | Paul Schwartz | Julie Cohen | Michael Froomkin | Pauline Kim | Daniel Solove | Chris Hoofnagle | Neil Richards | Paul Ohm | Tal Zarsky | Woodrow Hartzog | Ari Waldman | Karen Levy | Andrew Selbst |
| **Senior cohort** | Anita Allen | | | | | | | | | | | | | | |
| | Paul Schwartz | | --- | | | | | | | | | | | | |
| | Joel Reidenberg | | | | | | | | | | | | | | |
| **Co-founders** | Daniel Solove | | | | | | ----- | | | | | | | | |
| | Chris Hoofnagle | | | | | | | --- | | | | | | | |
| **First cohort** | Julie Cohen | | | --- | | | | | | | | | | | |
| | Neil Richards | | | | | | | | --- | | | | | | |
| | Danielle Keats Citron | | | | | | | | | | | | | | |
| | Paul Ohm | | | | | | | | | ---- | | | | | |
| **Second cohort** | Woodrow Hartzog | | | | | | | | | | | --- | | | |
| | Ari Waldman | | | | | | | | | | | | --- | | |
| | Ryan Calo | | | | | | | | | | | | | | |
| | Margot Kaminski | | | | | | | | | | | | | | |
| | Meg Leta Jones | | | | | | | | | | | | | | |
| **Interdisciplinary group** | Helen Nissenbaum | | | | | | | | | | | | | | |
| | Alessandro Acquisti | | | | | | | | | | | | | | |

**Table 4. Interlocution dynamics identified between my list of interviewees and the list of scholars offered as examples of each generational cohort***

**Notes***

**(1)** According to a combination of Paul Ohm's and Neil Richards's recollection and proposed categorization of cohorts.

**(2)** Although an interviewee for this project, Anita Allen was not included in any of the columns, since during her oral history interview she was not asked about informal reviewers/interlocutors.

### 1.4 Disputants share questions

In terms of the remaining element of a community of discourse—the degree to which the members of this community share questions (element (v)), the intellectual history advanced in the following four chapters (Chapters II through V) will in fact bring to the light how, over the last thirty years, American Privacy law scholars have been contributing to solving a consistent number and type of questions. As will be seen, the two main questions shared by the scholars here reviewed are: What are the harms that novel sociotechnical developments can cause? And, what legal tools, if any, can be used to prevent, address, or mitigate those harms?

Nonetheless, these scholars' specific discussions about the second question could also be said to revolve around more concrete questions regarding, among other topics, the effectiveness of the Fair Information Practices (FIPs) principles to hold data practices under control; the most appropriate way, if any, to implement notice and consent mechanisms; the rule making power of technology; the viability of going back to privacy's American origin—Tort law—to tackle the Digital Age's novel challenges; the role that the FTC should play in the Information Privacy law ecosystem; the effects of design both as a manipulative strategy and as a tool to protect privacy; the reach and limitations of anonymization as a privacy tool; the affordances that computer-science tools can provide for algorithmic accountability; the lessons that other areas of law, such as Intellectual Property or Fiduciary law, can teach Privacy law; and the actors (individuals themselves, corporations, or the government) who should be responsible for the protection of individuals—as well as social groups—from the data extraction economy.

***

As this review has indicated, the community of scholars that has developed *around* PLSC possesses the five elements necessary to constitute a "community of discourse." As such, its body

of intellectual work is suitable for a study of the discourse of intellectuals, such as that proposed by David Hollinger and described in this dissertation's Methodological Framework section.

### C. Relevance to the field

Before concluding this Chapter, I would like to briefly consider the relevance of PLSC to the field of Privacy law in America. When asked about her view of PLSC in relation to the field, during her oral history interview Karen Levy responded: "OK, it's a tough question. I mean, in some sense, I think... *I know they're not exactly the same, but PLSC stands in for the Privacy law field to me, in a lot of ways*" (oral history interview, November 17, 2023). In a similar fashion, when answering that same question Michael Froomkin commented: "I don't know, do I know the field of privacy, anymore? It's so big! *I don't have any reason to believe it's not representative, but I've never, but I've never looked*" (A. M. Froomkin, oral history interview, September 21, 2023).

Despite these considerations, which the interviewees themselves frame as based in perception more than in evidence, a more nuanced evaluation of this topic evidences that the field of Privacy law in America was not born with PLSC; and that the community that developed *around* this conference cannot be equated with the American Privacy law scholarship community at large, and even less so with the community that composes the American Privacy law field in general.

These realities, however, do not diminish the significance of the conference in the Privacy law field in America. As I expect to establish in this Sub-section, besides coalescing the field, PLSC has also provided its attendees the conditions to consider themselves as part of that field.

## 1. Differences with the field

As announced, PLSC did not create the field of privacy law in America. As Neil Richards recognized in his interview and was further developed in a previous Section, before the foundation of PLSC in 2008 there was already an "earlier wave" of scholars writing about privacy. And even earlier than these senior scholars, canonical work on privacy—briefly mentioned in the Introduction of this dissertation—had already been published by renown scholars in the field. As Priscilla Regan would point out, "Alan Westin had *Privacy and Freedom*. (…) there were those, the scholars who published books right before the Privacy Act was passed and kind of *The Data Bank Society*, you know, *The Assault on Privacy* by Arthur Miller. They were important in defining the field" (Priscilla Regan, oral history interview, September 18, 2023).

Similarly, evidence collected through the interviews has also made it clear that *nowadays* there is not a complete match between the community of scholars developed *around* PLSC and the American Privacy law scholarship community at large. First, as Neil Richards would simply state it during his interview, "there are people who write in Privacy law who don't attend PLSC," citing scholar Lori Andrews as an example (oral history interview, April 14, 2023).

Second, according to several interviewees' recollection (C. J. Hoofnagle, oral history interview, September 8, 2023; P. Ohm, oral history interview, September 22, 2023; A. D. Selbst, oral history interview, October 26, 2023), certain scholars who attended PLSC in its early years—such as Felix Wu, Orin Kerr, Peter Swire, and Eric Goldman—no longer join the annual gatherings. And yet, as Andrew Selbst would categorically claim with regards to Felix Wu, "I would absolutely consider him part of that community, right? So, I think, I think the community is broader than the people who go to the conference all the time at this point too" (oral history interview, October 26, 2023).

Third, as mentioned above, during their oral histories Pauline Kim and Paul Ohm both referred to a group of scholars within the American Privacy law scholarship community at large who, despite writing about privacy-related issues, hold a less positive view of privacy than the community of scholars that has developed *around* PLSC. As examples of this category, in his interview Paul Ohm would mention Orin Kerr, Lior Strahilevitz, and Jane Bambauer. But in addition to these names, this group of privacy critics is also composed of some scholars working on surveillance studies. According to Priscilla Regan,

> you've got privacy scholars, people who identify themselves as privacy scholars; and then you've got surveillance, OK? So, *David Lyon*, in particular, the group that's up in, you know, Canada at Queens University, it's also much more European, the definition of the issue is more surveillance and privacy, and the US it's more privacy. So, you have something that *Surveillance Studies people tend not to go to the Privacy Law Scholars Conference*. And there's some who, in the Privacy Law scholars group, who are in sort of both groups. So, Ryan [Calo] would be one, because he worked with Ian Kerr and others up in Canada; I was one, who was in both; Colin Bennett, also a Canadian scholar, we're kind of in both. But then you had, you know, privacy people in the [United] States who were not following, you know, surveillance…Who, *now I think it's more that they identify, you know, they recognize the value of looking at it as surveillance*. But, umm, you know, that I think is the key thing, *that difference between looking at it as privacy and then looking at it as surveillance. And surveillance is basically a broader concept than privacy*. (P. M. Regan, oral history interview, September 18, 2023)

As pointed out by Regan, surveillance studies scholars have adopted a broader approach to privacy-related issues. As an interdisciplinary field that "came to increased public and academic attention after the events of 9/11" (Marx, 2015, p. 734), surveillance studies grapple with "the nature, impact and effects of a fundamental social-ordering *process*" (Lyon et al., 2012, p. 1), namely, surveillance. Thus, by treating surveillance as a process, surveillance studies scholars place this social phenomenon "within a given domain of social, environmental, economic or political governance" which involves "a series of interlinked, distributed and distantiated institutions, systems, bureaucracies and social connections" (Lyon et al., 2012, p. 1). Against this

backdrop, they look to analyze "the local politics of surveillance," that is, how "numerous local contingencies pertaining to inter-institutional competition, local politics, specific fears/desires or even serendipity" (Lyon et al., 2012, p. 2) converge to make specific surveillance practices possible and appealing.

Having said that, more than this broader approach—which is indeed less common in privacy law scholarship, the key factor that dissociates surveillance studies scholars from the privacy law scholars here studied is their questioning about "the continued relevance of official privacy regimes or data protection provisions" (Lyon et al., 2012, p. 3). As detailly explained by one of the Canadian surveillance studies mentioned by Regan (David Lyon) and his co-authors (Kevin D. Haggerty and Kirstie Ball), "[a]lthough there is a wide spectrum of opinion on this topic [within surveillance studies], one can crudely break these down into those who have some faith in the existing privacy structures versus those who are more suspicious or critical" (Lyon et al., 2012, p. 3). Thus, while Colin Bennett and Regan herself are placed by Lyon and his co-authors in the first approach, "[a]t the other end of the continuum are those who tend to accentuate *the limitations of privacy as both a concept and a regime*. For them, proof of *the failure of privacy structures* is glaringly apparent in how a surveillance society has sprung up around us, notwithstanding a large and vibrant privacy bureaucracy" (Lyon et al., 2012, p. 3).

Finally, the community of scholars that has developed *around* PLSC cannot be equated either with the community that composes the American Privacy law field in general. As already mentioned, although some attorneys working at law firms with privacy practices, as well as policymakers, and advocates do attend the conference on a regular basis, American privacy practitioners at large are not generally covered by this community. In fact, when asked how he viewed the conference in relation to the field of privacy as a whole, Chris Hoofnagle—PLSC's co-

founder—categorically responded: “[i]t's VERY different. So, I mean, I'll set it up as opposed to the [International Association of Privacy Professionals] IAPP events, which are very much compliance focused. There's almost no compliance focus at PLSC. So, it's very different, yeah, very different, you know” (oral history interview, September 8, 2023). In a strikingly related way, in her interview Karen Levy would similarly point out:

> [PLSC] does stand in contrast to something like IAPP or something, right? Which is much more about kind of *compliance-oriented or like more technical*... You know, there are always papers every year that don't like... I evaluate papers to get into PLSC and *one of the things we often don't accept into the conference, because of limited space, is work that it's very kind of workman like or it's like, “here's the specifics of this clause.*” There's more interest, I think, in like a broader theoretical statement or kind of a connection to scholarship that is... how do I want to say this? *Beyond just practice*? So, that's one, right? (oral history interview, November 17, 2023)

As such, although—as seen in Section 2 of this Chapter—PLSC was initially designed to bring together a variety of stakeholders, it seems that nowadays the IAPP is better suited to meet the needs of privacy law practitioners interested in discussing compliance-related issues. As a result, many of the attendees to the IAPP gatherings could not be considered as part of the community that has developed *around* PLSC.

### 2. Contributions to the field

Despite these different mismatches between PLSC and the field of American Privacy law (which could be probably represented by a Venn diagram), the central role of PLSC within the field cannot be denied. First, although not having created the field, evidence from the oral history interviews shows how PLSC has significantly contributed to coalesce it. In addition, it has provided the conditions for its attendees to consider themselves as part of that field.

As mentioned earlier, when addressing the topic of mentorship, during their oral history interviews both Priscilla Regan and Neil Richards acknowledged the existence of scholars such as Alan Westin and Arthur Miller—in the case of Regan, and Paul Schwartz, Joel Reidenberg, Julie Cohen, an Anita Allen—in the case of Richards, who were writing about privacy way before PLSC. Interestingly, however, when referring to them, Regan and Richards would both describe these groups of scholars in opposition to the community of scholars that has developed *around* PLSC.

Unlike the PLSC scholars, Regan would say, Westin and Miller, "[t]hey kind of…*I don't think they became an active part of this sort of community that went on to sort of do scholarship in that area*. Umm, that may or may not be fair, but I think…" (oral history interview, September 18, 2023). Similarly, when referring to Allen, Schwartz, Reidenberg, and Cohen, Richards would argue: "I don't think *they were in conversation with each other*, though. That they were all writing about privacy, but *they didn't consider themselves part of a field, the same way that we do*" (oral history interview, April 14, 2023)**.** Consequently, although it is true that PLSC did not create the field, it seems to have provided a space where scholars writing about information privacy could come together to converse and grow into one body.

In addition, compared to the times of Westin and Miller, PLSC has in many ways provided the conditions for its attendees to consider themselves as part of the American Privacy law field. This, by giving them: (i) a space to increase the visibility of their scholarship; (ii) the opportunity to get to know about what's going on in a big portion of privacy scholarship; and (iii) what could be considered as an easy "mark of belonging."

Thus, PLSC has established itself as one of the most effective platforms for sharing in-progress scholarship. According to Neil Richards, this has resulted in it becoming a space that scholars join to ensure not only more citations, but also greater impact of their work. In Richards own words,

> (…) let me say for years, it's almost like, *if a paper doesn't happen at PLSC, it doesn't happen*, you know? I think *there are people who write in Privacy law who don't attend PLSC, whose work is cited less, whose work is read less, whose work has less influence*. (…) I think if they had come to PLSC and workshopped their papers, they would be (A) cited more, and (B), you know, considered within the core of privacy, in a way that, you know, I think other people are considered to be in that group." (oral history interview, April 14, 2023)

Besides allowing attending authors to expose their own scholarship, the conference has also proved to be an excellent venue for attendees to discover the latest research in the field. On this second point, during her interview Julie Cohen would forcefully describe PLSC as "(…) *THE place to have your finger on the pulse of what people are thinking about in the world of privacy scholarship*; there is no substitute for it" (J. E. Cohen, oral history interview, February 27, 2023).

Finally, it could also be said that, for many, attending to PLSC has become a mark of belonging to the field. An extreme version of this position could be found, for example, in Paul Ohm's account. According to him,

> Umm, I mean, if you're, *if you're in privacy, you're going to come to the conference some of the time, right?* If, if, *if there are scholars out there who claim to be privacy scholars and yet have never been to our conference, despite having many years, then I, then I don't know them, and I would be highly suspicious of their claim that they are privacy scholars, only because they are just not interacting with anyone in the field*. And I'm sure that what I just said is a gross overstatement, there... People will point out examples that I'm forgetting. But yeah, no, I think that's right. (oral history interview, September 22, 2023)

A more moderate version, in turn, can be seen in Anita Allen's oral history, where she considers the attendance at PLSC to be particularly important for junior scholars. In Allen's view,

PLSC is "(…) a very ambitious event and it has become a kind, for a lot of people, just to think *for younger scholars*, it's *a must-go-to annual event* now" (oral history interview, March 30, 2023).

Notably, as much as these three conditions may have benefited PLSC's attendees, it is also important to note how they may have also limited access to opportunities and status for those scholars who, for whatever reasons, have been unable to attend the conference, or have decided to either abstain from joining or step aside from the community of scholars that has developed *around* PLSC.

***

Several points have been made evident in this chapter. First, by tracing the origin and evolution of PLSC, this Chapter has demonstrated how the discussion format adopted by PLSC's founders has enabled it to flourish and be particularly valued by its participants. The invitation-only model with which PLSC was born, on the other hand, limited the conference's ability to expand the diversity of its pool of attendees. As a consequence, for its first eight years PLSC missed out on the opportunity to gain valuable insight from members of marginalized groups who did not have access to influential academic networks, as well as from less positive perspectives on privacy. Interestingly, this may explain the relative similarity of views—particularly in terms of normative goals—observed in the PLSC articles that will be discussed in Chapters IV and V.

Additionally, by reviewing PLSC's initial guiding principles, this Chapter also illustrated how the conference's founders were successful in creating an event that would annually bring together an interdisciplinary community of scholars with a wide range of academic maturity levels. As for the international character of PLSC envisioned by its founders, more efforts will probably have to be made to expand the conference beyond North America and Europe. In addition, it is also interesting to note the conscious path that the conference organizers have decided PLSC to

follow, from being a platform created to "foster greater connections between academia and practice" to being a space in which practitioners are welcome *as long as* they engage in scholarship.

In third place, the analysis of how the community of scholars that developed *around* PLSC lends itself to be considered a "community of discourse" not only supported the viability of the study of the discourse of intellectuals conducted in this dissertation, but also revealed interesting patterns regarding the structure of the community. Particularly, it showed that there appears to be an "inner circle" at PLSC, which consists of various (mostly) generational layers. Nevertheless, it also revealed that, rather than following a hierarchical structure between generations, this community has evolved as a network of academic friends who mentor and serve as informal reviewers/interlocutors for each other.

Finally, the role that PLSC has played in the broader field of American Privacy law—both as a coalescer and as a provider of conditions for its attendees to consider themselves part of that field—not only makes evident its relevance in the field, but also emphasizes the importance of the present dissertation. As mentioned in the Limitations section, the trends and patterns identified both in the intellectual history offered in Chapters II to V as well as in Chapter VI cannot be generalized to the whole privacy law scholarship or the American Privacy law field, in general. Yet, given PLSC's relevance to the field, the transformation that this community's scholarship has experienced (privacy's algorithmic turn) and the normative commitments that have driven its members over time (their evolving techno-legal imaginaries) should be of interest to the field as a whole.

With the provided background and these specific points in mind, we are now prepared to begin exploring the intellectual history of privacy's algorithmic turn, which will be covered in Chapters II to V.

## II. 1990-1999: Technology Revolutionary Times in Need of Regulatory Innovation

Having identified the community of scholars that has developed *around* PLSC as a "community of discourse," the time has come to tell its intellectual history. Or, more concretely, the intellectual history of the algorithmic turn experienced by the concept of information privacy used by this community. The purpose of this Chapter—as well as of the three that follow—is exactly that one.

Chapter II covers the first ten years of this intellectual history (1990-1999). As will be seen, between 1990 and 1999 American privacy law scholars witnessed the explosive combination of personal computers and the emerging commercial Internet, its increased use by the government, the healthcare sector, and workplace administrators, and the related growth of e-commerce and the data market. Additionally, during the last years of this decade scholars would also observe the sanction of the Health Insurance Portability and Accountability Act ("HIPAA") and the Children's Online Privacy Protection Act ("COPPA") by Congress, as well as the FTC's landmark enforcement action against GeoCities.

Against this backdrop, and echoing American society's expressed distrust in the aforementioned technologies and practices, during this decade scholars would call attention to the capacity of these technologies and practices to threaten individuals' autonomy and their ability to control their personal information. In response, scholars would consider a wide variety of regulatory tools. Many of them would call for the binding implementation of the Fair Information Practices (FIPs) principles, either through legislation or technological means. Other scholars, more skeptical about comprehensive solutions, would instead propose alternative scenario-specific interventions to protect information privacy, ranging from self-regulation to torts, and market-

based mechanisms. Thus, towards the end of the 20th century, American privacy law scholarship would seem united around the most important harms to be prevented, but uncertain as to the best tools for addressing them.

This Chapter proceeds as follows. The objective of Section A is to immerse the reader into the sociotechnical and techno-legal context of the 1990s, *as seen through the lens of the scholars here studied*. Therefore, details are provided about the most relevant information technologies and practices of the epoch—as seen by scholars, the societal attitudes that surrounded these technologies and practices, and the sparse but impactful ways in which the by-then current American legal system responded to them. Subsequently, in Section B I present the harms that scholars writing during these years considered most significant, along with the privacy tools they would offer between 1990 and 1999 to address them.

## A. Context

Although already established in the Research Methods section, it is important to note here that the context provided in this Section describes the information technologies and practices, societal attitudes, and legal systems of the 1990s as viewed *through the lens of the authors here reviewed*. Consequently, although the accounts here registered may sometimes be inaccurate or incomplete, or the scholars here cited believed things would occur but have not, my role in collecting and synthesizing their views has not been to correct or judge them.

Having said that, the purpose of this Section will be to place the reader in the technological, social, and legal context in which the privacy law scholars here reviewed were writing. By examining the main information technologies and practices of the 1990s, societal attitudes developed in response to them, and the legal frameworks that were in place and being discussed,

Section A provides a general overview of the multiple sociotechnical and techno-legal factors which may have influenced these scholars' thinking during the covered years.

## 1. Information technologies and practices

### 1.1. Personal computers and networks

According to American privacy law scholars writing between 1990 and 1999, at the dawn of the 1990s Americans were witnessing a dramatic evolution of information technology. First, the proliferation of personal computers, which had had its roots in the previous decade. Second, the explosive growth of comprehensive digital electronic networks, including the Internet and private service networks such as Prodigy, CompuServe, and America Online. Consequently, the 90s were characterized by a "rapidly growing network of computing and communication technologies" (Kang, 1998, p. 1193), commonly referred to as "cyberspace."

Since the mid-1950s, Americans had been following the use of information technology by the government and big corporations to create computerized databases (Nissenbaum, 1998). In that sense, as Kerry Kang would recognize it in 1998, "for the past three decades, many have warned about the privacy dangers posed specifically by the computer" (1998, p. 1199). Even up until 1992, scholars kept discussing the increasing capacity of computers—usually held by governments or big corporations—to gather, store, and process personal information (Bezanson, 1992; Kreimer, 1991; Reidenberg, 1992; Schwartz, 1992). They were also concerned about the practice of data matching, understood as "the electronic comparison of two or more sets of records to find individuals included in more than one data base" (Schwartz, 1992, p. 1340).

Nevertheless, the transition from mainframe computers to personal computers, and even more importantly, the "shift from the use of 'stand-alone' computers to networked systems, integrating

hundreds of terminals" (Rodriguez, 1998, p. 1440) throughout the 90's were considered by scholars as real game changers. As of 1994, more and more scholars began to use the word "cyberspace"—originally introduced by William Gibson (1984)—to refer to "electronic communications over computer networks" (Hardy, 1994, p. 994), "the electronic environment through which the computer literati engage interactively" (Branscomb, 1995, p. 1639), "the virtual world" (Reidenberg, 1996, p. 556), "the web of consumer electronics, computers, and communication networks that interconnects the world" (Kang, 1998, p. 1195), or "the environment created for communication and other activities through interconnected computers" (Schwartz, 1999, p. 1617).

The spread of personal computers gave both individuals and small, private organizations access to "sophisticated information-processing capabilities through inexpensive equipment" (Reidenberg & Gamet-Pol, 1995, p. 111). On top of that, several changes came along with the emergence of cyberspace. As summarized by Joel Reidenberg & Franqoise Gamet-Pol, the fact that information could flow on expanding networks—also known as the Internet,[38] the Information Superhighway,[39] or the Global Information Infrastructure ("GII")[40]—allowed "decentralized information processing, multiple uses of information, and cross-sectoral uses," as well as "real-

[38] For proper definitions of the Internet proposed at the time *see* the work of Trotter Hardy ("a collection of computer networks that are 'interconnected' with one another such that electronic mail and other text can be sent and received among them" (1994, pp. 996, footnote 5)); George P Long II ("the forerunner to the proposed 'information superhighway,' a national information infrastructure that will combine communications networks, computer databases, and consumer electronics" (1994, p. 1178)); Michael Froomkin ("computer-aided communications over distributed networks" (Froomkin, 1996a, p. 398)); and Paul Schwartz ("the worldwide collection of computer networks and gateways that utilizes TCP/IP, a specific set of software protocols for communication. Put more simply, the Internet is a network of linked computers including all the millions of personal computers that are connected to it" (Schwartz, 1999, p. 1618)).

[39] Defined by George P. Long II as "a national information infrastructure that will combine communications networks, computer databases, and consumer electronics" (1994, p. 1178).

[40] According to Jerry Kang, "[t]he GII, like all information infrastructures, moves information from sender to receiver through some medium. In cyberspace, information typically moves through a hybrid of wireline and wireless pathways" (1998, p. 1220).

time access to data and information services across borders" (Reidenberg & Gamet-Pol, 1995, p. 107). Likewise, thanks to the electronically networked interactions enabled by the Internet,

> more data than ever before *is made available in digital format*, which is significant because digital information is easier and less expensive than nondigital data to access, manipulate, and store, especially from disparate, geographically distant locations. Also *more data is generated in the first place* because of the ease of doing so, the very low cost, and the high value of data in an increasingly information-based society. (Cate, 1999, p. 178)

In that sense—as Lawrence Lessig would stress, unlike real space, the architecture of cyberspace allowed data to be "collected ceaselessly-invisibly, behind the scenes, efficiently, with no burden on the user" (1999a, p. 62). As a result, permanent, malleable, and transportable records —including so called "public information"—began to be systematized in vast banks of digital information and harvested through the use of a number of emerging techniques (Nissenbaum, 1998). According to Helen Nissenbaum,

> [a]t the heart of contemporary data harvesting is the activity known variously as "profiling", "matching"[,] "data aggregation[,]" and "data mining" in which disparate records, diverse sources of information about people, are aggregated to produce databases with complex patterns of information. (1998, p. 586)

Although still in their infancy at the moment, these emerging techniques identified by Nissenbaum would become widespread in American society (and around the world) over the next twenty years.

### 1.2. Related practices

Against this framework—which several scholars at the time named with the terms "information society" or "computer age"—the attention of the privacy law scholars reviewed in this project was captured by the following five practices: (i) the use of computer networks by governmental

bureaucratic structures that processed personal information, (ii) electronic monitoring in the workplace, (iii) an increasingly computerized and technologized healthcare system, (iv) a flourishing personal data market, and (v) the development of e-commence. Although other practices may have also popped up in the literature of these years, these were the codes related to the "practices" category that repeated the most during the open coding round conducted for this study.

### 1.1.1. The use of computer networks by governmental bureaucratic structures

According to Paul Schwartz (1992), although processing of information within governmental bureaucratic structures dates back to the industrial revolution, the emergence of computer networks in the 1990's heightened the reach and impact of such bureaucratic processing of data. In Schwartz's own words, "[t]he present historical moment, however, marks the Internet's extension and perfection of the established data processing model" (1999, p. 1643).

By 1995, Laura B. Pincus & Clayton Trotte reported that "[t]he various agencies within the government can now match their information regarding any one individual with the information of another agency and complete an entire information check on individual citizens" (1995, p. 52). Similarly, in 1996 Michael Froomkin (1996a) would describe how public databases were more and more becoming interlinked and how the distinction between "public" and "private" data was disappearing.

Finally, according to Helen Nissenbaum, "[t]he computerization of public records has made them available with far less effort, either directly from respective government agencies responsible for collecting them, or from intermediaries who have gathered and organized them" (1998, p. 577). Thus, in addition to the enhanced capabilities to process and share information highlighted by her

contemporaries, computerization and advanced networking capabilities also made public records more accessible to the public.

### 1.1.2. Electronic monitoring in the workplace

Thanks to the capabilities offered by computers and to "the pervasive use of electronic mail (E-mail) by private sector companies" (White, 1997, p. 1079), employers started to electronically monitor[41] and surveille[42] employees' behavior in the workplace. According to American privacy law scholars writing about this practice at the time, methods of electronic monitoring would include "monitoring all oral communications by employees, tracking every employee movement in the workplace, searching employee computer files, and reviewing employee electronic mail (e-mail) and voice mail" (Flanagan, 1994, p. 1256). In the view of these scholars, despite its long history, the collection of data at work had become more pervasive due to its electronic characteristics. For Robert G. Boehmer, for example,

> [m]onitoring and surveillance techniques are potentially more intrusive today, even though they may be physically less intrusive in many respects. Today, the intensity of monitoring is extremely high, even continuous, and can more easily be hidden. Furthermore, it is difficult, if not impossible, for an employee who does not have access to the technology or records of its operation to refute the results. Finally, there is greater capacity to retain and retrieve records of the monitoring and surveillance through the use of computers. (1992, p. 813)

Similarly, Paul Schwartz would note how "with computers, they can combine this information, analyze it exhaustively, and produce a composite picture of an employee's abilities, value to the

[41] According to Robert G. Boehmer, "[i]n the workplace, the term 'monitor' generally connotes observation undertaken to determine whether an employee is completing an assigned function in an appropriate manner" (1992, p. 749).

[42] According to Robert G. Boehmer, "[t]he term 'surveillance' generally connotes observation to determine employee behaviors and personal characteristics, such as whether an employee violated a work rule" (1992, p. 749). Similarly, according to Frank J. Cavico, "'surveillance' means employer-controlled observation of employees to ascertain employee performance, behavior, and characteristics" (1993, p. 1284).

company, and unique personal characteristics. The computer has revolutionized the personnel office" (1992, p. 135). Interestingly, scholars' concerns about these exact same practices would persist until the end of the 30-year studied period, with only slight changes in terms of the technology capabilities deemed problematic.

### 1.1.3. An increasingly computerized and technologized healthcare system

According to the scholars, computers also made it possible to use personal healthcare information in many stages of the administration of the health care system (Schwartz, 1999), thus creating a desire for a national healthcare information infrastructure. As explained by Lawrence O. Gostin, by 1995 "most individual health records [were] kept manually in voluminous paper files" (1995, p. 457). However, "*[p]lans* for the systematic collection, storage, use, and dissemination of a huge volume of uniform data sets in electronic form *are already under way* and *have an aura of inevitability*" (Gostin, 1995, p. 452). Four years later, Jerry Berman & Deirdre Mulligan would indeed report:

> [h]ospitals, their affiliated clinics, and physicians are using intranets to enable the sharing of patient, clinical, financial, and administrative data. Built on Internet technologies and protocols, the private networks link the hospital's information system, to pharmacy and laboratory systems, transcription systems, doctor and clinic offices and others. The United States government is contemplating the development of a *federal government-wide computer-based patient record system.* According to news reports, the Internet and World Wide Web-based interfaces are under consideration. *The private sector is moving to integrate network computing into a sensitive area of our lives, the doctor's office*. (1999, p. 567)

As these past two quotes about record systems evidence, it is notable to observe how, during these years, some scholars would describe the technological state of affairs by alternating between facts and organization's plans/aspirations about what *could be* eventually possible with existing technologies. In some cases, the mentioned plans and aspirations might even be accompanied by

deterministic framings, such as that previously offered by Gostin ("plans (…) are already under way and *have an aura of inevitability*" (Gostin, 1995, p. 452)).

Along addressing these expanding record systems, scholars would also highlight how the healthcare environment was also impacted during this period by significant technological advances in the field of genetic testing. In October of 1990 the Human Genome Project was launched. This project, led by an international group of researchers, aimed to sequence the entire genome of a selected number of organisms (*The Human Genome Project*, n.d.). Referring to it, in 1999 Lawrence O. Gostin & James G. Hodge Jr. stated: "As the Human Genome Project maps the human genome, genetic information will increasingly come to be an integral part of the corpus of health data" (1999, p. 22). However, American privacy law scholars had described the future of genetic data as promising even earlier. According to Epstein's 1994 article, "[i]n the case of Huntington's disease, genetic testing accurately predicts the future onset of the invariably lethal disease and offers strong clues as to its severity and time of onset. *Technology has given us the ability* to see written in the future what, up to now, has been left to pure chance" (1994, p. 2).

### 1.1.4. A flourishing personal data market

A fourth practice of this period that also captured the attention of several American privacy law scholars was the flourishing of a personal data market. In 1994, the direct marketing industry, which relies heavily on gathering massive amounts of personal data, contributed $350 billion to the American economy (Reidenberg, 1995). By 1995, credit bureaus—being Equifax, Trans Union, and TRW the three largest at the time—were "the principal private-sector collectors, managers, and sellers of consumer information" (Shorr, 1995, p. 1760). Same as direct marketers, "credit bureaus [bought] information from the Census Bureau, state motor vehicle agencies,

insurance companies, magazine subscription services, telephone book publishers, and roughly sixty other sources" (Shorr, 1995, p. 1761). And computers turned out to be of great way to do it efficiently.

However, as electronically networked interactions began to happen, and traces of people's activities were directly recorded into electronic databases, direct marketers and credit bureaus were joined by other "second-order purveyors of information" (Nissenbaum, 1998, p. 563), such as mailing list brokers and ad-supported cybermediaries,[43] who also collected and processed personal information for profiling. As a result, by the end of the 20th century Paul Schwartz would report how "personal information itself has been increasingly commodified during the last decades. In the private sector, a flourishing trade exists in selling personal data for profit" (1999, p. 1642).

### 1.1.5. The e-commerce development

Finally, there was the development of e-commence. According to Fred H. Cate,

> [m]uch of the Web's explosive growth is due to the rapid increase in businesses online. In 1995, World Wide Web hosts designated ".com" for commercial uses slightly outnumbered those designated ".edu" for educational institutions, which were the historical backbone of the Internet. By January 1998, ".com" sites outnumbered their ".edu" counterparts more than two-to-one. (1999, p. 17)

The rapid growth of businesses online was of special interest to American privacy law scholars due to the tracking capabilities that were developed around them, thanks to technologies such as the "cookies," which "enable Web sites to surreptitiously collect information about your online activities and store it for future use" (Berman & Mulligan, 1999, p. 559). As in the case of Gostin,

[43] According to Ai-Mei Chang, P.K. Kannan, and Andrew B. Whinston, "[i]n early 1996 there were only two ad-supported cybermediaries offering freebies on the World Wide Web, but now there are more than a hundred vying for users' attention. Many cybermediaries that offer freebies have recently become the focus of acquisitions" (Chang et al., 1999, p. 85).

and Berman & Mulligan noted earlier, when referring to these capabilities Michael Froomkin would also notably alternate between facts and predictions of what these tracking technologies could do in the future—and in effect do now. Writing in 1996, Froomkin would stress:

> *Tomorrow*, rather than the FBI attempting to profile the reading habits of a small number of people with suspected foreign connections, *businesses will be profiling everyone who uses the World Wide Web*.
> Even today, it is relatively simple to monitor web page accesses whether or not the person reading a page initiates a commercial transaction. Most Web browsing software is designed to allow routine monitoring. (1996a, pp. 486–487)

Finally, and also referring to the Internet's tracking capabilities, by 1998 Jerry Kang would describe the by-then current online situation with the following metaphor, which became highly popular among scholars:[44]

> As soon as you enter the cyber-mall's domain, the mall begins to track you through invisible scanners focused on your bar code. It automatically records which stores you visit, which windows you browse, in which order, and for how long. The specific stores collect even more detailed data when you enter their domain. (1998, p. 1198)

Curiously, in the years to come, these online tracking dynamics would in fact replicate in actual malls and other physical locations, such as supermarkets, via in-store tracking technologies (Gupta, 2021).

### 1.1.6. Other less significant practices

Besides these five practices, there were two other networked computer-based practices that, although much less coded in the reviewed literature, also drew the attention of a few American

[44] Lawrence Lessig, for example, would use it in his 1999 article *The Law of the Horse: What Cyberlaw Might Teach* (1999b, p. 505).

privacy law scholars during the studied period, namely: plans for the development of "intelligent transportation systems" ("ITS") and the emergence of a copyright management industry.

As Michael Froomkin reported in 1996, "[m]any countries, including the United States, are exploring the possibility of 'intelligent transportation systems' (ITS). Under ITS, the position of every vehicle on the road would be monitored to manage traffic flow, prevent speeding and perhaps implement road pricing and even centralized traffic control" (1996a, p. 485). These systems, also referred to as Intelligent Vehicle Highway Systems ("IVHS"), called the attention of privacy law scholars due to their capacity to collect "information on where travelers go, the routes they use, and when they travel" (IVHS AMERICA Legal Issues Committee, n.d., p. 2), which made them worthy of the "panoptic technologies" title (Van Den Hoven, 1997, p. 33).[45]

In that context, in 1995 the Santa Clara High Technology Law Journal organized a symposium and published a special issue on IVHS. According to one of the authors who contributed to the symposium,

> Here it is of great importance that a fully developed IVHS will not exist in an informational vacuum. IVHS's information will exist alongside that provided by *other developments already in existence and likely to grow*, such as computerization of census and IRS information, computer records of people's credit-card purchases, their bank transactions, their credit histories generally, their telephone calls, their medical conditions, their education and employment histories, and of course the records of their brushes with the law, even of arrests that end in acquittal. Add to this the so-called "information highway" *on which we will all soon be riding*, with its automatic recording of all interactions, not to mention *the FBI's desire* to keep it eternally wiretappable. (Reiman, 1995, p. 33)

[45] Referring to Oscar H. Gandy Jr.'s 1993 book *The Panoptic Sort: A Political Economy of Personal Information* (Gandy Jr, 2021).

Like some of his contemporaries here highlighted, in this account of the IVHS technologies Reiman would also interestingly move back and forth between facts, predictions, and organizations' aspirations.

Regarding the emergent copyright management industry, in 1996 Julie Cohen raised the issue of "the various copyright management technologies that are being developed to enable copyright owners to monitor readers' activities in cyberspace" (1996, p. 2). Through these technologies, Cohen would argue, complex data mining techniques were starting to be applied to monitor individual reading habits for "copyright management" purposes. As will be seen in the next Chapter, between 2000 and 2007 several other scholars would join Cohen in focusing their attention on this emerging industry.

## 2. Societal attitudes

According to the scholars' accounts, these sociotechnical practices were initially received by American public with distrust. As reported by Joel Reidenberg in 1992, the *Equifax-Harris Report on Consumers in the Information Age* had found that by 1990, Americans were already more distrustful of industry than government with respect to the collection and use of personal information (Louis HARRIS Assocs. & Westin, 1990) (Reidenberg, 1992). In fact, the public rejection to Lotus Development Corporation's and Equifax Inc.'s 1990 attempt to sell CD-ROM disks that contained actual and inferred personal information of 80 million householders was considered by some American privacy law scholars (Froomkin, 1996a; Nissenbaum, 1997) as clear evidence of that wariness.

The sentiment of caution persisted over time. According to Helen Nissenbaum, "in June 1994, when ABC's Nightline anchor Ted Koppel conducted a poll, 73% of respondents said they

viewed the sale of records to mail-order companies to be an invasion of privacy" (1997, p. 212). Likewise, but citing his own national public-opinion survey (Louis HARRIS Assocs. & Westin, 1995), in 1996 Alan Westin would report:

> Eighty-two percent of the American public said in 1995 they are "concerned today about threats to their personal privacy." This is up from thirty-four percent in 1970, sixty-four percent in 1978, and seventy-nine percent in 1990.
> In the broad area of consumer privacy, eighty percent of Americans say that "consumers have lost all control over how personal information about them is circulated and used by companies." This is up from seventy-one percent who felt that way in 1990. Consumers say they are resisting intrusive information collection wherever possible. Fifty-nine percent report that they have "refused to give information to a business or company because [they] thought it was not really needed or was too personal," up from forty-two percent in 1990. (1996, p. 272)

In Westin's own words, these views were "closely correlated with and basically driven by two factors—strong majority distrust of public and private institutions and fears of technology abuse" (Westin, 1996). Notably, Westin's selection of factors is interesting in that they were already present in 1996, when commercial Internet's widespread adoption was still in its infancy.

For Anita Allen, writing in 1999, "[t]he popularity of anonymous and encrypted communication on the Internet [during the 90's] could be evidence that technology has not worn away the taste for privacy" (1999a, p. 733). Similarly, the availability of a variety of products and services designed to provide anonymous surfing and to prevent meaningful tracking of browsing behavior was also cited by Scott Killingsworth (1999) as evidence of the existence of user privacy concerns. In fact, as early as 1994 George P. Long II would have already reported how "the anonymous exchanging of information ha[d recently] become available on a widespread basis" (1994).

At the sunset of the twentieth century, scholars like Joel Reidenberg (1999) and Jerry Berman & Deirdre Mulligan (1999) would still raise the fact that numerous polls and surveys, such

as the Harris Poll conducted by Business Week (1998, p. 102), revealed how "the lack of privacy protections is a major barrier to consumer participation in electronic commerce" (Berman & Mulligan, 1999, p. 553). Nevertheless, during those final years of the 1990s, American privacy law scholars also began to comment on how concerns about privacy had started to fade. In 1999, for instance, Jeff Sovern (1999) claimed that, despite finding it objectionable that businesses routinely sell their personal information, most consumers would not opt out of this trade. Similarly, that same year Anita Allen pointed out:

> The final decades of the twentieth century could be remembered for the rapid erosion of expectations of personal privacy and of the taste for personal privacy in the United States. Recent polling data as well as high profile litigation and policy debates suggest impressively high levels of concern about physical and informational privacy. *Certain legal and policy trends; certain modes of market, consumer, and political behavior; and certain dimensions of popular culture, though, suggest low levels of concern*. (1999a, p. 729)

Looking to explain this phenomenon, Allen would attribute this contradiction to an avalanche of three different factors: (i) the emergence of technologies that facilitate individuals' exposure, allow the government to monitor them, and allow corporations to gather and exchange their personal information; (ii) opportunities to earn money and fame by writing books, selling personal information to publishers, and appearing on sensational television programs designed to expose people's private lives; and (iii) opportunities to consume other people's privacy through magazines, tabloids, or the Internet (Allen, 1999a). As examples of the latter, she would cite the JenniCam and SaraCam projects, which had been launched in the past few years to peep into the bedroom lives of young women (Allen, 1999a).

## 3. Legal system

As American privacy law scholars would report during this studied period, a few federal privacy laws had already been passed in the U.S. by the time the 1990s began. In 1970 Congress had approved the Fair Credit Reporting Act, which protects information collected by credit bureaus, medical information companies, tenant screening services, and other consumer reporting agencies. In 1974, in turn, federal legislators passed the Privacy Protection Act, which was later amended in 1988 by the Computer Matching and Privacy Protection Act, "because the Privacy Act provided little protection to individuals who were subject to data matching" (Schwartz, 1995, p. 588). Likewise, in 1988 Congress also approved the Video Privacy Protection Act. And in the early 1990s, the Drivers' Privacy Protection Act was passed to protect the records in possession of the State Departments of Motor.

Other than this patchwork-type framework, which scholars would constantly refer to and criticize, as the 1990s dawned "[t]he American legal system d[id] not contain a comprehensive set of privacy rights or principles that collectively address[ed] the acquisition, storage, transmission, use and disclosure of personal information within the business community" (Reidenberg, 1992, p. 208). And over the course of the decade, this situation would not change. Rather, self-regulatory efforts would increase, while concrete regulatory and enforcement initiatives would only become reality by the end of the twentieth century.

### 3.1 A multilayered and sectoral regulatory framework

Through the entire decade, many American privacy scholars would highlight—and several times criticize—the fact that the existing privacy rules in America were contained in a multilayered

regulatory framework, and that they had been developed on an ad hoc, targeted manner. As early as 1992, Joel Reidenberg would contend that

> [i]n the United States, however, no single source of privacy rights covers each data processing activity. Information privacy rights emerge from a complex web of federal and state laws that have responded to narrowly identified problems, while industry practices afford some additional non-legal protection. (1992, p. 201)

Later on, in 1996, Alan Westin would point out:

> the U.S. approach to privacy remains a more eclectic blend of constitutional interpretation, pin-pointed and sector-specific legislation, sector-based administrative agency rules, common-law judicial interpretation, labor-management bargaining (where employees are union-represented), voluntary organizational policies, and market-based dynamics. (1996, pp. 282–283)

And towards the end of the decade, Lawrence Lessig would describe a very similar panorama, stating:

> We have no general federal statute protecting privacy, whether informational privacy or data privacy. We don't even have federal statutes effectively protecting medical privacy-the only group with that sort of protection is individuals in drug rehab clinics. Instead, where we have responded with laws, the laws are limited to particular problems or contexts. (1999a, p. 62)

Besides the fact that this situation seemed immutable despite the passing of the years, it is also remarkable to see how, if the late Joel Reidenberg, the late Alan Westin, or Lawrence Lessig were to report on the current state of affairs today, their description would be very similar even 25 years later.

Interestingly enough, time and again scholars (Lessig, 1999a; Nissenbaum, 1998; Reidenberg, 1999) would also cite the passage of the Video Privacy Protection Act and the Drivers' Privacy Protection Act as examples of the reactive tendency of the American approach to privacy legislation. They would narrate how Congress responded with the former Act after a national

newspaper published the video rental records of Robert Bork, who had been nominated as Associate Justice for the Supreme Court. Likewise, they would describe how public indignation stirred by the murder of actress Rebecca Shaefer led to passage of the Drivers' Privacy Protection Act, after it was revealed that her murderer had traced her whereabouts through drivers' records.

Likewise, American privacy law scholars writing during the 90's (Cate, 1999; Lessig, 1999a; Nissenbaum, 1998; Pincus & Trotter, 1995; Reidenberg, 1995, 1999; Reidenberg & Gamet-Pol, 1995; Schwartz, 1995; Swire, 1998) would repeatedly contrast the sectoral thinking approach of the United States with the omnibus perspective adopted in the European Union. Inspired by the Organization for Economic Cooperation and Development's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data issued in 1980, in 1981 the Council of Europe adopted the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. And, at the beginning of the 1990's, the Commission of the EU proposed to member states a Directive on Data Protection, which was definitely adopted in 1995 and entered into force in 1998.

Although lamenting the dispersion of standards and the significant gaps in the protection of American citizens' privacy, scholars would not necessarily endorse the extension of the EU Data Protection Directive to the U.S. According to Peter P. Swire (1998), for example, the Directive was not prepared to address the special problems arising from the Internet, due to the timing of its discussion and entry into force. Similarly, Fred H. Cate would acknowledge the differences between the American and the European contexts that would impede such a legal transplant. In Cate's words,

> in the United States, however, the government is constitutionally prohibited under the First Amendment from interfering with the flow of information, except in the most compelling circumstances. The EU data protection directive is plainly contrary to that constitutional maxim, and the suggestion that the directive should be extended to the

> United States exacerbates that conflict, as well as threatens U.S. leadership in information technologies and services. (1999, p. 179)

In fact, among American privacy law scholars there was awareness of the particular circumstances of the American context that had prevented the development of a comprehensive approach to privacy. As Joel Reidenberg briefly summarized it in 1992, "[t]his mosaic approach derives from the traditional American fear of government intervention in private activities and the reluctance to broadly regulate industry" (1992, p. 209). This fear, which he would later describe as "a strong antistatist element" (Reidenberg, 1995, p. 501), was also similarly recognized by Paul Schwartz, who in 1995 would point out:

> In the United States, an ambivalence about government has meant skepticism about finding ways for it to empower people. The desire for a minimalistic state offers a reason not to regulate. As a result, in the context of data protection, individual self-determination often is seen simply as a pre-existing quality whose protection merely requires an absence of state power. (1995, p. 616)

In addition, some scholars would also cite the constitutional emphasis on protecting citizens against the government, but not on protecting them directly from each other, as another reason for the minimal restrictions on the treatment of information by private entities (Reidenberg, 1995). And, last but not least, scholars would also highlight the Clinton Administration's view of the role of the Internet law of privacy as "facilitating wealth-creating transmissions of information, including those of personal data" (Schwartz, 1999, p. 1611), as a possible cause of the government's inaction in the face of the privacy challenges posed by the Internet.

### 3.2 Companies' and industry groups' prevailing self-regulatory efforts

Probably due to this patchwork-type model, as the 1990's decade progressed scholars would register how the promotion of self-regulatory codes or guidelines by companies and industry

groups prevailed. As reported by Peter P. Swire in 1997, "[a] significant element of current thinking about privacy, however, stresses 'self-regulation' rather than market or government mechanisms for protecting personal information" (1997, p. 1). During the 90's, scholars (Berman & Mulligan, 1999; Reidenberg, 1999) would recurrently cite third-party privacy "seal" programs such as TRUSTe, the Better Business Bureau's Online Privacy Program ("BBBOnLine"), and the Online Privacy Alliance ("OPA") as evidence of these self-regulatory tendencies. Alluding to these initiatives, in 1999 Scott Killingsworth commented:

> For over four years the FTC has consistently encouraged industry self-regulation efforts such as these seal programs, which promise such benefits to the government as avoidance of the First Amendment issues that arise when the government attempts to control the flow of information, and conservation of limited government enforcement resources. (1999, p. 67)

As will be seen, in the coming years scholars would begin to report how the FTC requirements to industry would increasingly reflect a more hands-on approach.

### 3.3 Concrete but impactful regulatory actions

By the end of the decade, scholars would also highlight emerging public-sector initiatives that evidenced "rising political appetite for privacy protection" (Dreyfuss, 1999, p. 3). According to Fred H. Cate's 1999 article *The Changing Face of Privacy Protections in the European Union and the United States*—which might have been likely written in 2024 in relation to the past legislative sessions,

> *"Privacy" is the new hot topic in Washington* and other national and state capitals as we head into the new millennium. The debate over privacy is reaching a fevered pitch as policymakers, public interest advocates, and industry leaders clash over how much is enough and over what role the government should play in protecting it. The U.S. Congress, after decades of virtually ignoring privacy issues, considered almost 1000 bills—one out of eight bills introduced-addressing some aspect of privacy in its 104th session [(1995-1997)]. The 105th Congress [(1997-1999)] debated an even broader

> array of privacy bills, ranging from identity theft to collecting data from children, confidentiality of health care records to employers (sic) use of credit reports, privacy in banking to privacy on the Internet. Congress also held a series of hearings on privacy issues. State legislatures were no less attentive to privacy issues. In 1998, 2367 privacy bills were introduced or carried over in U.S. state legislatures; forty-two states enacted a total of 786 bills. (1999, p. 174)

In particular, several authors writing about surveillance in the workplace (Baxi & Nickel, 1994; Gantt, 1995; King, 1994; Miller & Poe, 1996; Rodriguez, 1998; Schnaitman, 1999; White, 1997; Wilborn, 1998) would mention the Privacy for Consumers and Workers Act ("PCWA") introduced by Senator Paul Simon in 1993, which, if passed, would have severely restricted employer monitoring. Additionally, although the passage in 1996 of the—today significant—Health Insurance Portability and Accountability Act ("HIPAA") was not particularly highlighted in the sample of papers reviewed for this period, the Department of Health and Human Services' ("HHS") 1997 submission to Congress of recommendations on protecting the confidentiality and security of individually-identifiable health information was (Hodge Jr., 1999).

Compared to HIPAA's sanction, Congress's approval of the Children's Online Privacy Protection Act ("COPPA") in 1998 was highlighted by more scholars writing during this period. According to Jerry Berman & Deirdre Mulligan, this Act "was supported by children's advocates, privacy advocates, and companies" and represented "tangible evidence that common ground is within reach" (1999, p. 553). In addition, by "provid[ing] a clear statutory authorization for an FTC role in one part of cyberspace" (Schwartz, 1999, p. 1040), this law was also presented by Paul Schwartz as a wise move from Congress to force the Executive branch to act despite the Clinton Administration' hesitation.

Finally, during these years American privacy law scholars would also take note of some few but significant efforts from the Federal Trade Commission ("FTC") and the Department of Commerce.

First and foremost, some scholars (Cate, 1999; Killingsworth, 1999; Schwartz, 1999) emphasized the relevance of the FTC's enforcement action against GeoCities, which would significantly go down in history as the first Internet-related privacy case by the FTC. GeoCities served as a web hosting service, which also provided services such as free e-mail, clubs, and contests. As a result of a consent order, the company was forbidden from making misleading statements about its data collection, use, or disclosure practices, as well as required to obtain the express consent of parents before collecting the personal information of children. Importantly, at the time this order would by described by scholars both as the FTC's "first Internet privacy case" (Cate, 1999, p. 175) and as "a roadmap of Fair Information Practices [("FIPs")]" (Killingsworth, 1999, pp. 70–71).

In turn, in his scholarship Fred H. Cate (1999) would also recognize the Department of Commerce's efforts to negotiate a "safe harbor" code with the European Commission. The importance of these negotiations was clear in light of the threats by Europe to block the flow of personal information to the United States, which Paul Schwartz (1995, 1999) and Joel Reidenberg (1999) would repeatedly raise throughout the decade as an additional reason to take legislative action.

***

Judging by this sociotechnical and techno-legal context, which has said before was narrated through the lens of the scholars here reviewed, the most significant events of these first ten years were, without a doubt, the emergence of the commercial internet and the proliferation of the

personal computers. In addition to these technological developments, which would have a profound effect on the course of technological innovation in the years to come, the sanction of HIPAA and COPPA by Congress, as well as the FTC's enforcement action against GeoCities, would go down in American legal history as landmark events. Yet, at the time scholars were describing these events, they may not have realized their future significance.

## B. American privacy law scholars' response

Echoing American society's distrust in the sociotechnical changes mentioned above, the American privacy law scholars whose work I reviewed for this period would tend to agree among them on the harms that the described technologies and practices could cause individuals. In contrast, however, their opinions regarding the best means to address these harms would be widely divergent. So much so, that none of them would specifically reflect what was actually happening in the American legal system at the time.

### 1. Identified harms

In the view of most American privacy law scholars writing between 1990 and 1999, computers and networks increased the volume of personal information available to public and private entities. "The power of computers and networks to gather and synthesize information" (Nissenbaum, 1997, p. 218) allowed governments and private companies to obtain bits of personal information from many sources. Likewise, because both communications and transactions were now traceable, individuals became subject to real-time observation—referred by many of the scholars as

"surveillance"[46]—that was detailed, cumulative, invisible, automatic, continuous, omnipresent, and pervasive.

According to Lessig, the "feature of the Net that creates the problem of privacy" was the "the invisible, automatic collection of data" (1999b, p. 519). Relatedly, for Michael Froomkin, "the Internet or related networks may become the foundation of the opposite of anarchy: life in a transparent data ocean, a life in which data recording everyone's movements, tastes, purchases, medical history, reading habits, and contacts with officialdom are commodified and available to some, and perhaps even to all" (1996a, p. 507). Thus, scholars writing during these years were concerned about the ability of public and private entities to access records that were finely granulated, "detailed, computer-processable, indexed to the individual, and permanent" (Kang, 1998, p. 1199).

Under these circumstances, which Paul Schwartz described in 1999 as "a privacy horror show" (1999, p. 1640), privacy harms such as the **danger of inaccurate records** (Pincus & Trotter, 1995; Reidenberg, 1992; Schwartz, 1995) and the **possible loss of anonymity** (Cohen, 1996; Milligan, 1999; Reidenberg, 1995; Schwartz, 1999) were discussed in American privacy law scholarship during the period under study. According to Laura B. Pincus & Clayton Trotter, for example, "[b]eyond the pure threat of unwarranted invasions of privacy, a problem exists regarding the accuracy of such records" (1995, p. 52). And when talking about the emergence of a copyright management industry, Julie Cohen would highlight: "This vision of the future of copyright management could entail total loss of reader sought anonymity in cyberspace" (1996, p. 6).

[46] According to Gary Marx, "the topic [of surveillance] in its modern form has been of interest to scholars at least since the 1950s" (Marx, 2015, p. 734). Yet, the 1990s references to surveillance spotted here are unlikely to be part of the surveillance studies literature, since—as discussed in Chapter I—surveillance studies only gained attention as a field after the 9/11 terrorist attacks in 2001.

There were, however, two other harms that particularly caught the attention of scholars, namely, the threat to individual autonomy and the loss of the individuals' ability to control their personal information.

### 1.1. A threat to individual autonomy

Several scholars writing in the 90s would refer to the corrosive effect of electronic surveillance on individual autonomy (Branscomb, 1995; Froomkin, 1996a; Gantt, 1995; Glancy, 1995; Kang, 1998; Milligan, 1999; Reidenberg, 1995; Reiman, 1995; Schwartz, 1992, 1995, 1999; Shorr, 1995; Van Den Hoven, 1997). According to Schwartz, "the computer offers the state and society a powerful way to control the behavior of individuals" (1992, p. 1342). How so? In this scholar's words,

> [T]his digitalization of personal information heightens the ability of bureaucracies to "*adapt an individual to a predetermined, standardized* behavior that aims at the highest possible degree of compliance." By using personal data to shape behavior patterns, the state may *repress the ability of individuals to make free decisions* about values and preferences and to act on these choices. (Schwartz, 1992, p. 1362)

Thus, according to these scholars, in the managerial data processing model individuals would look to match their conduct to behaviors defined and prioritized by computer models. "Data gathering," Schwartz would explain, "places pressure on individuals to conform to institutional standards of behavior" (1995, p. 583). For example, when it comes to getting access to welfare benefits, citizens would adapt their actions to please the expectations of the state's computerized systems. As Joel Reidenberg (1995) would complement, the fact that deviations from predicted behavior are questioned and negatively rewarded inevitably influences the individuals' choices. Thus, people would tend to act in ways that are publicly acceptable, and as a result, "our every move is fitting data for observation by others" (Reiman, 1995, p. 39).

Similarly, scholars would highlight how the mere knowledge that their actions are being recorded by computers can also alter the individuals' decisions. In that sense, "awareness of being visible makes people the agents of their own subjection" (Reiman, 1995, p. 5). For instance, in 1995 Scott Shorr would denounce how "one may decline to purchase a magazine or birth control device in a grocery store for fear that the check-out machine will record and maintain records of these transactions that unknown others can peruse, sell, and use as the basis for personal judgments" (Shorr, 1995, p. 1768). According to these scholars, this effect of awareness—which drawing upon First Amendment caselaw from the 1950s several scholars would refer to as a **"chilling effect"** (Froomkin, 1996a; Milligan, 1999; Reiman, 1995)—also ends up constraining the individuals' freedom to act, leading to what Jerry Kang would catalog as "self-censorship" (1998, p. 1260). As M.J. van den Hoven's example about "Bill" aptly illustrates,

> Information about Bill, whether fully accurate or not, facilitates the formation of judgements about Bill. Judgements about Bill, when he learns about them, suspects that they are made, fears that they are made, *may bring about a change in his view of himself, may induce him to redefine his desires, to reorder his preferences or make him behave differently than he would have done without them*. (1997, p. 36)

As a result, scholars would call attention to the ways in which the increased accessibility to personal data suspends self-ownership and hinders the individuals' self-governance and self-determination. According to Jeffrey H. Reiman, for example,

> Growing up in the informational panopticon, *people will be less likely to acquire selves that think of themselves as owning themselves*. They will say mine with less authority, and yours with less respect. And I think that selves that think of themselves as owning themselves are precisely what we understand as "moral selves." They are selves that naturally accept ownership of their actions and thus responsibility for them. They naturally insist on ownership of their destinies and thus on the right to choose their own way. (1995, p. 40)

Finally, for some of the scholars of the epoch (Kang, 1998; Reiman, 1995; Schwartz, 1999), not only individual autonomy, but also **democracy** was affected by the electronic surveillance enabled by computers and networks. For them, if individuals do not enjoy space to experiment with, reflect on, and entertain beliefs (Reiman, 1995); if they do not have areas of limited access to deliberate—alone and together with others—about how to live their lives (Schwartz, 1999); and if they lack "the capacity to reflect upon and choose personal and political projects and how best to further them" (Kang, 1998, p. 1260), they lose their capacity for critical reflection, on which social participation depends. As Reiman would eloquently point out in 1995, "unless, in forming their own views, people can find within themselves the resources for better views, *neither democracy nor individualism can be expected to improve human life*" (1995, p. 42). Likewise, in 1999 Schwartz would argue: "*democracy* in the United States depends on group deliberation as well as individuals who are capable of self-determination" (1999, p. 1613).

### 1.2. The loss of the individuals' ability to control their personal information

Besides the threat to individual autonomy, during the years covered in this Chapter a significant number of scholars also raised the loss of the individuals' ability to control their own data as a notable harm. "[A]s vastly greater quantities of information are collected and transmitted to an ever increasing number of users in remote locations," Lawrence O. Gostin would clearly explain, "the ability of consumers to control the dissemination of personal information is sharply reduced" (1995, pp. 492–493). According to the scholars, circumstances that may have possibly contributed to this threat to individuals' control over their personal information include: (i) the ignorance of people about the complex processes by which their personal data are processed (Schwartz, 1999);

and (ii) “fewer and fewer direct contacts (…) between individuals and those holding personal information” about them (Reidenberg, 1992, p. 198).

In the view of scholars writing in the 1990s, this lack of control posed a threat to privacy in a variety of ways, including: third party access, secondary uses, and profiling. To begin with, an individual’s lack of control over her data could result in **unauthorized disclosures of personal information to parties other than the initial recipient**. As Christopher S. Milligan would explain by the end of the 20th century, “[t]he term ‘data creep’ describes the way in which information given and used for one purpose, such as public records, *tends to be disseminated-from the governmental agency that collects the information to a company that compiles databases of information, and then finally to the consumers of this information*” (Milligan, 1999, p. 329).

Likewise, scholars would denounce how “[d]igital communications leave traces and portraits of every interaction with the network, and these traces may be put to a variety of unwanted **secondary uses**” (Reidenberg & Gamet-Pol, 1995, p. 106). In particular, they would raise alarms about possible cross-sectoral uses (Bibas, 1994; Reidenberg, 1992). And in the specific practices highlighted above, such as electronic monitoring in the workplace, Robert G. Boehmer (1992) and to Frank J. Cavico (1993) would for example explain how impermissible and illegitimate secondary uses of recorded data about an employee could include, for instance, identifying and disciplining whistleblowers. In fact, scholars would notice how the potential for abuse was also significant. In particular, in the case of electronic surveillance in the workplace abusive uses could include voyeurism (Lee, 1994). In other contexts, “[a]busive husbands have employed the Internet to hunt fleeing wives. Similarly, criminals have used the Internet to steal identities” (Sovern, 1999, p. 1048).

Finally, several scholars would also raise how data gatherers could combine data from various existing sources to construct detailed personality profiles (Boehmer, 1992; Cohen, 1996; Froomkin, 1996a; Gostin, 1995; Kang, 1998; Nissenbaum, 1997; Reidenberg, 1992; Reiman, 1995). As Julie Cohen would aptly explain, the activity of **profiling** was not new for the epoch:

> For transactions that occur in "real" (as opposed to digital) space, however, the ability to profile one's customer base is limited to some extent by customers' willingness to self-report — for example, by filling out product registration cards. In contrast, profiling in the digital age holds out, for the first time, the tantalizing promise of "perfect" information, because *digital communications can be structured to create detailed records of consumer purchases and reading activities*. (1996, p. 6)

Similarly, in 1994 Steven A. Bibas would report how "[c]omputers today track our telephone calls, credit-card spending, plane flights, educational and employment records, medical histories, and more. Someone with free access to this *information could piece together a coherent picture of our actions*" (Bibas, 1994, p. 591).

Thus, in the 1990s American privacy law scholars would describe how the accumulation, compilation, and aggregation of data into profiles could both allow private and public entities to learn much more—and make **inferences**— about the private lives of individuals, and generate "a spate of dire **predictions**" (Reidenberg & Gamet-Pol, 1995, p. 593). In Jeffrey H. Reiman's words, "by accumulating a lot of disparate pieces of public information . . .[y]ou can find out who her friends are, what she does for fun or profit, and from such facts others can be inferred, whether she is punctual, whether she is faithful, and so on" (1995, p. 29). Similarly, analytic methods already available at the time "allow the observer to generate information not only revealing what the observed person did, but *what they have the potential to do in the future*" (Boehmer, 1992, p. 768).

According to a number of scholars (Berman & Mulligan, 1999; Glancy, 1995), by the mid-90s data collectors had already started to use these capabilities to provide personalized content and

targeted advertising to individuals. Likewise, taking into consideration these identified capacities of information technologies for inference and prediction, scholars would further highlight the "synergistic threat to privacy" (Kang, 1998, p. 1240) posed by portraits. In Helen Nissenbaum's words, "the value of information can be seriously affected by combining and compiling it with other information. Metaphorically speaking, with information one can sew a silk purse out of a sow's ear" (Nissenbaum, 1997, p. 216). Similarly, according to Michael Froomkin, "although profiling may not necessarily change the amount of actual data in existence about a person, organizing the data into easily searchable form reduces her effective privacy by permitting 'data mining' and correlations that were previously impossible" (1996a, p. 399).

Interestingly, this synergistic threat correlates with another type of risk that some few other authors of that era would assign, not to profiling specifically, but to massive data collection in general. According to Jeffrey H. Reiman, for example,

> [i]nformation-gathering in any particular realm may not seem to pose a very grave threat precisely because it is generally possible to preserve one's privacy by escaping into other realms. Consequently, as we look at each kind of information-gathering in isolation from the others, each may seem relatively benign. However, as each is put into practice, its effect is to close off yet another escape route from public access, so that *when the whole complex is in place, its overall effect on privacy will be greater than the sum of the effects of the parts*. (1995, p. 34)

While Reiman would use the term "informational panopticon" to refer to this risk, Anita Allen would describe it as "the aggregation problem." According to Allen, "numerous little consensual and nonconsensual privacy losses, too trivial to protest individually, *aggregate into a large privacy loss* that is a detriment to the liberal way of life" (1999a, p. 740).

### 1.3. Sparse but visionary references to other harms/circumstances

Besides these two prevalent privacy harms—harm to individual autonomy and possible threats derived from the loss of control over personal information, sparse mentions to **manipulation** are worth noting. Although manipulation would only become preponderant in the privacy law scholarship of the second half of the twenty-teens, in 1995 visionary[47] scholar Joel Reidenberg would refer to how "[t]he ubiquitous availability of extensive information risks the *manipulation*, molding, and adjustment of individual conduct" (1995, p. 536). Similarly, but in the specific context of the Intelligent Vehicle Highway Systems, in 1995 Dorothy J. Glancy pointed out: "ITS can *manipulate* individual decisions about modes, times and destinations of travel by means of route guidance, traffic congestion information, persuasion and advertisements of products and services" (1995, p. 166). Finally, in 1997 Helen Nissenbaum claimed: "portraits are developed not for the purpose of developing friendship or intimate association, but to *manipulate*, motivate, and judge" (1997, p. 217).[48] Despite the fact that these early mentions of this harm did not include a thorough exploration of what manipulation could mean in the digital context, the fact that a few scholars were already referring to it in the 1990s is noteworthy.

Additionally, before concluding, a quick mention should also be made of the importance that during these early years visionary scholars would give to emerging **power imbalances**. In the

[47] Throughout this Chapter, as well as the following ones, I use the terms "visionary" and "pioneer" to recognize scholars who were among the first to spot a given harm or propose a tool, way before their contemporaries.

[48] Although Lawrence Lessig did not refer to manipulation in the articles he published between 1990 and 1999, in his 1999 book *Code and Other Laws of Cyberspace* he would discuss this harm as one of the possible risks associated with computer profiling. Thus, even though this book—given its nature as such— was not formally part of the sample of documents reviewed for this study, its visionary reference to manipulation is worth noting here:

> profiles will begin to normalize the population from which the norm is drawn. The observing will affect the observed. The system watches what you do; it fits you into a pattern; the pattern is then fed back to you in the form of options set by the pattern; the options reinforce the pattern; the cycle begins again. (Lessig, 1999, p. 154)

same 1995 article previously mentioned, Joel Reidenberg would also highlight how "the concentration of information techniques leads to an *imbalance of political power*" (1995, p. 536). Likewise, in the context of workplace privacy, that same year Larry O. Natt Gantt stated: "[t]hese new monitoring technologies have intensified employee privacy concerns because the instruments *abolish the desirable balance of power* between employers and employees" (1995, p. 346). Similarly, writing in 1996, Michael Froomkin would note: "in an imperfect market profiling *threatens to change the balance of power* between consumers and sellers" (1996a, p. 480). Finally, in 1999 Paul Schwartz would argue: "the Internet creates a model for decisionmaking through personal data use that *shifts power* to private organizations and public bureaucracies" (1999, p. 1612). According to Schwartz, "[t]hese developments, experienced in small and large ways by millions of Internet users, are creating a *new hierarchy of power*" (Schwartz, 1999, p. 1646).

As will be seen in Chapters III through V, by the end of 2020 the exacerbation of these power asymmetries would have drawn the attention and interest of a much greater number of scholars, significantly impacting the privacy tools by them proposed.

## 2. Proposed privacy tools

According to the scholarship reviewed for this period, as of 1990 industry self-regulation had been the most popular privacy approach in American society. Between 1990 and 1999, however, many scholars would agree that this alternative was not being effective in preventing the privacy harms by them identified at the time.

As Joel Reidenberg would maintain in 1992 and repeatedly in the years to come, "self-regulatory schemes have been adopted by some industries and by various companies. Although these schemes may offer privacy protection, *they do not provide enforceable legal rights and do*

*not seem to have permeated the vast majority of information processing entities*" (1992, pp. 208–209) (Reidenberg, 1995, 1999; Reidenberg & Gamet-Pol, 1995). Similarly, some authors addressing electronic monitoring in the workplace would also refer to the inconvenience of relying on self-regulation by employers. Larry O. Natt Gantt, for example, would claim: "[t]his solution is unacceptable because employers often believe they have significant incentives to marginalize the protection of employee privacy. Consequently, *American businesses have largely failed to revise their in-house privacy policies despite their increasing use of electronic monitoring*" (Gantt, 1995).

Instead, scholars writing during this period would propose the following variety of alternative avenues: a FIPs-like legislative solution, solutions based on the rule-making power of technology, scenario-specific solutions arguably able to address specific contexts, and compound solutions combining different alternatives.

### 2.1 FIPs-like comprehensive legislative solutions

A first group of scholars would tend to call for a legislative solution (Boehmer, 1992; Conlon, 1996; Gantt, 1995; Gostin & Hodge Jr., 1999; Pincus & Trotter, 1995; Russell, 1995). The proposed legal interventions were supposed to be *comprehensive*, in order to solve the problems of existing legal safeguards which, as seen earlier, were "fragmented and inconsistent, with major gaps in coverage, and there [were] significant theoretical problems with its structure" (Gostin, 1995, p. 495). Likewise, most of the reviewed scholars also considered that the proposed legislation should be adopted *at the federal level*, "[b]ecause personal information flows are not

confined to state or national borders" (Reidenberg, 1992, p. 238) and "to aid business compliance without undue hardship" (Boehmer, 1992, p. 812).[49]

More specifically, several scholars writing during this period argued that Congress should pass national legislation that would make mandatory and enforceable what was already known at the time as the Fair Information Practices principles ("FIPs"**)**. These principles had been proposed by the U.S. Department of Health, Education, and Welfare in 1973 and later included in a set of voluntary guidelines adopted in 1980 by the OECD. Nevertheless, until then, in the U.S. they had only been turned mandatory in certain sectoral laws (e.g., the Privacy Act or the Video Privacy Protection Act) or had been dispersed in "legal rules, industry norms, and business practice" proposed by different "standard makers-namely government, industry groups, and individual companies" (Reidenberg, 1995, p. 508).

For example, when looking to balance the public need for health information against individual claims to privacy, in 1995 Lawrence O. Gostin proposed "a federal preemptive statute based on *fair information practices*" (1995, p. 456). Similarly, writing also about healthcare and trying to find an optimal pattern of knowledge and privacy, in 1997 Paul Schwartz argued that "the law should put in place *fair information standards* that provide a privacy safety net for all health care consumers" (1997, p. 5). Likewise, seeking to respond to the cumulative effects of eroding privacy tastes and expectations, in 1999 Anita Allen would argue: "It may also be a matter of regulating the corporate sector more aggressively, requiring *fair information practices* that give

[49] Others, however, would advocate for "both a general data protection law (providing a safety net in an age of technological change) and specific laws directed at discrete data systems" (Schwartz, 1992, p. 1375). According to Paul Schwartz, "[l]egislation, therefore, must not only take the form of a general data protection law, providing a safety net in an age of rapid technological developments, but must also consist of specific laws directed at discrete sectors of data application" (1995, p. 563).

employees and consumers greater control over what information is collected and how it is used" (1999a, p. 756).

To be clear, during the reviewed time most scholars would not directly use the term "FIPs." Rather, many of them would talk about a set of benchmark principles that in terms of content, corresponded to what the Data Protection laws were looking like at that moment around the world. Drawing on a description provided by Joel Reidenberg, "[t]he basic principles of this global consensus form four sets of standards: (1) standards for data quality, (2) standards for transparency or openness of processing, (3) standards for the treatment of particularly sensitive information, and (4) standards for the enforcement of *fair information practices*" (Reidenberg, 1995, p. 513).

Inspired by Germany, for example, in 1992 Robert G. Schwartz Jr. advocated for "a new Federal Data Protection Act" (1992, p. 138). Similarly, that same year Paul Schwartz articulated three principles of an American law of data protection, which "should be organized around three elements: The maintenance of transparent information processing systems, the assignment of limited procedural and substantive rights to the data subject, and the establishment of independent monitoring of the processing of data" (1992, p. 1375). Later on in the decade, he would add a fourth element: "the creation of a statutory fabric that defines obligations with respect to the use of personal information" (Schwartz, 1995, p. 555). In that sense, Schwartz would argue, "[a] statute authorizing the collection of personal information must generally specify the purposes of data collection, place limitations on the period of information storage, and provide measures of data security. It must also create special protection for certain kinds of sensitive data" (1992, p. 564).

Likewise, when it came to intelligent transportation systems ("ITS") scholars would claim the establishment of requirements similar to the ones included in the OECD's guidelines. According to Dorothy J. Glancy, for instance,

> Privacy laws may also require that all ITS providers first establish *the need* for individually identifiable information about ITS users and then publish *privacy statements* describing the personal information which the ITS system intends to collect, the reasons for collecting it, how the information will be used and how long it will be kept. Privacy laws may also establish *a legal right on the part of each ITS user to access all information about herself* collected by ITS providers, as well as *the identities of everyone requesting or receiving personal information* about her from an ITS system. Privacy laws may further require *destruction of individually identifiable information*, once the described need for it is satisfied, and, in any event, after the passage of a short specified period of time. Privacy laws could also *prohibit compilation by ITS of individual travel profiles and travel histories without the consent of the person involved*. (1995, p. 186)

Therefore, although framed in different ways, many proposals in the ITS sphere would tend to revolve around the FIPs principles of notice, choice, access, data quality, security, collection limitation, and accountability.

In a similar fashion, several privacy law scholars focusing on privacy in the workplace (Bindler, 1992; Conlon, 1996; Flanagan, 1994; Lee, 1994; McCartney, 1994; Schnaitman, 1999; Wilborn, 1998) would argue that a new federal law should grant employees certain enumerated rights, such as the right to notice, the right to be informed about how the employer would use the data obtained, the right to review their own records and to correct or amend inaccurate or incomplete records, the right not to be monitored in private spaces; as well as a remedy for the violation of the listed provisions. According to Susan Ellen Bindler, for example, "legislation granting employees affirmative rights in the work place will strike a better balance between employer and employee interests" (1992, p. 856).

Notably, these claims for a legislative solution would usually come along declarations on the necessity of creating an American data protection authority or national privacy "czar." Privacy law scholars such as Paul Schwartz (1992, 1995, 1997), Joel Reidenberg (on his own and along with Franqoise Gamet-Pol) (1992, 1995, 1999; Reidenberg & Gamet-Pol, 1995), Donald R. McCartney (1994), Lawrence O. Gostin (1995), Anita Allen (1999a), and Jerry Berman & Deirdre Mulligan (1999) would stress the need of having an institution in charge of: (i) studying the effects and implications of data processing practices; (ii) offering independent expertise; (iii) monitoring data processing practices and compliance with laws; (iv) assuring flexibility for contextual differences in the application of laws; (v) achieving public awareness of identified privacy concerns and the need for further regulation; (vi) articulating a comprehensive vision of privacy protection for the US; (vii) assisting citizens to exercise their rights; (viii) determining if industry codes of practice comply with the underlying rights and even granting safe harbor protections for company practices; and (ix) representing the US in front of foreign data protection authorities.

### 2.2 Solutions based on the rule-making power of technology

To be sure, not every privacy law scholar writing during this epoch would agree about the necessity or effectivity of enacting the FIPs through data protection-type laws. For example, even though Alan Westin supported the enactment of pre-emptive federal privacy legislation in certain sectors such as healthcare (Westin, 1996), he would be against applying this solution in the workplace space. According to Westin, "when advocates claim that performance monitoring is a privacy issue-and seek state or federal legislation or court rulings to outlaw employer monitoring or provide notice each time monitoring is used-the concept of privacy is stretched beyond its rational limits" ( 1996, p. 282).

More generally, several authors would show skepticism about the ability of the law, by itself, to protect privacy on the Internet and in electronic commerce. In 1996, for instance, Michael Froomkin would contend:

> Unfortunately, *whether data protection laws are effective in providing long-term protection of the privacy of personal information remains uncertain*. Data protection laws are likely to work best when the data collectors are few, or operate in industries that are already highly regulated, such as banks. Bigger databases are easier to regulate that many small databases: "the more concentrated the profile data, the greater the privacy that is possible by regulation." As data collection and communication techniques grow, however, it is at least possible, and perhaps likely, that the large centralized database will become as much of a dinosaur as the mainframe, to be replaced by networks of small, interlinked databases continually updated in real time. *Data protection regulation would be particularly difficult in such a world. Worse, the international nature of data flows limits the ability of any single nation to enforce its data protections laws*. (1996a, pp. 490–491).

Thus, as an alternative he would propose using technology to ensure anonymous communications ("through a combination of encryption and chained computers running remailer programs" (1996a, p. 506)) and transactions (through "cryptographic protocols for secure electronic transactions" (1996b, p. 49)). According to him,

> [i]n the absence of effective data protection laws, anonymous communication and transactions are the only techniques that are likely to allow one to control the dissemination of personal information and thus even partly realize the idea of home as a secure fortress. Digital anonymity may be a rational response to a world in which the quantity of identifying data on each of us grows daily, and the data become ever easier for government and private parties to access. (1996a, p. 491)

That same year, Joel Reidenberg would similarly claim:

> *Basic regulatory policymaking*, whether under the anti-statist American approach or the comprehensive European approach, *is ill suited to the [Global Information Infrastructure] GII*. Instead, a new "network governance paradigm" must emerge to recognize the complexity of regulatory power centers, utilize new policy instruments such as *technical standardization* to achieve regulatory objectives, accord status to networks as semi-sovereign entities, and shift the role of the state toward the creation of an incentive structure for network self-regulation. (1996, p. 930)

With these claims, both Froomkin and Reidenberg referred to what soon would be coined by Reidenberg himself and Lawrence Lessig as "Lex Informatica" (Reidenberg, 1998), "code is law," or architecture-technologies (Lessig, 1999). Since at least 1995, scholars writing about Intelligent Transportation Technologies, such as Dorothy J. Glancy (1995) and Jeffrey H. Reiman (1995), had started to talk about the possibility of using technological safeguards to protect privacy. However, it was in 1998 when Reidenberg extensively theorized about the rule-making power of technology and networks. In his article *Lex Informatica: The Formulation of Information Policy Rules through Technology*, he contended:

> Historically, law and government regulation have established default rules for information policy, including constitutional rules on freedom of expression and statutory rights of ownership of information. This Article will show that *for network environments and the Information Society, however, law and government regulation are not the only source of rule-making. Technological capabilities and system design choices impose rules on participants.* The creation and implementation of information policy are embedded in network designs and standards as well as in system configurations. Even user preferences and technical choices create overarching, local default rules. (1998, p. 554)

In a similar fashion, in 1999 Lessig would argue: "What is missing in discourse about cyberspace and its regulation is a richer understanding of the range of architectures that are possible. We must develop *an attitude that analyzes architecture as critically as it analyzes laws- an attitude that understands the politics in both*" (1999a, p. 65).

In terms of this intellectual history, these claims—which inserted themselves in broader conversations about the Net as "lawless" (Cate, 1999; Johnson & Post, 1996; Reidenberg, 1996; Schwartz, 1999) and the "law of the horse" (Easterbrook, 1996; Hardy, 1994; Johnson & Post, 1996; Lessig, 1999b)—mark a first turning point in the discussion about regulatory techniques to protect information privacy in an era of personal computers and networks. First, as the second half

of the 1990s progressed, American privacy law scholars began to realize that, in addition to a legal regulatory regime, "several technical solutions provide valuable tools to establish fair information practice policy on global networks" (Reidenberg, 1998, p. 562). Thus, even though the FIPs kept being considered as one of the most popular approaches to regulate privacy, the means to enforce them became more diverse, including both laws enacted by a legislature (commonly known as statutes) and technological standards implemented through code.

According to Reidenberg, for example, "effective privacy does not end with a legislative enactment. The guarantee of privacy for citizens requires *a combination of law and technology that affords mechanisms to assure the fair treatment of personal information*" (1999, p. 787). And he was far from being alone in these appreciations. As Jerry Berman & Deirdre Mulligan would contend in 1999, "[l]aw is only one tool for protecting privacy. In this global, decentralized medium, *we must promote applications of technology* that limit the collection of transactional information that can be tied to individuals" (1999, p. 573). In a similar tone, that same year Fred H. Cate would argue:

> *Digital technologies offer individuals enormous privacy protection* and the ability to access information with disclosing anything about themselves. This is not to suggest that technologies are a panacea or that law is irrelevant, but simply that *the Internet is empowering many people to protect their rights in a way that the law so far has been able to*. (1999, p. 231)

Second, as this change of focus happened, the role of legal rules suffered changes too. Instead of being used to impose transparency obligations and standards of data quality, and to establish procedural and substantive rights and systems of independent monitoring, the law started to be depicted as an instrument to provide incentives to influence the development of privacy-protective technologies and privacy-enhancing default settings through diverse strategies such as favorable tax treatment, accreditation, and allocation of liability. As explained by Reidenberg

himself, "[l]aw, nonetheless, has an important place in the elaboration of Lex Informatica. Law may encourage the development of Lex Informatica *by imposing liability on various network actors,* and *law may provide immunity or safe harbors for implementation of technical rules*" (1998, p. 583). Similarly, in a 1999 article Lessig would argue that the role of the government should be now to regulate indirectly, through the regulation of cyberspace's code. In his words,

> the most effective way to regulate behavior in cyberspace will be *through the regulation of code - direct regulation either of the code of cyberspace itself, or of the institutions (code writers) that produce that code*. Subject to an increasingly important qualification, we should therefore expect regulators to focus more upon this code as time passes. (1999b, p. 514)

As will be seen in the following three Chapters, although this focus on the rule-making power of technology would lose some of its forcefulness in the years to come, it would never disappear from the minds of American privacy law scholars, constantly reappearing under new names (e.g., Privacy enhancing technologies ("PETs"), computer science's proven strategies).

### 2.3 Scenario-specific solutions

A third group of scholars would also react against the legal standards solution, but for the unlikeliness that a uniform statutory response could appropriately address all possible scenarios and industries. Pauline Kim, for instance, would contend: "Because legislative protection of privacy is necessarily piecemeal and reactive in light of such rapid change, *limiting the source of public policy to specific statutes seems especially inappropriate when considering issues of privacy*" (1996, p. 727). Also in the sphere of privacy in the workplace, I. Trotter Hardy would argue:

> the low transaction costs that follow from the existing contractual relationship and the wide variation in desires for privacy by both employers and employees in the employment setting-not to say the rapid technological changes that make it hard to

> know what “e-mail in the workplace” will look like in only a few years' time-show that a *uniform statutory response for all industries is very much inappropriate here*. (1994, p. 1033)

Despite this common ground of opposition, the scenario-specific alternatives actually proposed by the different scholars would considerably vary, ranging from self-regulation to tort-based approaches, and market-based solutions.

### 2.3.1 Self-regulatory tools

In order for the interventions to be context-specific, some of these scholars would call for maintaining the prevalent self-regulation approach. Scott Killingsworth, for instance, would encourage companies to adopt the FIPs but through either their own privacy policies or “Privacy Seal” programs such as those sponsored by TRUSTe or BBBOnLine. According to him,

> The flexibility that makes these principles so widely acceptable to consumer advocates, government, and industry alike could be equally well described as "vagueness," and the specter of endowing these principles with the force of law-to be further defined, refined, and expanded in the American way, through detailed regulations and endless litigation-is enough to make any businessperson an apostle of self-regulation. *Self-regulation, after all, is simply the ability to decide for oneself what the term "reasonable" means*. (1999, p. 71)

Especially in the sphere of workplace surveillance, more and more scholars would encourage employers to draft their own privacy policies. According to Jarrod J. White, for example,

> [e]mployers unwilling to sit idly by and ignore misuse of the company's E-mail system should *undertake the drafting of a comprehensive E-mail policy*. Not only does an E-mail policy limit or eliminate potential liability from privacy lawsuits but also such a policy may proactively decrease E-mail abuse by alerting employees that their employer will be watching. (1997, p. 1103)

Likewise, as part of his proposed solutions—which included modifying Title III and the Electronic Communications Privacy Act of 1986 (ECPA)—Thomas R. Greenberg would recommend employers to "publish and post a policy defining the intended business uses of E-mail and voice mail systems, and indicate that these systems may be accessed by the employer without notice to employees" (1994, pp. 249–250). And in a similar vein, Christopher S. Miller would suggest: "As a result of the uncertain legal environment, as well as several other factors, employers should establish explicit policies with respect to issues of e-mail usage, control, and monitoring to ensure protection from potential causes of action, and to foster organizational goals generally" (1996, p. 111).

### 2.3.2 Tort-based approaches

Instead, other fewer scholars would propose to go back to the origin of the right to privacy in America—Privacy Torts—and adapt the existing Privacy Torts to the Internet age.

For example, Andrew J. McClurg would recommend redefining the *tort of intrusion upon seclusion*, to encompass a right of "public privacy" (1995, p. 989). Relatedly, but in the realm of privacy in the workplace, Pauline T. Kim would argue that "the *common law tort of invasion of privacy* should be recognized as a public policy limiting an employer's authority to discharge" (1996, p. 724). According to her, "[o]nce the common law right of privacy is recognized as a public policy limiting the at-will rule, the employee stands in a wholly different position when confronted with potentially intrusive practices by her employer" (1996, p. 728). John A. Jurata Jr., in turn, would propose a new standard for determining newsworthiness in the *private facts tort*, "a standard that considers the social use of the information, the extent of prying into private lives for the information, and most importantly, the private or public status of the victim" (1999, p. 492).

Other scholars would go further and propose a non-privacy tort, namely, breach of confidence. Randall P. Bezanson, for instance, would suggest "that the privacy tort be formally interred," and be replaced, instead, by the tort of breach of confidence. According to Bezanson, "I suggest that (…) we look to the concept of breach of confidence to provide legally enforceable protection from dissemination of identified types of personal information" (1992, p. 1174). Similarly, Michael Harvey would argue that "an enforceable duty of confidentiality can overcome all of these objections and provide a better balance of privacy and First Amendment interests than the existent private-facts tort" (1992, p. 2393).

However, these claims would not be free of contestation. For Susan M. Gilles, for example, "breach of confidence will not prove an effective replacement for the ailing private-facts tort" (1995, p. 84). According to her, even though appealing and effective, a tort-based action for breach of confidence would turn to be unconstitutional. This, by being unable to survive First Amendment scrutiny under the standards established in 1991 by the Supreme Court in *Cohen v. Cowles Media Co*.

### 2.3.3 Market-based solutions

Nevertheless, other scholars would consider that even torts disregarded individual preferences and countervailing values. As a result, they would instead opt for a market solution based on property rights and/or Contract law.

According to Stephanos Bibas, a contractual solution could give individuals the power to choose privacy or not, while balancing the individual's desire for privacy against the rights of others to benefit from the information economy. "[T]he price mechanism," Bibas would argue, "takes into account individual values, needs, and tradeoffs, allocating resources to their most

valued uses. Pricing, unlike central planning, respects consumer preferences. It adjusts resource-allocation decisions to maximize value and swiftly takes changed circumstances into account" (1994, p. 604). Likewise, Scott Shorr would contend that "an alternative legal regime grounded in property and contract law can protect privacy from credit bureau invasions without unreasonably infringing free commercial speech" (1995, p. 1759).

Although relatedly, both Richard S. Murphy (1996) and Jerry Kang (1998) would suggest that a privacy default rule should be set first, around which parties would be able to contract. According to Murphy, "[a] privacy default rule, however, would force the vendor to bring such practices to the attention of the consumer, and pay for the information (with money, or more likely, product inducements) if it were worth it to do so" (1996, p. 2414). In a similar fashion, Kang would encourage legislators to draft a uniform federal law titled the Cyberspace Privacy Act, which would include only one default rule: "Unless the parties agree otherwise, the information collector should process personal data only in functionally necessary ways" (1998, p. 1259). "If an information collector seeks to process personal information beyond these identified ways," Kang would argue, "it must contract around the default rule with the individual. For an agreement to be genuine, a clear and conspicuous offer has to be made" (1998, p. 1272).

In turn, Lawrence Lessig would suggest relying on technology "to construct a regime where those who would use the data internalize this cost, by paying those whose data are used" (1999a, p. 63). In that sense, he would combine the technology-as-law approach proposed by Reidenberg and himself and described earlier, with a market solution based on a property regime. According to Lessig, "[p]roperty regimes make little sense unless transactions involving that property are easy. And one problem with the existing architectures, again, is that it is hard for individuals to exercise choice about their property" (1999b, p. 520). Thus, looking to respond to

this flaw, Lessig would propose to rely on technologies such as the Platform for Privacy Preferences (P3P), designed by the World Wide Web Consortium (W3C), to negotiate the price to be paid by the market.

As will be seen in the next Chapter, this P3P-based solution proposed by Lessig would become the target of considerable criticism in the years to come.

### 2.4 Compound solutions

Due to the complexity of the Internet era, by the end of the decade many of these scholars would be arguing for the need of a combination of many of these different alternatives—especially focusing on legal regulation, technology, auto-regulation, and the market. Joel Reidenberg, for instance, would argue:

> For global networks, governance should be seen as *a complex mix of state, business, technical, and citizen forces.* Rules for network behavior will come from each of these interest centers. Within this framework, the private sector must be a driving force in the development of the information society and governments must be involved to protect public interests. At the same time, policymaking cannot ignore technological concerns and technologically-driven decision-making. (1996, p. 926)

Similarly, in 1999 Paul Schwartz would recognize the importance of all the different approaches, although underscoring the statutory solution as the principal building block. According to Schwartz:

> *all three of these techniques, including self-regulation, have an important role in developing effective privacy norms*. Under current conditions in cyberspace, however, *it is the law's imposition of standards that is of essential importance*. A statutory expression of privacy norms for cyberspace will be the most effective first step in promoting democratic deliberation and individual self-determination in this new realm. This legal action will lead to three significant benefits: (1) the prevention of a lock-in of poor privacy standards on a societal level; (2) the creation of preconditions for effective market and self-regulatory contributions to privacy protection; and (3) the termination of United States intransigence on the wrong side

> of ongoing negotiations with the European Union about trans-Atlantic transfers of personal data. (1999, p. 1615)

As Chapter III will show, between 2000 and 2007 other scholars would also support the idea of combining the FIPs-based statutory solution with other complementary alternatives.

***

From this Chapter, three main reflections follow. It appears evident that scholars writing during this period were relatively united regarding the potential harms that personal computers and the Internet could cause individuals, namely, the threat to individual autonomy and the loss of individual control over personal information. While these harms could be described as mainly affecting the individual's "ability to exercise control over information about oneself" (Solove, 2002c, p. 1092) and "the protection of one's personality, individuality, and dignity" (Solove, 2002c, p. 1092), their effects on *collective values* such as democracy would also be recognized by scholars writing during this time.

As a second point, unlike the identified harms, the avenues proposed by scholars at the time to address these harms were still highly in flux. Additionally, none of these proposed avenues appeared to coincide with what was actually happening in the American legal system at the time. As Congress continued its quest to approve *sectoral* laws such as HIPAA and COPPA, a substantial number of scholars supported the Fair Information Practices (FIPs) principles contained within these laws, but considered they should either be implemented through a *comprehensive* privacy law or through technology. Even those scholars who agreed that a sectoral approach was necessary would reject the statutory approaches finally adopted by Congress during those years. Rather, they would prefer that the legal system responded to the needs of specific sectors,

industries, and individuals through either inaction (allowing self-regulatory tools to grow), updated torts, or market-based solutions.

Finally, it seems important to note how, despite the FTC's landmark GeoCities case, most scholars writing at the time were not yet focusing on the Commission as a key privacy player.

## III. 2000-2007: A Period of Technological Sophistication and Relative Convergence

As announced in Chapter II, the purpose of the present Chapter is to continue tracing the intellectual history of the algorithmic turn experienced by the privacy law scholarship produced by the community of scholars that developed *around* PLSC. For doing so, this Chapter covers the first seven years of the twenty first century (2000-2007).

As I hope to demonstrate in the following pages, at the turn of the century American privacy law scholars were not surprised by radical sociotechnical developments that differed from those they had already encountered in the 1990s. Having grappled in the previous decade with concepts and techniques such as cookies, data mining, and computer profiling, during this period scholars would become more sophisticated in their understanding of these technologies. While doing that, scholars would also attentively follow the regulatory implementation of the sectoral privacy laws that had been sanctioned by Congress by the end of the twentieth century, as well as the rise of the FTC as a key player in the American information privacy regulatory landscape. Likewise, following previous alarms from Jeff Sovern (1999) and Anita Allen (1999a), they would start to notice a growing ambivalence of American society about the value of privacy, in which individuals would keep manifesting concerns about their privacy, but at the same time exposing their personal information online.

Against this context, scholars would further develop their conceptualization of the reach and scope of the two privacy harms to individuals' autonomy and control already identified by them in the previous decade. In response to them, scholars would begin to narrow down the regulatory alternatives discussed in Chapter II, uniting around a clear opposition to market-based solutions,

showing openness to a diverse array of tort-based solutions, and overwhelmingly supporting proposals for legally enacted FIPs. During these years, technology-based solutions would stand out as one of the only areas in which the scholars studied continued to hold a wide range of opinions.

This Chapter proceeds in a similar fashion to Chapter II. The objective of Section A is to immerse the reader into the sociotechnical and techno-legal context of the 2000-2007 period, *as seen through the lens of the scholars here studied*. For that purpose, details are provided about the data collection, processing, and use techniques that were considered more relevant by the scholars during this period, the societal attitudes that surrounded these technological advancements, and the various ways in which the American legal system responded to them. Having done that, in Section B I present the harms that scholars writing during these years considered most significant, as well as the privacy tools they would offer between 2000 and 2007 in order to address them.

## A. Context

The purpose of this Section is to place the reader in the technological, social, and legal context in which the American privacy law scholars reviewed for this study were writing between 2000 and 2007. For doing so, in the next pages I review the main information technologies and practices of this period, the most salient societal attitudes developed in response to them, and the legal frameworks that were in place or being discussed during those years. As a result, this Section offers a general overview of the multiple sociotechnical and techno-legal factors which may have influenced these scholars' thinking during the covered years.

As in the previous Chapter, it is important to emphasize that the overview offered here is presented *through the lens of the scholars reviewed for this study*, and therefore, does not necessarily guarantee the accuracy of their perceptions and visions.

## 1. Information technologies and practices

According to Gaia Bernstein, "between 2000 and 2003, the U.S. online population expanded from eighty-six million in 2000, to one hundred and twenty-six million in 2003. In 2001, 56% of adults in the United States used the Internet, while by 2003, 63% of American adults were online" (2006b, p. 274). Thus, as the 21st century dawned, American privacy law scholars were seeing the growing expansion of cyberspace.

As years passed and scholars gained a better understanding of the practices that had emerged in the framework of the "information society" (see Chapter II), their focus gradually shifted from computers and networks to the flow of personal information across them. As Tal Zarsky (2004a), Neil Richards (2005), and Daniel Solove (2006a) would similarly pose during these years, "the entire flow of personal information can be divided into three distinguishable segments: (1) the *collection* of personal information regarding relevant individuals; (2) the *analysis* of the information collected and (3) the *use and implementation* of the analyzed information for the benefit of the database holders" (Zarsky, 2004a, p. 17). More than on the technologies *per se*, during the period under study scholars would devote more attention to the journey of personal information through these three phases.

### 1.1. Collection of information: Online tracking and other technologies with invasive capabilities

In terms of collection, since the late 1990s scholars had referred to the use of "cookies" in the context of e-commerce (Berman & Mulligan, 1999). However, during the years to come, they got to comprehend and highlight multiple other ways of online collection of personal information. As a result, time and again scholars (Blanchette & Johnson, 2002; Bresnahan, 2000; Debusseré, 2005; Evans, 2007; Garrie & Wong, 2006; Hetcher, 2000b; Kerr, 2001; Lin, 2002; Nehf, 2003; Reidenberg, 2000; Solove, 2002a) would bring up a classification similar to the following: "Currently, there are two basic ways personal information is collected in cyberspace: (1) by directly collecting information from users (*registration* and *transactional data*); and (2) by surreptitiously tracking the way people navigate through the Internet (*clickstream data*)" (Solove, 2001, p. 1411). Comparing *transaction data* versus *clickstream data*, in 2000 Joel Reidenberg would comment:

> the surveillance aspect of clickstream data is also qualitatively different from earlier forms of transaction data. The *detail* offers a picture that was previously not readily compiled. While the depth of information available from clickstream data might have been obtainable with a private investigator recording an individual's every move, such surveillance would have been treated as harassment. In the past, privacy was preserved from the isolation of discrete bits of information. The difficulty in assembling such information provided protection to individuals. *Clickstream data break down this protection*. (Reidenberg, 2000, p. 1322)

Likewise, regarding clickstream data, scholars would also refer to the different types of mechanisms that, besides cookies, were being used by companies to surreptitiously track users online, including web bugs (Bernstein, 2006a, 2006b; Cohen, 2001; Peek, 2003, 2003; Schwartz, 2000a) and spywares (Barnes, 2006; Bernstein, 2006a, 2006b; Schwartz, 2004).

In addition to online tracking technologies, authors writing during this period would also identify additional sources of information about Internet users, including digital rights management ("DRM") systems used as strategies of copyright enforcement and which had been already noted by Julie Cohen since the previous decade (Cohen, 1996) (Cohen, 2002, 2003; Froomkin, 2000b; Hoofnagle, 2004; Katyal, 2004; Richards, 2006; Woodford, 2004); Internet public discussion groups such as USENET and listserv (Kerr, 2001); and web logs—"blogs"—(Byers, 2007; Evans, 2007; Hong, 2007; Kirkland, 2006; Lichtenstein & Darrow, 2006; Rita & Gunning, 2006; Solove, 2003a; Swaya & Eisenstein, 2005).[50] By the end of the studied period, pioneer scholar Patricia Sanchez Abril would also talk about online social networking sites (OSNs) such as MySpace, Facebook, and Friendster (Sanchez Abril, 2007a, 2007b). According to her,

> In the past five years, OSNs have exploded in popularity. Although the term "social networking" can describe many frameworks, the term usually refers to *websites whose main purpose is to act as a connector between users*. The primary species of this cyber-genus is websites that facilitate communication via user-generated Web profiles that can include personal information, music, pictures, links, video clips, real-time transcripts of conversations, and often-colorful self-musings. (Sanchez Abril, 2007b, p. 13)

Furthermore, scholars would refer to other technologies that, although not necessarily used on the Internet, were also facilitating the collection of raw personal information ("information-gathering technologies" (Lin, 2002, p. 1103)). According to Michael Froomkin, for instance, these technologies would include:

> (…), growing automated surveillance in public places, deployment of facial recognition technology and other biometrics, cell-phone tracking, vehicle tracking, satellite monitoring, workplace surveillance, (…), hardware-based identifiers, (…)

[50] In Matthew E. Swaya & Stacey R. Eisenstein's words, "[w]eb logs, otherwise known as blogs, are essentially journals and diaries posted online that discuss topics ranging from family to politics" (2005, p. 2). According to Elizabeth R. Rita & Eric D. Gunning, "the number of blogs worldwide has virtually exploded-from 23 recorded blogs in 1999 to more than 33.2 million blogs as of March 23, 2006, with a new blog created every second" (2006, p. 55).

> and sense-enhanced searches that allow observers to see through everything from walls to clothes. (Froomkin, 2000b, p. 1461)

In a similar way, in 2004 Helen Nissenbaum would refer to the following list of technologies "that expand[] the capacity to observe people," including among them "enhanced modes of gathering or capturing information as in automated road toll systems like EZ Pass, video surveillance and face recognition systems, (…), biometrics, thermal imaging, and more" (Nissenbaum, 2004, p. 122). Other authors, in turn, would talk about Closed Circuit TV ("CCTV") cameras (Koops & Leenes, 2005), camara phones (Kato Ku, 2005), and location tracking technologies. Regarding the latter, several scholars would specifically point out to the use of global position satellite ("GPS") systems by employers to track off-duty movements of employees (Cuijpers, 2007; Evans, 2007; Herbert, 2006; Swaya & Eisenstein, 2005; Yung, 2005) and of radio frequency identification ("RFID") tags by manufacturers and retailers (Brito, 2004; Herbert, 2006; Hildner, 2006; Nissenbaum, 2004; J. E. Smith, 2007; L. S. Smith, 2006; Surden, 2007).

As seen, the tracking technologies used on the Internet would not be the only sociotechnical systems that would be collecting individuals' persona information during these years. Rather, technologies with incorporated cameras, location tracking capabilities, and biometric systems were also being increasingly spotted by American privacy law scholars writing between 2000 and 2007.

### 1.2. Analysis of information: Data merging and mining

Regarding the analysis of the information collected, scholars writing during this period would emphasize the actors' ability to merge data from several sources—including public records being transformed from paper-based to electronic and linked to the Internet (DeVries, 2003; Nehf, 2003; Richards, 2005; Solove, 2002b; Winn, 2002)—to create massive electronic dossiers of individuals.

According to Jean-François Blanchette & Deborah G. Johnson, "[o]nce collected, [transaction-generated information] TGI is easily aggregated and correlated with other kinds of data: Web browsing, demographics, credit card transactions, and cellular use together *provide a much finer resolution of the digital persona than each can by itself*" (2002, p. 39). In particular, several scholars (Nehf, 2003; Solove, 2001) would highlight ad-placement network DoubleClick's "ability not only to track users' clickstream as they travel from site to site, but also to be able to *link the data gathered online with an offline data source*" (Givens, 2000, p. 352).

Two aspects about this cross-correlation capacity were especially salient for scholars during these years. First, the diminishing costs of computing and storage (Citron, 2007; Cuaresma, 2002; Froomkin, 2000b; Lin, 2002; Reidenberg, 2000; Winn, 2002). As Danielle Keats Citron would describe in 2007, "[j]ust as data processing has rapidly advanced, so has the storage of information. In the past two years, the country's largest databases have tripled in size, while data collection costs have fallen by half" (2007, p. 247). Second, the growing use of data mining applications—which existence had already been announced by some scholars in the previous decade (Cohen, 1996; Froomkin, 1996a; Nissenbaum, 1998)—to infer additional information or to make predictions about individuals (Hirsch, 2006; McClurg, 2003; Peek, 2003; Solove, 2007; Solove & Hoofnagle, 2006; D. J. Steinbock, 2005; Westin, 2003; Zarsky, 2003, 2004a, 2004b). According to Tal Zarsky, for example,

> Data mining is *the enhanced ability to analyze vast amounts of personal information*. The data mining tools, also known as Knowledge Discovery in Databases, or KDD applications, *search for patterns and clusters within datasets*, without receiving a hypothesis from the analyst and do so in an almost fully automated process. The availability of data mining tools changes the information landscape, as it allows the user to derive more knowledge from less data. (Zarsky, 2004b, p. 995)

Additionally, in 2006 Daniel J. Solove & Chris Jay Hoofnagle would add the following distinction:

> *Subject-based data mining* involves analyzing records where a specific individual or individuals are identified and there is particularized suspicion that they are involved in criminal activity. *Pattern-based data mining* presents greater difficulties. Prospective pattern-based data mining involves analyzing record systems for various suspicious patterns of activity and then investigating those individuals who meet the particular pattern or profile. (Solove & Hoofnagle, 2006, pp. 378–379)

Thus, scholars would become more sophisticated in their understanding of these technologies over time, not only beginning to distinguish between transactional data and clickstream data, but also between subject-based and pattern-based data mining techniques.

### 1.3. Use and implementation of analyzed information: Computer profiling, personalization, and database rental and sale

Finally, in terms of the "use and implementation of the analyzed information" (Zarsky, 2004a, p. 17), scholars would almost unanimously talk about "computer profiling" and "personalization" as the most common uses.[51] Referring to profiling, Marcy Peek, for example, would comment: "[t]his ability to profile Internet users is perhaps one of the most significant, yet ignored consequences of the Internet and, indeed, of the Information Age" ( 2003, p. 94). Similarly, in Jennifer Bresnahan's words, "[p]ersonalization is the latest darling of the business world" (2000, p. 8). Interestingly, the novelty of these practices remarked by both authors strikingly contrasts

[51] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Allen, 2001; Barnes, 2006; Beckmann, 2001; Bresnahan, 2000; Cohen, 2003; Culnan & Bies, 2003; Garrie & Wong, 2006; Hirsch, 2006; Lin, 2002; McClurg, 2003; Nehf, 2003; Nissenbaum, 2004; Reidenberg, 2000, 2002; Richards, 2005; Solove, 2002a; Sovern, 2001; D. J. Steinbock, 2005; Zarsky, 2003)

with the many ways in which the concepts of "profiling" and "personalization" are used in common jargon today, as well as assumed by many scholars to occur almost everywhere.

At the time, however, several scholars would take the space and time to explain how, by creating highly detailed personality profiles on individual consumers, Internet companies could deliver tailored services to their users. "The company will utilize technology to customize its site according to what it knows about the visitor. Companies can also send personalized, interactive email messages, urging individuals to reconsider a product they lingered over during their last visit to a website" (Bresnahan, 2000, p. 10). In addition, scholars would also highlight how personal profiles provide "much greater targeting capabilities for advertisers" to conduct targeted marketing. According to Daniel Solove,

> This revolution in targeting technology is possible because web pages are not static like magazine pages. They are generated every time the user clicks. Each page contains spaces reserved for advertisements and specific advertisements are download into those spots. The dynamic nature of web pages makes it possible for a page to download different advertisements for different users. (Solove, 2001, p. 1410)

Furthermore, another use commonly referred to by scholars during these years—and announced as the "flourishing personal data market" by some of them since the previous decade (Nissenbaum, 1998; Reidenberg, 1995; Shorr, 1995; Schwartz, 1999)—was the renting and selling of databases (Bresnahan, 2000; Lin, 2002; Litman, 2000; Moshell, 2005; Nguyen, 2004; Nissenbaum, 2004; Rule, 2004; Schriver, 2002; Schwartz, 2004, 2000a; Solove, 2001, 2002b; Solove & Hoofnagle, 2006). According to Jolina C. Cuaresma, for instance, "[i]nformation itself is a product that has monetary value. Some firms that profile their consumers will use the same data to compile marketing lists. These lists are then sold to other merchants to augment traditional sources of income" (2002, p. 506).

## 2. Societal attitudes

Just like Jeff Sovern (1999) and Anita Allen (1999a) had started to point out by the end of the twentieth century (as described in Chapter II), between 2000 and 2007 scholars would report how societal attitudes about privacy were mostly ambivalent. Thus, while polls would keep showing society's concern about the increasing lack of privacy, individuals would continuously use the Internet to expose themselves to others.

### 2.1 Worries about the increasing lack of privacy

During this period scholars would repeatedly claim that "there is no question that people want privacy. Surveys show that people are concerned about their growing lack of privacy" (Cuaresma, 2002, p. 515). For instance, they would cite surveys reported by the FTC in its 2000 Report *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress*, which had found that "67% of consumers were 'very concerned' and 92% 'concerned' about the misuse of their personal information online." In addition, "82% of online households believe that government should regulate the use of personal information online, and 92% do not trust online companies to keep this information confidential" (Blanke, 2000, p. 74).

Citing a 2001 Harris Interactive survey, Mary J. Culnan & Robert J. Bies would claim that "a strong majority of online users have refused to provide information or have decided not to purchase something from a company because they weren't sure how their personal information would be used. Further, more than 40% avoided visiting specific Web sites because of dubious privacy practices" (Culnan & Bies, 2003, p. 332). Similarly, in 2002 Lawrence O. Gostin & James G. Hodge Jr. would report: "Over 80% of respondents in one survey suggested they had 'lost all

control over their personal information.' In another national survey, 78% of respondents felt it is very important that medical records be kept confidential" (Gostin & Hodge, Jr., 2002, p. 1440). Likewise, Elbert Lin would highlight: "[a]ccording to the Pew Internet & American Life Project, fifty-four percent of Americans consider online tracking a 'harmful invasion of privacy'" (Lin, 2002, p. 1107). And when it came to health privacy, the panorama would not be different. In 2007, for instance, Sharona Hoffman & Andy Podgurski would report:

> A 2005 National Consumer Health Privacy Survey, which queried 2000 people, revealed that sixty-seven percent of respondents were "somewhat" or "very concerned" about the confidentiality of their medical records. Furthermore, thirteen percent of respondents claimed that they had attempted to protect their own privacy by avoiding medical tests or visits to their regular physicians, asking doctors to distort diagnoses, or paying for tests out-of-pocket so that no medical documentation would be sent to insurance companies. (Hoffman & Podgurski, 2007, p. 335)

Although some other accounts were different (e.g., Nguyen, 2004), Alan Westin would report how, even after the 9/11 terrorist attacks, individuals' concerns for consumer privacy would still remain high. According to Westin,

> While 9/11 altered citizen-government privacy balances into the foreseeable future, *consumer privacy issues have remained essentially the same*; *increased trust in government has not been matched by any increased trust in business*. A survey of Internet users in early 2002 found that 87% were still concerned about privacy threats when they went to shop or seek information online (Harris Interactive & Westin, 2002a). When asked how the 9/11 events affected their views of consumer privacy issues, *74% said they remained as concerned as before and 26% said they were even more concerned now. Only 1% said they were less concerned*. (Westin, 2003, p. 449)

Evidently, this profound sense of unease about private companies was underlined by a wide range of data privacy scandals that took place over these years. As Westin himself would also point out, "[w]hile customized marketing helped link business offers to individualized lifestyles and interests, expanded mail marketing and especially telemarketing in the 1990s drew increased

consumer annoyance. And, the mass media continued negative coverage of what was portrayed as privacy-intrusive business marketing" (Westin, 2003, p. 442).

### 2.1.1. Scandals

One of the media-covered privacy wrongs most cited by scholars (e.g., Bernstein, 2006b; Culnan & Bies, 2003; DeVries, 2003; Litan, 2001; McClurg, 2003; Reidenberg, 2002; Rotenberg, 2001; Schriver, 2002; Siebecker, 2003; Solove, 2001; Zarsky, 2004a) between 2000 and 2007 was that of Doubleclick, which—as mentioned earlier— became famous for tracking users' clickstream across websites to profile individual uses and deliver targeted advertisement. This practice, by itself, raised criticism among consumers. However,

> [w]hat made many people especially nervous—and what triggered federal and state investigations—was a plan the company announced in early 2000. The company intended to *marry the data it compiled online about the behavior of individuals on their computer with offline information obtained in a merger with offline direct marketer Abacus*. This combination would have enabled DoubleClick to link the computer user with his or her personal identity. Under the of protest that followed, the company backed away from that plan. (Litan, 2001, pp. 1064–1065)

Another scandal that was popular among this period's active scholars (e.g., Allen, 2001; Beckmann, 2001; Schriver, 2002; Spencer, 2002) also happened at the beginning of the 21st century, but in the framework of the dot-com crash. In this case, the Internet retailer Toysmart.com filed for bankruptcy and announced that it would sell its database of customer information as an asset. As Richard A. Beckmann reported,

> [t]he issue received attention from consumer groups, regulatory and legislative arms of federal and state governments, and national media (…) [and] *was vigorously opposed* in both the courts of law and public opinion *as a violation of Toysmart's privacy policy*. Toysmart subsequently abandoned the plan, at least temporarily, thereby eliminating the immediate need for judicial resolution of the conflict. (Beckmann, 2001, p. 765)

Finally, a third scandal spotted by scholars (e.g., Allen, 2003; DeVries, 2003; Farmer, 2003; Solove, 2007; Solove & Hoofnagle, 2006) during this period was related to what came to be known as the "Total Information Awareness" (TIA) program. Following the 9/11 terrorist attacks, the Defense Department announced that it was working on a project to link data from independent electronic databases from businesses (e.g., credit card purchases, e-mails, travel itineraries) and apply sophisticated computer data-mining techniques in order to identify potential terrorists and predict future terrorist attacks. Nevertheless, similar to what happened with other scandals, "[w]hen the program came to light, a public outcry erupted, and the U.S. Senate subsequently voted to deny the program funding, ultimately leading to its demise" (Solove, 2007).

Interestingly, of all the technologies and practices employed at the time for the collection, analysis, and use of data, data merges seem to have caused the most controversy in American society at the time. And given these recurrent public outcries, during these years scholars would generally forecast that "in this century, the general societal yearning for a retrieval of the 'right to be let alone' will grow steadily more intense" (Smolla, 2002, p. 322).

### 2.2 Continuous exposure of individuals' personal information online

These same scholars, however, would also report how, despite the worries and cries mentioned above, in their day to day life individuals used the Internet to make themselves accessible to others (Allen, 2000b; Kang & Buchner, 2004; Sanchez Abril, 2007a), kept sharing their personal information online (Bresnahan, 2000; Givens, 2000; Haynes, 2007; Westin, 2003), and would not adopt privacy enhancing technologies such as cookie management systems (e.g., P3P) and anonymizer software to protect their privacy (Bernstein, 2006b).

As Ann Bartow, for example, would recognize, "[i]n the abstract, many of us may be concerned about personal privacy, but when we are out swimming the web, this concern may be overshad owed by a desire to participate fully in online life" (2000, pp. 635–636). In fact, in 2004 Paul Schwartz would contend that "[a] strong conception of personal data as a commodity is emerging in the United States, and individual Americans are already participating in the commodification of their personal data" (2004, p. 2057). In a similar way, in 2006 Gaia Bernstein would claim: "non-privacy norms related to the collection of personal information have become entrenched among the Internet's commercial users. The entrenchment of non-privacy norms among commercial users occurred rapidly" (2006a, pp. 274–275). And, as an example of this, they would repeatedly point to the "reality-TV shows, blogging, and live broadcasting of mastectomy and birth" that at the time would be part of what some of them would refer to as "our modern 'culture'" (Kang & Buchner, 2004).

Likewise, despite the manifested concerns about the pervasiveness of the data collection practices, scholars would also highlight how Americans would not necessarily have a preferred type of intervention or solution—if any. According to Bartow, for example, "even if the government could be persuaded to protect consumer data, it is uncertain what the scope and nature of that protection would ultimately be. Not everyone is comfortable having the government make decisions about who gets access to our personal information" (2000, p. 672). Similarly, in 2000 Julie Cohen would point out: "There is much disagreement about what comes next, but there is also a growing (if still inchoate) consensus that something needs to be done" (2000, p. 1375).

In striking contrast, scholars writing during this period would attribute the identified paradox to reasons very different from those Anita Allen (1999a) had considered by the end of the twentieth century. While in 1999 Allen's offered reasons had mostly revolved around the affordances offered

by new technologies for people to share their lives with others, during these years scholars would rather attribute this phenomenon to the lack of understanding that Americans had about: (i) the reach and extent of their privacy rights; as well as (ii) the scope and intricacy of personal information collection and use by commercial entities..

According to Beth Givens, for example, "I have observed that many consumers believe they have far more protection in law than they actually do, whether it's a real-world experience they are describing or an on-line experience. They often say to me, 'There's a Privacy Act you know, and I have rights'" (Givens, 2000, p. 353). Similarly, when it came to workplace privacy, Peter J. Isajiw would highlight how "[s]tudies also show that most employees believe that their e-mails are private" (Isajiw, 2001, p. 75). Relatedly, "it appears that individuals are unaware of the scope and intricacy of personal information collection and use of such information by commercial entities on the Internet" (2006b, pp. 274–275), Gaia Bernstein would argue. Others, in turn, would attribute this paradox to Americans' recognition of "the multitude of benefits resulting from more efficient government, business, and law enforcement functions when information in digital form is readily accessible" (Nehf, 2003, p. 4).

### 3. Legal system

Similar to the 1990s decade, in the early 2000s scholars would keep condemning the lack of comprehensive privacy protection in the US legal system (Blanke, 2000; Bresnahan, 2000; Cuaresma, 2002; Culnan & Bies, 2003; DeVries, 2003; Nehf, 2003, 2005; Reidenberg, 2002; Schriver, 2002; Wesche, 2002). As well, they would continue to make comparisons between the US and Europe, where stricter regulations had been enacted through the European Union's Directive on Data Protection, which became effective in 1998 (Bartow, 2000; Bignami, 2005;

Blanchette & Johnson, 2002; Givens, 2000; Reidenberg, 2000; Rothstein, 2000; Rule, 2004; Samuelson, 2000; Wakana, 2003).

As Julia M. Fromholz would claim in the early 2000s, "[i]n the European Union ('EU'), governments have moved aggressively to regulate the use of personal data. In the United States, on the other hand, the government has largely refrained from such regulation, instead allowing companies and associations to regulate themselves, save for a small number of narrowly drawn regulations targeting specific industries" (Fromholz, 2000, p. 461). In particular, many scholars would lament the US's failure to regulate the use of personal information by the direct marketing industry (Bernstein, 2006a; Givens, 2000).

At the same time, during these years scholars would also recognize "the climate of frenzied regulatory activity in the privacy arena" (Allen, 2001, p. 770) that had started to emerge since the mid-1990s, as well as the rising role of the FTC as a key player in the American privacy law landscape. Finally, many of them would begin to provide evidence of the inefficacy of some of the self-regulatory tools (e.g., "Privacy Seals") that had arisen since the previous studied period.

### 3.1. Frenzied legislative efforts

As announced in Chapter II, legislative efforts undertaken since the mid-1990s culminated in the enactment of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Children's Online Privacy Protection Act of 1998 ("COPPA"). Additionally, by the end of the 1990s-decade Congress also sanctioned the Gramm-Leach-Bliley Act of 1999 ("GLBA"). While due to its timing this latter act was not covered by the scholars publishing articles between 1990 and 2999, the scholars reviewed in the present Chapter did extensively refer to it (Allen, 2003;

Cuaresma, 2002; Janger & Schwartz, 2002; McGeveran, 2003; Schriver, 2002; Swire, 2002). As Peter Swire would explain in 2003 with regard to these three statutes,

> The political rationale for moving first on this sensitive data is easy enough to see—it was easier to get political consensus that there should be binding, legal protections for the most sensitive types of information, and there was general agreement that children's, financial, and medical records qualified as sensitive. By contrast, there was less consensus that information collected by web sites over the Internet was inherently sensitive. (Swire, 2003, p. 867)

In addition, during these years some scholars would also acknowledge Congress' amendment of the Family Educational Rights and Privacy Act ("FERPA") (Daggett & Huefner, 2001; Salzwedel & Ericson, 2003), as well as the introduction of several bills, including: (i) the Notice of Electronic Monitoring Act ("NEMA") (Court & Warmington, 2004; Watson, 2001), which if enacted into law would have impacted workplace monitoring of employee communications and computer use; and (ii) the Online Privacy Protection Act ("OPPA") (Hetcher, 2000b; Levin & Nicholson, 2005), which would have required the FTC to issue regulations to protect the privacy of individuals not covered by COPPA. Finally, other scholars (Brito, 2004; L. S. Smith, 2006) would also highlight the legislative endeavors taking place at the state level, where "hundreds of new consumer privacy laws were enacted each year in 2000 and 2001, with coalitions of Republican and Democratic political leaders uniting to reflect the privacy concerns of suburbanites, women, Internet users, and other desirable local constituencies" (Westin, 2003, p. 446).

### 3.2. Federal agencies' rising initiatives

Besides legislative actions, during this period scholars would also praise federal agencies' efforts to issue regulations to implement the recently passed laws. For example, the FTC adopted the

COPPA rule, which went into effect in April 2000 (Jamtgaard, 2000). Similarly, in order to implement the Gramm-Leach-Bliley Act, in May 2000 the FTC also promulgated the Privacy of Consumer Financial Information Rule, while the Federal Financial Institutions Examination Council ("FFIEC") agencies issued the "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" (DeVries, 2003; Schriver, 2002; Singh, 2006).

As it might be remembered, HIPPA's 1996 sanction was not highly remarked by the scholars reviewed in the previous Chapter. Several scholars writing between 2000 and 2007 would however highlight the fact that in December 2000, the U.S. Department of Health and Human Services ("HHS") issued the Federal Privacy Rule under HIPAA (Gostin et al., 2002; Hoffman & Podgurski, 2007; Pritts, 2002; Winn, 2002). Referring to this Rule, in 2003 Alan Westin would extol how, in early 2001, President Bush turned down industry requests to postpone and reconsider the Rule, "demonstrating the political force of the public's new privacy attitudes" (Westin, 2003, p. 447).

Also, many scholars writing during this period would refer to the newly Safe Harbor agreement reached between the US Department of Commerce (DOC) and the European Union in 2000 (Blanke, 2000; Fromholz, 2000; Jamtgaard, 2000; Swire, 2005; Westin, 2003; Whitmant, 2004). As approved, this Safe Harbor provided a framework through which American businesses who agreed to abide by a set of privacy-protection principles would be deemed to provide adequate protection, and therefore, would be allowed to conduct transatlantic data transfers. On this last point, however, in 2003 Alan Westin would note that "as of mid-2002, only about 200 U.S. companies, mostly smaller firms, had signed on to Safe Harbor, and they signed on mostly for transferring personnel data" (Westin, 2003, p. 447).

When it came to the FTC, during these years the scholars evaluated the agency's increasing privacy actions in a mixed manner. On the one hand, many scholars would emphasize the Commission's indecision in requesting Congress to enact privacy legislation (Bartow, 2000; Blanke, 2000; Hetcher, 2000a). As several commentators would report, in its 1998 Report to Congress the FTC "threatened to recommend to Congress that it enact privacy legislation, if more respectful industry customs and usages were not forthcoming through industry self-regulation" (Hetcher, 2000a, p. 2047). In its 1999 Report, in turn, the agency concluded that legislation mandating greater privacy protection was "not appropriate at this time." However, in its 2000 Report, the Commission changed its posture again, recommending the enactment of a federal Internet privacy statute based on the following four Fair Information Practices Principles (FIPs): notice, choice, access, and security. Finally, as a new administration came in, "the new FTC Chairman, Timothy Muris, announced that the agency would seek to expand enforcement of *existing* laws rather than call for new legislation" (Schriver, 2002, p. 2799).

On the other hand, scholars would also highlight the FTC's active role in correcting misbehavior in information practices (Allen, 2001; Jamtgaard, 2000; Schriver, 2002; Sovern, 2001). According to Steven Hetcher, for example,

> [i]n 1995, the FTC was asked by Congress to investigate the privacy risks associated with computer databases. The Agency has been increasingly involved with electronic privacy issues ever since. It has held *workshops* to bring industry participants together with privacy advocates in an attempt to encourage self-regulation. It has *set up a website* to provide consumers with information on industry data-gathering practices, and to instruct consumers on measures they may take to be proactive about protecting their individual privacy. By far, however, the greatest amount of attention has been toward promoting the emergence of an industry-wide practice of establishing website privacy policies. The FTC has *made the website industry aware that the Agency views privacy policies as a key element of self-regulation*. (Hetcher, 2000a, pp. 2046–2047).

In addition to these business guidance activities, authors would repeatedly refer to several privacy-based investigations against private companies that the FTC conducted during this period, following its historic enforcement action against GeoCities (Allen, 2001; Beckmann, 2001; Cohen, 2000; Nguyen, 2004; Schriver, 2002; Solove, 2003b). As reported by scholars, pursuant to its authority under section 5 of the FTC Act, which mandates that the Commission address unfair and deceptive trade practices, in July 2000 the FTC filed its first enforcement action under COPPA. Filling it against Toysmart.com, in the case the FTC would allege that the company's announcement to sell its customers' information was contrary to the representation made in its privacy policy. Relatedly, the year after the FTC

> announced the settlements of its first line of civil penalty cases brought under COPPA. Monarch Services, Inc. and Girls Life, Inc., operators of www.girlslife.com; Bigmailbox.com, Inc., and Nolan Quan, operators of www.bigmailbox.com; and Looksmart Ltd., operator of www.insidetheweb.com, were charged with violating COPPA by illegally collecting personal information from children under thirteen. (Allen, 2001, p. 766)

Moreover, in September 2001, the FTC also filed suit against Lisa Frank, Inc., for violating COPPA and section 5 of the FTC Act by making false or misleading statements about parental consent on its privacy policy. In February 2002, in turn, it filed suit against American Pop Corn Company for collecting personal data from children without parental consent. Finally, in a case against the pharmaceutical company Eli Lilly, the FTC did not only look to ensure that the companies' data practices were in line with the their privacy policies, but also "begun to require greater security as part of its settlements" (Solove, 2003b, p. 1272). As a result,

> [a]s of August 2006, the FTC had brought actions resulting in eighteen consent agreements or stipulated judgments pursuant to the Unfair Trade Practices Statute (Section 5 of the FTC Act), five actions under the Fair Credit Reporting Act, and eleven actions pursuant to the Children's Online Privacy Protection Act ("COPPA"). Other enforcement actions have been brought by the FTC for failure to provide adequate security of online personal information in violation of websites'

> own representations that the information would be treated in a secure and safe manner, a violation of Section 5 of the FTC Act. And a number of enforcement actions have been brought against companies for sharing, renting, or selling personal information in violation of promises in online privacy policies, but only where there is such a promise. (Haynes, 2007, pp. 603–604)

As will be seen in Chapter IV, the remarkable reach of these enforcement actions would lead Daniel Solove & Woodrow Hartzog to write two different articles (Solove & Hartzog, 2014; Hartzog & Solove, 2015) on the scope and potential of the FTC privacy jurisprudence, describing it as "the broadest and most influential regulating force on information privacy in the United States—more so than nearly any privacy statute or common law tort" (Solove & Hartzog, 2014, p. 585-586). Nevertheless, between 2000 and 2007 not all scholars were of that opinion yet. Thus, while a few scholars would indeed celebrate this trade practice theory approach—mainly based on the FTC's monitoring of privacy policies—(Hetcher, 2000b, 2000a; Schriver, 2002), even describing the commission as a "website privacy 'norm entrepreneur'" (Hetcher, 2000a, p. 2046), others would criticize it as narrow, limited, inadequate, and unsatisfactory, over-focused on transparency, and ineffective to address harmful practices such as commercial profiling or data leaking (Citron, 2007; Cohen, 2003; DeVries, 2003; Gellman, 2003; Reidenberg, 2002; Wakana, 2003).

### 3.3. Increasing but ineffective self-regulatory efforts by Internet businesses

During this period, many scholars would point out how, in response to the FTC's approach to enforcement, the DOC's Safe Harbor, and multiple survey findings and negative media coverage, many Internet businesses had voluntarily decided to adopt or revise their privacy policies and to implement new internal mechanisms to comply with the Safe Harbor (Bernstein, 2006b; Givens, 2000; Hetcher, 2001; Swire, 2003; Westin, 2003). Likewise, looking to build consumer trust and

stand out among competitors, companies would also continue joining third-party "Privacy Seal" programs, promising to subscribe to a set of privacy principles proposed by the seal providers (Bartow, 2000; Beckmann, 2001; Bernstein, 2006b; Fromholz, 2000; Froomkin, 2000b; Litan, 2001).

By the end of the period studied in this Chapter, however, certain scholars would also start to provide evidence of the inefficacy of some of these self-regulatory mechanisms. In 2006, for example, Dennis D. Hirsch would comment the following with regards to the Online Privacy Alliance (OPA):

> Subsequently, it became apparent that the OPA Guidelines would not be sufficient. Only a hundred or so companies and associations joined the group, with major players such as Amazon.com and Lycos choosing to remain on the sidelines. Pressure has again begun to build for federal regulation, leading even the OPA to conclude that it has "come up short." (Hirsch, 2006, p. 51)

***

In contrast to the previous period (see Chapter II), in which the emergence of the commercial internet and the proliferation of personal computers could be considered as revolutionary, the technological advances witnessed by the scholars discussed here were probably not the most representative events of the period reviewed. Rather, based on the sociotechnical and techno-legal context provided above, the 2000-2007 period can be characterized primarily by the rise of the FTC as a prominent player in the American privacy law environment.

To be clear, during these covered years the FTC's policy guidance and enforcement actions were not always positively judged by the scholars writing during those years. Yet, it is undeniable that, as a result of the increasing number of enforcement actions led by the agency during these years, by the end of the period the FTC had become increasingly visible to scholars.

Finally, the context provided for this period can also be described as one of growing ambivalence of American society about the value of privacy, which incipient roots had already been noted by Jeff Sovern (1999) and Anita Allen (1999a) by the end of the 1990s.

## B. American privacy law scholars' response

Considering this sociotechnical and techno-legal context, it is no surprise that the American privacy law scholars here studied would continue to focus their attention on relatively the same harms as they had highlighted in the previous studied period. In terms of their proposed privacy tools, however, the state of flux described in Chapter II would give way to a much more coordinated community, which during these years would be considering fewer alternatives than previously, and with stronger positions on the majority of them.

### 1. Identified harms

Like the 1990s, during the first few years of the 21st century (2000-2007) American privacy law scholars would continue highlighting the threats to individuals' control over their personal information as well as to their autonomy, as the two main privacy harms of the epoch. However, the nature and scope of these two harms would considerably change during this period.

#### 1.1. Modified threat to the individuals' "sense" of control: Lack of control over one's life

Between 2000 and 2007, scholars' perspective on the loss of individuals' control over their personal information would be highly influenced by Daniel Solove's framing of the situation in Frank Kafka's *The Trial* terms. According to Solove's 2001 article *Privacy and Power: Computer*

*Databases and Metaphors for Information Privacy*, "the problem [—which he would coin as the "database problem"—] is best captured by Franz Kafka's depiction of bureaucracy in The Trial—a more thoughtless process of *bureaucratic indifference, arbitrary errors, and dehumanization, a world where people feel powerless and vulnerable, without any meaningful form of participation* in the collection and use of their information" (Solove, 2001, p. 1398).

Thus, the loss of control that during these years Solove and his collogues would describe not only implicated that "consumers have very little ability to keep their personal information private, especially online" (Bartow, 2000, p. 634) (Litan, 2001; Schwartz, 2000a). Additionally, it would also include: (i) "'*control out of control'*—the fact that our personal information is not only out of our control but also is often placed within a bureaucratic process that lacks control and discipline in handling and using such information" (Solove, 2001, pp. 1444–1445); and (ii) the loss of the individuals' "ability to exercise meaningful control *over our lives*" (Solove, 2001, p. 1419). To pit this second situation another way, during these years there would be a shift in scholars' minds from loss of control *over one's data* to loss of control *over one's life.*

As framed by scholars writing during this period, this modified harm to the individuals' control (or "sense" of control, as it could be better framed here) has various related harms. First, several scholars would highlight the **lack of meaningful participation that individuals had in the decisions over the collection and use of their personal data** (Nehf, 2003; Reidenberg, 2002; Richards, 2005; Solove, 2001, 2007, 2002b, 2003b, 2006a). Joel Reidenberg, for example, would refer to this phenomenon as "the individual's non-participatory role in the treatment of personal information. Such a situation occurs when an individual has no opportunity to object to the processing of personal information or when participation is obtained under false pretenses"

(Reidenberg, 2002, p. 882). Likewise, in his 2006 *Taxonomy of Privacy* Solove would label this harm with the term "exclusion" (2006a).

Second, an impressive number of scholars would highlight how, as a consequence of this lack of participation from data subjects, individuals' personal information would be exposed to a wide array of **abuses and misuses** (Citron, 2007; Cohen, 2003; Evans, 2007; Haynes, 2007; Herbert, 2006; Hetcher, 2000b; Hirsch, 2006; Hoofnagle, 2004; Kesan, 2002; Lin, 2002; McGeveran, 2003; Reidenberg, 2002; Richards, 2005; Singh, 2006; J. E. Smith, 2007; Solove, 2001, 2007, 2002a, 2002b, 2003b; Solove & Hoofnagle, 2006; Winn, 2002; Zarsky, 2003, 2004a). Thus, during these years scholars would refer to harms such as identity theft, criminal impersonation, stalking, harassment, predation on children, unjustified interrogation and arrests, solicitation of contributions (in the case of campaign finance disclosures (McGeveran, 2003)), government profiling of political ideals, social ostracism, junk mail, blackmail, and corporate espionage. Likewise, in the workplace context, "[a]buse may also take the form of voyeurism, union-busting, ferreting out whistleblowers, and creating pretenses to fire members of protected employee groups" (Kesan, 2002, p. 320). Even, scholars would contend that this lack of participation and control could put at risk human relationships of "friendship, intimacy, and trust" (Nissenbaum, 2004, p. 149).

Besides, during this period scholars introduced two particular misuses that would become increasingly prevalent in the years to come. The first of these misuses was to use out-of-context—and sometimes inaccurate—personal information to make decisions with significant consequences over people' lives, resulting in the **denial of opportunities** such as jobs, loans, or licenses (Cohen, 2001; Hirsch, 2006; Nehf, 2003; Richards, 2006; Solove, 2001, 2001, 2006, 2002a, 2002b, 2003a; Zarsky, 2003; D. Steinbock, 2006; Sanchez Abril, 2007a; Solove, 2007). According to these

authors, although the information in databases fail to show a nuanced and complete picture of our lives, "this 'faceless infrastructure' employs the data to deny us jobs, credit, insurance, and other social goods, often without our knowledge" (Hirsch, 2006, p. 6); "[c]ommercial actors judge in order to determine the commercial treatment (including prices and terms) that an individual will receive. State actors judge in order to allocate public resources and to mete out (or withhold) civil or criminal sanctions. These are decisions with concrete consequences" (Cohen, 2000, p. 7); and "[w]atch listing can now deny visas, bar access to air travel, and block employment in certain transportation sectors" (D. Steinbock, 2006, p. 66). In a way, the emerging prevalence of these denials of opportunities would be the reason why, during these years, the scholars' approach to the loss of individual's control would shift—as explained—from loss of control *over data* to loss of control *over lives.*

The second—and related—misuse that would become very relevant in the next fifteen years was **the use of personal data to discriminate data subjects** (DeVries, 2003; Evans, 2007; Gostin & Hodge, Jr., 2002; Hildner, 2006; Kim, 2002; Koops & Leenes, 2005; Phillips, 2003; Schwartz, 2000b; Solove, 2002a; Zarsky, 2004a). As early as the 2000, Michael Froomkin would contend: "Among the possible harmful effects are *various forms of discrimination*, ranging from price discrimination to more invidious sorts of discrimination" (Froomkin, 2000b, p. 1469).

On the less offensive side of the spectrum, during these years Tal Zarsky (2003, 2004a) would indeed refer to the problem of **price discrimination**. In his view, "[t]his issue should be a dominant claim in any discussion concerning the regulation of the collection, analysis, use of personal information, and data mining especially" (Zarsky, 2003, pp. 26–27). Similarly, in the context of the collection of employees' data about off-duty activities, Laura Evans would contend that

"employer could also use employees' information to discriminate against employees should the data reveal personal attributes that the employer does not like" (Evans, 2007, p. 1116)

In turn, on the more invidious side of the spectrum—the Jim Crow type discrimination, Paul Schwartz (2000b), Marcy Peek (2003), and once again Zarsky (2003)[52] would refer to the by-then emerging practice of **"weblining,"** which would be commonly described as the online red-lining. According to Peek, "[r]edlining is understood as not only having a negative economic effect on the 'disenfranchised,' but also as creating a more subtle dynamic of 'stigmatization [that] decreases one's ability to secure basic rights of citizenship'" (2003, p. 104). For Schwartz,

> [t]he danger is that Weblining will hinder or even reverse the democratization of opportunity that Cate advocates. It goes far beyond the existing model for secured credit; it can be used to *restrict economic and informational possibilities for different groups and for individuals in a fashion that reflects and reinforces existing prejudices and mistaken beliefs*. (2000b, p. 757)

Similarly, when talking about personal health data, Lawrence O. Gostin & James G. Hodge Jr. would highlight how "[d]isclosure to employers or insurers (e.g., health, life, or disability) can result in discrimination" (Gostin & Hodge, Jr., 2002, p. 1442). Similar assertions would be done during this period by Pauline Kim (2002), Will Thomas DeVries (2003), and Radhika Rao (2006) but with regards to **genetic information**. According to Rao, for example,

> The danger is that individuals will be judged according to genetic stereotypes and divided into groups based upon their genetic predispositions. Thus, invasions of genetic privacy are not only selective, but also segmenting: they balkanize a population based upon its genes, generating genetic divisions that may produce new structures of inequality. (Rao, 2006, p. 828)

[52] Unlike Schwartz and Peek, though, Zarsky would not consider "weblining" as a specific consequence of the era of data mining and profiling. In fact, he would contend that "it is possible to view the effect KDD tools have on this matter of discrimination in a different light, and possibly find that the use of such applications should be encouraged, as they may be of great assistance in diminishing the negative effects of such discrimination and 'Weblining'" (Zarsky, 2003, p. 27).

However, it is important to mention that at that point in time not every scholar would agree with these concerns about genetic discrimination. In 2006, for example, Gaia Bernstein would claim that "the bulk of methodologically sound empirical research on discrimination by employers and insurers *points otherwise*. It overwhelmingly demonstrates that *genetic discrimination by employers and insurers is rare and is generally on the decline*" (2006b, p. 260).

Likewise, it is also important to note how, in these discussions about discrimination, Marcy Peek (2003) would move a step further, highlighting the related **subordinating and oppressive effect of discrimination**. According to Peek,

> Formalism as a jurisprudential mode of analysis views literal, formal, one-to-one equality as an end in and of itself. (…) The principles of anti-subordination and anti-oppression, rather than formalism, must be applied to the practice of online profiling to truly understand its oppressive aspects. Such principles allow us to avoid the mistake of "overlook[ing] structural disadvantage" and instead "call[] for equalizing treatment by redistributing power and resources in order to rectify inequities and to achieve real equality." (Peek, 2003, p. 108)

As a pioneer, Peek's approach was unique at the moment, and would only become popular during the second half of the twenty-teens.

### 1.2. Modified threat to individual autonomy: Reduction of the individual to a set of data points

Extremely interrelated with the modified threat to individuals' sense of control just explained, during the early 2000s scholars would also refer to the **individuals' sense of exposure, vulnerability, and frustration** resulting from this constant risk of abuse and misuse (Bresnahan, 2000; Nehf, 2003; Richards & Solove, 2007; Solove, 2001, 2002a, 2002b, 2003b). As a harm in itself, "[t]his reality creates a *sense of unease, vulnerability, and powerlessness*—a deepening sense that one is at the mercy of others, or, perhaps even more alarming, *at the mercy of a*

*bureaucratic process that is arbitrary, irresponsible, opaque, and indifferent to people's dignity and welfare*" (Solove, 2002b, p. 1194). Following Solove, James P. Nehf would similarly contend: "We are *at the mercy* of an unknowable digitized process-a world where people feel powerless and vulnerable" (Nehf, 2003, p. 3).

In the view of some scholars writing during this period (Cohen, 2001; DeVries, 2003; Koops & Leenes, 2005; McGeveran, 2003; Nehf, 2003), this sense (and state) of vulnerability could have detrimental consequences for the values of human dignity and freedom. Framed in this way, this harm would strongly relate to the threat to individual autonomy highlighted in scholarship in the 1990s. However, unlike those previous claims, which mostly identified the lack of "zones of 'relative insularity'" (Nissenbaum, 2004, p. 148) as the origin of this threat, during these years most scholars would point somewhere else, namely, to **the treatment of individuals as a simple collection of information that informs decisions about them**.

Will Thomas DeVries, for example, would contend that "[t]he underlying problem of informational privacy in the digital age is *the ability to access and aggregate vast amounts of otherwise harmless personal data into a form that can do real damage* to the individual's sense of self-determination and autonomy" (2003, pp. 307–308). Similarly, in Julie Cohen's view, "*[t]hese third-party judgments*, (…), necessarily affect both the process of individuation and the limits of autonomy. Autonomy is inescapably a function of context and a matter of degree" (Cohen, 2001, p. 7). Likewise, Bert-JaapKoops & Ronald Leenes would explain that "[a]n individual will feel harmed in her integrity because she feels less an individual, less autonomous, and less dignified *when society treats her as a collection of information fragments* rather than as an integral human being" (Koops & Leenes, 2005, p. 185). Thus, more than from a lack of spheres where a person can feel unobserved and insulated from outside scrutiny, during the years under study the threat to

autonomy would mostly come from the individual's reduction to a set of data points on which decisions were made.

To be clear, this is not to imply that, with the turn of the century, American privacy law scholars had forgotten about the traditional harm to autonomy. During the years under review several scholars would keep raising concerns about how public and private surveillance activities would not only threaten individuals' autonomy—in the sense of protected zones—(McGeveran, 2003; Reidenberg, 2002), but also have a **"chilling effect"** (Cohen, 2003; Froomkin, 2000b; Hoofnagle, 2004; Katyal, 2004; Mcdonald & Cranor, 2006; McGeveran, 2003; Richards, 2005; Sanchez Abril, 2007a) and ultimately harm **democracy** (Blanchette & Johnson, 2002; Nissenbaum, 2004; Sobel, 2002; Solove, 2002a; Zarsky, 2003). However, as explained previously, in the first decades of the 21st century scholars identified a second source of this threat, being it the reduction of individuals to a set of data points.

### 1.3. Sparse but visionary references to other harms/circumstances

Before concluding, it is worth mentioning that, during these years, Tal Zarsky (2003, 2004a, 2004b) would join the group of pioneer scholars—Joel Reidenberg (1995), Dorothy J. Glancy (1995), and Helen Nissenbaum (19970[53]—who back in the 90s had brough up **manipulation** as another possible harm in the "information society." According to Zarsky, "recent trends of convergence in the media market lead to the danger of the *'autonomy trap'*—the ability of content providers to influence the opinions and conceptions of individuals by providing them with tailored content based on the provider's agenda and the individual's personal traits" (Zarsky, 2004a, p. 30). In the years to come, more and more privacy law scholars would keep joining this group.

[53] And Lawrence Lessig, with his 1999 book *Code and Other Laws of Cyberspace*.

Likewise, during these years Solove (2001, 2007, 2002b, 2002a) and a few other scholars (Cuijpers, 2007; Nehf, 2003; Nissenbaum, 2004; Phillips, 2003; Schwartz, 2000a) would join the nascent group of scholars who, in the 1990s, had started to emphasize the existence of **power imbalances** between individuals and bureaucratic institutions. Writing in 2001, Solove would point out:

> One aspect of the problem is that *inequalities in power relationships* are increased significantly by the use of databases. The problem stems from a group of disempowering practices associated with databases. Affording more mutuality of access to information will do little to alter this power imbalance because information is much more of an effective tool in the hands of a large bureaucracy. Information is not the key to power in the Information Age— knowledge is. Information consists of raw facts. Knowledge is information that has been sifted, sorted, and analyzed. *The mere possession of information does not give one power; it is the ability to process that information and the capabilities to use the data that matters*. (2001, pp. 1456–1457)

As will be seen in the next two Chapters, as more scholars would become aware of the importance of paying attention to these power imbalances, the types of privacy tools proposed by this community would radically change during the next twenty years.

## 2. Proposed privacy tools

Unlike the previous studied period (1990-2000), when proposed privacy solutions were still in flux, between 2000 and 2007 scholars would start to agree in many fronts. As will be outlined in this Section, during these years most scholars united around a clear opposition to market-based solutions, and an openness to considering a diverse array of tort-based solutions. Likewise, during this period proposals for legally enacted FIPs—which came from the previous studied period—would receive overwhelming support. The only area where scholars would still have very different views in terms of proposed tools would be in their positions regarding technology-based solutions.

This, due in part to the wide range of technological solutions being considered at this time (Platform for Privacy Preferences ("P3P"), Self-Help Technologies, and Privacy Enhancing Technologies ("PETs")).

### 2.1. Backlash against market-based solutions

Unlike previous years, when certain scholars still trusted in the power of the industry's self-regulatory efforts, between 2000 and 2007 self-regulation was rarely supported by academics. Likewise, although some proposals would still come up for (traditional and intellectual) property rights (Bartow, 2000; Froomkin, 2000a; Rule, 2004) and contract law solutions (McClurg, 2006; McGeveran, 2001), these years could be characterized by a massive backlash against market-based solutions.[54]

Several scholars writing during this period would reject these proposals both on theoretical and practical grounds. On a theoretical level, scholars claimed that market-based approaches "treat preferences for informational privacy as a matter of individual taste, entitled to no more (and often much less) weight than preferences for black shoes over brown or red wine over white. But *the values of informational privacy are far more fundamental*" (Cohen, 2000, p. 1423). Likewise, they would highlight how these approaches—usually personified in scholar Lawrence Lessig's proposal covered in Chapter II, of a market solution that relied on technology (the Platform for Privacy Preferences (P3P)) to negotiate the price to be paid by the market—ignored the relevant history and evolution of the FIPs in the US (Rotenberg, 2001).

[54] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Cohen, 2000, 2001, 2003; Kang & Buchner, 2004; Koops & Leenes, 2005; Lewis, 2007; Litman, 2000; Nehf, 2005; Rao, 2006; Rotenberg, 2001; Solove, 2001, 2003b)

At a practical level, scholars would refer to the failures in the privacy market, due to—among other reasons—information asymmetries (Nehf, 2005). Besides, they would contend: "the problem with market solutions is not merely that it is difficult to commodify information (which it is), but also that *a regime of default rules alone* (consisting of property rights in information and contractual defaults) *will not enable fair and equitable market transactions in personal information*" (Solove, 2001, p. 1454). Finally, many scholars would tend to ask practical questions like:

> How can someone control a piece of personal data, once it is sold and part of the opaque data-merging market? How could data subjects control their data when confronted with "take it or leave it" contracts of powerful market parties? What will the administrative costs be of paying for use of personal data, perhaps on a royalty basis? And would such a system not require more processing of personal data in order to pay the data royalties? In short, *this approach ultimately fails*. (Koops & Leenes, 2005, pp. 196–187)

Thus, as will be seen next, only combined proposals—of the type of "market-based tools + another approach"—would survive this backlash era.

### 2.2. Strong support for legally enacted FIPs

Parallel to the aforementioned backlash against market-based solutions, during these years American privacy law scholars' faith in the power of legally enacted FIPs grew exponentially (Blanchette & Johnson, 2002; Cohen, 2000, 2003; Culnan & Bies, 2003; Gellman, 2003; Givens, 2000; Hetcher, 2001, 2000b; Hoofnagle, 2004; Jamtgaard, 2000; Janger & Schwartz, 2002; Reidenberg, 2002; Rotenberg, 2001; Solove, 2001, 2003b; Solove & Hoofnagle, 2006; Swire, 2003).

Outliers to this trend would obviously exist. Laura Hildner (2006), for example, would consider the idea of FIPs-based comprehensive privacy legislation as unrealistic given America's political

dynamics and unsuitable for technologies like the RFID. On this last point, Hildner would comment:

> FIPs *seem aimed at systems not entirely applicable to RFID*: ones with clearly identifiable data collectors whom consumers deliberately entrust with their information to facilitate a transaction. The aim then becomes making sure the data collectors are subject to meaningful restraints on using and sharing that information. RFID systems complicate this framework because *they allow anyone with a reader to become an undetectable data collector*. (2006, p. 163)

But aside from a few exceptions, examples of a general dispositionfor legally enacted FIPs abound. According to Beth Givens, for example, "there is a need for Congress to enact legislation that provides individuals with a baseline of privacy protection on the Net *by codifying the fair information principles*" (2000, p. 355). Similarly, in 2000 Julie Cohen would urge the enactment of data privacy legislation that, besides specifying the parameters for effective consent, would also include "non-consent-based requirements for fair information practice" (Cohen, 2000, p. 1435). Likewise, when referring to the Digital Rights Management ("DRM") systems, in 2003 she would contend:

> *More faithful adherence to the FIPs* would enhance the information privacy of users of copyrighted works and other information goods (…). Extending the full protection of the FIPs to all consumers is appropriate in an age in which personal profiling increasingly tracks not only purchases of durable goods but also private intellectual activities.

In a similar way, when talking about the "database problem," in 2001 Daniel Solove would claim:

> Unfortunately, in the United States the Fair Information Practices have only been selectively incorporated into various statutes in a limited number of contexts. *A more comprehensive incorporation of the Fair Information Practices*, as developed by HEW and expanded upon by the OECD and the European Union Privacy Directive, *would go far towards addressing the privacy problem as I have characterized it*. (2001, p. 1461)

Two years later, and taking into account the identified power imbalances pointed out above, Solove would even add:

> *Understood broadly, the Fair Information Practices establish an architecture that alters the power dynamic between individuals and the various bureaucracies that process their personal information*. The Fair Information Practices focus on two general concerns: participation and responsibility. They aim to structure the information economy so that people can participate meaningfully in the collection and use of their personal information. (…) Additionally, *the Fair Information Practices bring information processing under better control*. (…) The Fair Information Practices recognize that personal data processors have special responsibilities and that they must be regulated in order to ensure that they maintain accurate and secure records and use and disseminate information responsibly. (Solove, 2003b, pp. 1267–1268)

Accordingly, in their *Model Regime of Privacy Protection* published in 2006, Solove and Chris Jay Hoofnagle acknowledged having incorporated many of the FIPs, although specifically tailoring them to commercial data brokers (Solove & Hoofnagle, 2006, p. 358).

However, three trends would distinguish this call for FIPs-type laws from the claims heard during the 1990s. First, during the early 2000s some scholars would open the door for the **combination of legislated FIPs with other kinds of tools**. As anticipated in his 1999 article (Schwartz, 1999), in 2000 Paul Schwartz would, for example, open the door for property rights solutions, as long as they were preceded by a FIPs-based law. According to him,

> Recourse to Fair Information Practices (FIPs) offers the best way to establish rules for the fair treatment of personal data on the Internet. Yet, FIPs are not without potential shortcomings if structured only as command-and-control rules. Therefore, *an American Internet privacy law consisting of FIPs should include both mandatory and default elements* (Schwartz, 2000b, p. 787)

In Schwartz's view, while the FIPs-type mandatory rules would level the field and establish the unnegotiable rules, the existence of default rules would allow for private bargaining of the type Lawrence Lessig had envisioned (Janger & Schwartz, 2002; Schwartz, 2000b) and which Schwartz

himself would come to imagine in 2004 with his own "model of propertized personal information" (Schwartz, 2004, p. 2059). A similar view was shared at the time by Jean-François Blanchette & Deborah G. Johnson. According to them,

> our point is not to argue against the use of the market, but rather to emphasize the importance of structuring markets *to ensure that they promote data protection standards*. In other words, markets alone are not likely to achieve a desirable degree of data protection or social forgetfulness. However, *markets together with model standards articulated in the overarching general principles of a code of fair information practices* can support markets and facilitate the development of trust between consumers and companies. (Blanchette & Johnson, 2002, p. 41)

Besides Schwartz (2000b) and Blanchette & Johnson (2002), the case of Julie Cohen is also illustrative of another—although slightly different—type of combined mandatory FIPs+ solutions. As said earlier, in 2000 Cohen would urge for the enactment of data privacy legislation that included requirements for fair information practices. Nevertheless, in that same article Cohen would also be very clear about the fact that "[l]egal protection alone cannot create or guarantee informational privacy" (Cohen, 2000, p. 1438). For her, this proposed legislation should be accompanied by the development of privacy-protective technologies and design parameters, which the law should also incentivize and establish.[55] Likewise, in 2003 she would add: "For consumer protection law to provide meaningful protection for intellectual privacy (or any other kind of privacy), the proceduralist standards embodied in the FIPs must be augmented by *substantive privacy standards*" (2003, p. 603). As would be the case with many of her contributions, although sui generis at the moment, Cohen's claim for substantive standards—such as the EU's designation of certain kinds of sensitive information as off-limits, or the set of limits on the collection, use,

[55] In addition to ongoing regulatory oversight, as well as rulemaking.

retention, and trading of a certain kind of data—would become increasingly common in the second half of the twenty-teens (see Chapter V).

The second trend that would also distinguish this call for FIPs-type laws from that of the 1990s would relate to the scholars' particular focus on **digging into one of the FIPs principles, namely, choice/consent**.[56] In the sample of scholarship reviewed for the 1990s, Stephanos Bibas (1994) and Jeff Sovern (1999) were some of the few scholars, if not the only ones, to refer to the opt-in/opt-out categories. However, in the early 2000s several scholars would begin to grapple with this distinction. In most cases, scholars would recommend that legislators adopt an opt-in approach (Janger & Schwartz, 2002; Nehf, 2003; Schwartz, 2004, 2000b; Solove, 2001, 2003b; Spencer, 2002; Strandburg, 2005). According to James P. Nehf, for instance,

> regulation mandating that consumers opt-in rather than opt-out, for example, can in some circumstances achieve a more balanced approach to the disclosure of information. Opt-in systems place the incentive on entities that want to acquire personal information, in both the government and private sector, to make it as easy as possible for individuals to give meaningful consent to the collection and use of their information. (Nehf, 2003, pp. 67–68)

Yet, many of these academics would also qualify this consent, requiring it to be informed and "meaningful" (Bartow, 2000; Cohen, 2000; Nehf, 2003; Schwartz, 2004; Solove, 2001; Spencer, 2002). For Julie Cohen, for example, "consent cannot be meaningful as to unknown uses or unspecified recipients. In theory, effective data privacy legislation should require that individuals *be given specific information, and the opportunity to consent or refuse, as to each contemplated reuse or transfer*" (2000, p. 1433). For Daniel Solove, "effective privacy

[56] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Bartow, 2000; Cohen, 2000; Gostin et al., 2002; Gostin & Hodge, Jr., 2002; Janger & Schwartz, 2002; Kim, 2002; Nehf, 2003, 2005; Schwartz, 1999, 2004, 2000b; Solove, 2001, 2003b; Solove & Hoofnagle, 2006; Spencer, 2002; Staten & Cate, 2003; Strandburg, 2005; Zittrain, 2000).

regulation must require an opt-in system *which requires a meaningful range of choices as well as addresses inequalities in knowledge and power* and other impediments to voluntary and informed consent" (2001, p. 1459). And even under these circumstances, some scholars (Bartow, 2000; Janger & Schwartz, 2002; Schwartz, 2000a; Solove, 2003b) would still be skeptical about the consent figure's power to resolve individuals' inability to value their own data and recognize the harm that may result from relinquishing control. As will be seen in the next two Chapters, over time, this latter position would become more popular among American privacy law scholars.

As a final trend, many scholars aware of the fact that "[t]he effectiveness of the Fair Information Practices depends upon how they are applied to particular privacy problems and how they are enforced" (Solove, 2003b, p. 1238), would dedicate their academic pieces to **evaluate the operationalization of the FIPs in recently passed legislation**, such as COPPA (Allen, 2001; Solove, 2001; Stuart, 2005), HIPAA (Gostin et al., 2002; Gostin & Hodge, Jr., 2002; Hoffman & Podgurski, 2007; Pritts, 2002; Winn, 2002), and the GLBA (Cuaresma, 2002; Janger & Schwartz, 2002; Singh, 2006; Solove, 2003b). Exceptions aside (Swire, 2002), in most cases scholars would conclude that although these new laws were better than no regulation, they were still watered-down versions of the FIPs.

Evaluating COPPA, for example, Anita Allen would comment: "Fair information practice standards first promulgated in the 1970s are embodied in COPPA's requirements of notice, access, and security. COPPA requires certain fair information practices of covered Websites" (Allen, 2001, p. 762). This, however, would not make COPPA a perfect legal regime. According to Allen,

> COPPA was designed to protect the informational privacy of children and their families from excessive and unwanted disclosures of personal information. It was

> designed to impose certain fair information practices on e-commerce, and to educate the public. COPPA was not designed to bring to a halt data collection, advertising, and sales practices that target young people and their families." (Allen, 2001, p. 767)

Similarly, when assessing the HIPAA Privacy Rules, Joy L. Pritts would contend that:

> [t]he recently issued Federal Health Privacy Rule has effectively evened out some of this discrepancy by establishing a federal floor of privacy protections based on fair information practices. The Federal Rule, however, *does not afford adequate protection of health information because it has limited applicability and areas of lax protection*. (Pritts, 2002, p. 327)

Regarding its alleged limited applicability, Pritts would raise attention to the fact that the HIPAA Privacy Rules applied covered only a limited group of persons and organizations that hold health information, while leaving employers, life insurers, and health care providers who do not engage in electronic standard transaction unregulated. Sharona Hoffman & Andy Podgurski (2007) would also make related allegations but with regard to the HIPAA Security Rule.

### 2.3. Tort-based solutions

Another area where scholars' support substantially increased between 2000 and 2007 was Tort-based solutions. Despite some skepticism about their real utility for the "information society" (Bresnahan, 2000; Froomkin, 2000b; Rothstein, 2000; Solove, 2001, 2003b), following suit from academics writing in the 1990s (Bezanson, 1992; Harvey, 1992; Jurata Jr., 1999; Kim, 1996; Mcclurg, 1995) scholars would constantly come up with proposals to stretch existing Privacy Torts or create new ones. Some of them, for example, would propose creative strategies to inform the application of the existing Privacy Torts. Thus, while Lior Jacob Strahilevitz (2005) would recommend drawing insights from the literature on information transmission

through social networks to empirically determine the extent of dissemination that a plaintiff should have expected after a disclosure of information, Katherine J. Strandburg (2005) would suggest considering the personal information norms of particular social groups in analyzing the reasonable expectations of privacy in particular social settings.

Other scholars would argue that courts should invigorate the tort of *intrusion upon seclusion*, by employing a new mode of interpretation to cover "intrusions into public-private realms as well" (Crisci, 2002, p. 241) (Kato Ku, 2005) as well as electronic intrusion and monitoring (Cohen, 2003). Another scholar would combine it with the elements of negligent infliction of emotional distress (NIED), to create a new cause of action to protect employees' privacy against monitoring (Wesche, 2002).

With regards to the tort of *misappropriation of name or likeness*, some scholars would propose to use it to respond to harms derived from the collection of data for data mining, profiling, and sale (Cohen, 2003; McClurg, 2003; Reidenberg, 2002). Finally, regarding the *public disclosure of private facts* tort, Rodney A. Smolla (2002) would suggest strengthening this tort by combining it with the property-like elements of the intrusion tort. Relatedly, Patricia Sánchez Abril would propose "a new conception of the tort that transcends technology and physical space" (2007b, p. 3) and could be applicable to harms in Online Social Networks ("OSNs"). Similarly, Tal Zarsky would contend:

> [C]ourts should consider *broadening the use* of the tort of "disclosure of private fact" (or "invasion of privacy") referred to above. At this time, the "disclosure" tort is not accepted in all states. Moreover, even where accepted, the plaintiff rarely wins, as the courts require the publicized matter to be highly offensive to a reasonable person, communicated to the public at large and not a legitimate concern of the public. Since the public's standard of "reasonable" is constantly shifting to the extreme, plaintiffs are finding it considerably more difficult to prove the elements of this tort. As Rosen suggests, perhaps courts should set a higher standard of reasonable conduct by which defendants must abide, regardless of society's current subjective standard. (Zarsky, 2004a, p. 50)

Finally, following Randall P. Bezanson (1992) & Michael Harvey (1992), during the studied years Jessica Litman (2000), Brandon McKelvey (2001), Peter A. Winn (2002), and Neil Richards & Daniel Solove (2007) would also propose the use of the tort of *breach of confidentiality* as an alternative—or complement, in the case of Richards & Solove—to the common law of Privacy. In support of their proposals, most would highlight the relationships of trust that underpinned the widespread collection of personal information. Even, Litman would refer to her proposal as "[a] relational approach to data privacy protection" (2000, p. 1311). Interestingly, in 2001 Ian Kerr (2001) would also refer to the relationship of trust and confidence between online service providers and their users, but to explore the possible applicability of the equitable principles governing the law of fiduciaries. As will be seen, this relational approach would become very popular in scholarship in the years to come.

### 2.4. Technology-based solutions

Unlike the clear opposition to market-based solutions and the evident support for FIPs-based laws and tort-based solutions, which seemed almost unanimous in the community, scholars' positions about technology-based solutions were all over the place during the studied period. This, in part, due to the wide range of technological solutions being considered during this time.

Thanks to Lawrence Lessig (Lessig, 1999b, 1999a), several scholars began the 21st century grappling with the World Wide Web Consortium's Platform for Privacy Preferences (P3P) Project. As explained in Chapter II, Lessig's proposal assumed that by using this software transmission protocol consumers would be able to establish their privacy preferences, compare them with the privacy standards of websites, and as a result, negotiate the price to be paid by

the market. In the new century, scholars like Jonathan Zittrain (2000), William McGeveran (2001), Mary J. Culnan & Robert J. Bies (2003), and Jerry Kang & Benedikt Buchner[57] (2004) would support the convenience of implementing P3P or P3P-like tools (e.g., trusted systems). In contrast, Paul Schwartz (2000b), Marc Rotenberg (2001), and Peter Swire (Swire, 2003) would argue against them, primarily highlighting their technical and privacy-protecting shortcomings, as well as their "few signs of life" (Rotenberg, 2001, p. 24).

When it comes to self-help technologies, many scholars would be incredulous about the efficacy of technologies such as ad-blocking software and cookie disablement (Bartow, 2000; Cohen, 2001; Nehf, 2005), but more optimistic about the usefulness of encryption, anonymity, and/or pseudonymity software (Farmer, 2003; Peek, 2003; Wesche, 2002; Zarsky, 2004b).

In contrast, when talking about Privacy Enhancing Technologies (PETs) in general, most scholars would describe them in a positive light (Blanchette & Johnson, 2002; Cohen, 2000, 2003; Froomkin, 2000b; Reidenberg, 2000; Schwartz, 2000a, 2000b; Westin, 2003). Even, some would begin to consider **integrating them into the technical systems' design** (Bernstein, 2006a; Cohen, 2000, 2003; Froomkin, 2000b; J. R. Reidenberg, 2000; Schwartz, 2000b, 2000a). Inspired by the value-sensitive design approach proposed by Batya Friedman and her colleagues, in 2003 Julie Cohen would for example contend: "one can articulate as an explicit norm of the design process the goal of minimizing privacy-invasive constraints" (Cohen, 2003, p. 584). Interestingly, she would even include this measure as part of the structural changes that—along with ideological changes—should be pursued to intervene the "political economy

[57] However, Kang and Buchner's support to P3P was less radical. "We agree with Rotenberg that it would be simplistic to assume that P3P could provide some magical technological fix to all relevant privacy concerns. At the same time, we do not rule out the possibility that P3P-like implementations might become one valuable element among others in an ideal solution set." (Kang & Buchner, 2004, p. 263)

of information markets" (Cohen, 2001, p. 17). Although a visionary at the moment, Cohen's reference to the necessity to intervene the political economy as a whole would become recurrent in American privacy law scholarship in the next two decades.

Importantly, most of the scholars supporting any of these technology-based solutions—P3P, self-help technologies, and PETs—would emphasize the importance of considering them as part of integrated systems, where technologies were only one part of the solution (and which would also typically include laws incentivizing the development of these technologies) (Blanchette & Johnson, 2002; Cohen, 2000; Culnan & Bies, 2003; Froomkin, 2000b; McGeveran, 2001; Schwartz, 2000a).

### 2.5. Free speech concerns

Before closing, it is relevant to note that, when proposing these different tools, many scholars writing during these years would be mindful of concerns about free speech. Recognizing how "[m]any restrictions on the free flow of information designed to protect a 'right of privacy' in sensitive personal information have faced intense scrutiny under the First Amendment" (Winn, 2002, p. 621), it would be common to see scholars: (i) evaluating and delimiting the reach and scope of the free speech rights *vis a vis* privacy (Baker, 2004; Bresnahan, 2000; Cohen, 2000; N. Richards, 2005; D. J. Solove, 2006b); (ii) questioning existing tools or other scholars' proposals based on First Amendment grounds (Froomkin, 2000b, 2000a; Hetcher, 2001; McClurg, 2006); or (ii) explaining how their own proposed solutions could survive eventual First Amendment challenges (Bartow, 2000; McGeveran, 2001; D. J. Solove, 2002b; Winn, 2002).

***

Three main reflections can be drawn from this Chapter. Probably due to the fact that the technological advances witnessed by scholars during this period (2000-2007) were not particularly revolutionary in comparison to the previous decade, the harms considered by American privacy law scholars during these years did not radically change either. That does not mean, however, that the harm's reach and scope would remain exactly the same. As was seen, rather than raising alarms about the loss of control *over one's personal data*, the scholarship described here would be more attentive to the loss of control *over one's life*. Similarly, instead of being worried about the lack of zones of insularity for self-development, by the end of the 2000-2007 period scholars where more concerned about the threat to autonomy derived from the reduction of individuals to a set of data points on which decisions were being made. Despite these relevant changes, both harms would continue being linked to individuals' autonomy, dignity, and sense of self-ownership.

Secondly, it is interesting to observe how the evolution of the proposed privacy tools during these years indicates both conflict and convergence among the members of the community studied. On the one hand, the described backlash against market-based solutions, for example, can be highlighted as an important conflict in the discourse of the community reviewed here. On the other hand, the overwhelming support for legally enacted FIPs illustrates a moment of high cohesion within the history of this intellectual discourse. So much so that in 2003 Paul Schwartz & William M. Treanor would even refer to this significant trend as the "new privacy," forcefully arguing that: "the generally agreed upon path to the new privacy is through FIPs, which are generated primarily through the legislative process" (2003, p. 2180). Thus, as powerful as the technology-as-law movement could have been during the 1990s, this period's overwhelming claims about the necessity of FIPs-based legislation would mark a second turning point in the American scholarly discussion about regulatory techniques to protect information privacy.

Lastly, it seems important to note how, other than the evaluations done by some scholars to the operationalization of the FIPs in COPPA, HIPAA, and GLBA, very few cross-pollination (or in a sense, "co-production") seemed to be happening during these years between these scholars' work and what was being produced by the American legal system. This, even despite the rise of the FTC as a prominent player in the American privacy law environment.

## IV. 2008-2014: A New State of Flux for Eventful Times

In accordance with what was announced in Chapter II, the present Chapter continues tracing the intellectual history of privacy's algorithmic turn in the sample of American privacy law scholarship here reviewed. Specifically, this Chapter focuses on the period between 2008 and 2014, which coincides with the first seven years of the Privacy Law Scholars Conference ("PLSC").

As will be seen, the years covered in this Chapter could be considered as some of the most eventful in this intellectual history so far. During this period, scholars would witness the popularization of social networking platforms, the sustained use of online behavioral advertising by private companies, and the Big Data revolution. In parallel, they would be attentive to the multiple privacy-related interventions advanced over these years by the FTC, the Obama Administration, and the industry itself. All this, while American society's attitudes towards privacy remained ambivalent, giving meaning to what in 2007 Patricia A. Norberg, Daniel R. Horne, & David A. Horne had come to coin as the "privacy paradox" (Norberg et al., 2007).

In light of this agitated techno-legal context, the number of harms detected by the privacy law scholars reviewed here increased significantly between 2008 and 2014, while their nature also changed considerably. Taking these harms into consideration, scholars writing during these years would begin to depart from the path taken by their intellectual community over the last seventeen years. In particular, during the period under review scholars would begin to identify the limitations of the FIPs in the Information Age. As a result, they would once again expand the possible regulatory options, proposing to either adapt the FIPs' key elements to the Digital Age, abandon them and subsequently adopt old (e.g., Tort law) or new alternatives (e.g., social norms, co-

regulation), draw upon other areas of law (e.g., Fiduciary law, Contract law, Environmental law), or still implement the FIPs but through a Privacy by Design ("PbD") approach.

Similar to Chapters II & III, the structure of this Chapter is the following. In Section A I offer an overview of the sociotechnical and techno-legal context of the 2008-2015 period, *as seen through the lens of the scholars here studied*. For that purpose, details are provided about the most important technological developments of the period, the societal attitudes that surrounded them, and the various ways in which Congress, the FTC, the Obama Administration, and the industry reacted to them. Following this, I present the traditional and new harms identified by scholars over the course of these years, as well as the once again expanded repertoire of legal instruments proposed by them to address those harms.

## A. Context

This Section looks to situate the reader within the technological, social, and legal context in which the American privacy law scholars here reviewed were writing between the years 2008 and 2014. Here, I review the main information technologies and practices of this period, the most salient societal attitudes that developed in response to them, and the legal frameworks that existed during those years. The purpose of this Section is to provide a general overview of the multiple sociotechnical and techno-legal factors that may have influenced the thinking of these scholars during the first seven years of PLSC.

As in Chapters II & III, when reading this Section it is important to have in mind that the overview offered here is presented *through the lens of the scholars reviewed for this study*. As a result, my role in collecting and synthesizing these accounts has not been to judge or correct them, even if the accounts here might sometimes look deterministic, inaccurate, or exaggerated.

## 1. Information technologies and practices

In 2009, Woodrow Hartzog cited a Pew Research Center study that stated that "[o]ver seventy percent of U.S. adults are online" (2009, p. 895). In 2010, Larry Ponemon would point out that "according to research firm IDC, despite the current economic downturn, the volume of digital data generated in 2008 increased 3 percent more than forecast and is expected to double every 18 months" (2010, p. 1). In fact, in 2014, Dennis Hirsch would cite a New York Times' article to report that "ninety percent of the world's data, from the beginning of human history until the present, has been produced in just the past two years. This total is projected to double every two years for the foreseeable future" (2014a, p. 380)

Against this backdrop, between 2008 and 2014—which as mentioned before correspond to the first seven years of PLSC—American privacy law scholars would keep highlighting the "proliferation of online data collection, processing, analysis, and storage capacities leading businesses to employ increasingly sophisticated technologies to track and profile individual users" (Tene & Polonetsky, 2012a, p. 356). Yet, this epoch would also increasingly be described by scholars as the "era of *social media* and *behavioral tracking*" (Hartzog & Stutzman, 2013b, p. 387) (boyd & Marwick, 2011). Likewise, other scholars would describe it as well as "the era[58] of *Big Data*" (D. D. Hirsch, 2014a, p. 375; Rubinstein, 2014, p. 861; Tene & Polonetsky, 2012b, p. 68; Warner & Sloan, 2014; Yakowitz Bambauer, 2012, p. 207).

Thus, in contrast to the 2000-2007 period—where scholars tended to offer an overview of various data collection, processing, and use techniques, during these years the majority of scholars would concentrate their efforts on addressing: (i) one specific technology used to *collect*

[58] Or "age."

information (social networking platforms), (ii) one particular way of *analyzing* information (Big Data); and (iii) one specific *use* of the processed information (online behavioral advertising).

### 1.1. Social networking platforms

As seen in Chapter III, Online Social Networks (OSN) had been spotted in previous years by pioneer scholar Patricia Sánchez Abril (2007a, 2007b). However, it was during this period when several scholars started to address online social networks (also referred to in the scholarship reviewed as social networking platforms, social media services, social media platforms, or networked technologies)—mostly Facebook, but also MySpace, Google Buzz (followed by Google+), Twitter, and LinkedIn—as one of their main objects of study (and in many times concern).[59]

At least four elements about social media platforms drew the scholars' attention during this period. First, the augmented capacity that social networking platforms' users had there to "share updates, comments, photographs, videos, and other information through posts" (Schwartz & Solove, 2011, p. 1847). As Woodrow Hartzog would describe in 2014, "the most likely publisher of personal information in the Internet age is the person herself" (2014, p. 766). To be clear, this characteristic was not unique of social media services. Rather, it is proper of applications and services pertaining to the "second generation of the Internet" (Gratton, 2014, p. 5), also known as "Web 2.0," "in which users *generate* content and *voluntarily* share personal data about themselves and their associates" (Rubinstein & Good, 2013, p. 1344).

[59] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (boyd & Marwick, 2011; Brandimarte et al., 2013; Citron, 2009; Edwards & Harbinja, 2013; Gratton, 2014; Hartzog, 2009, 2011, 2014; Hartzog & Stutzman, 2013b, 2013a; I. Kerr, 2013; MacCarthy, 2011; Madejski et al., 2012; Nissenbaum, 2009; Peek, 2009; N. Richards, 2013; Rubel & Biava, 2013; Rubinstein & Good, 2013; Schwartz & Solove, 2011; Strahilevitz, 2010; P. Swire, 2012; Warner & Sloan, 2014).

The "Web 2.0" phenomenon had been recognized in American privacy law scholarship since the previous studied period (2000-2007), when several scholars were focusing on "blogs" (Byers, 2007; Evans, 2007; Hong, 2007; Kirkland, 2006; Lichtenstein & Darrow, 2006; Rita & Gunning, 2006; D. J. Solove, 2003a; Swaya & Eisenstein, 2005). However, its replication in social networking platforms became of interest for many others between 2008 and 2014 (Brandimarte et al., 2013; Gratton, 2014; Hartzog, 2014; Hartzog & Stutzman, 2013b; Madejski et al., 2012; Schwartz & Solove, 2011; Tene & Polonetsky, 2012a). Likewise, during these years some scholars would identify how, unlike blogs, social networking platforms came with an additional affordance—also spotted since the 1990s in the JenniCam and SaraCam projects (Allen, 1999a), namely, the opportunity to watch others. As Marcy Peek would eloquently highlight in 2009,

> in the last few years we have seen a shift from simply enjoying being watched to a phenomenon of *enjoying "watching each other"*; in other words, the watcher and the watched become mutual observers and derive intellectual, psychological, and/or sexual satisfaction from knowing what the other is doing at discrete times or at all times. This phenomenon I term the "bilateral relational vector." (2009, p. 57)

As a second element, some scholars (D. E. Bambauer, 2014; Chander, 2011; Citron, 2009; Lipton, 2012) would focus their attention on "abusive online conduct" (Lipton, 2012, p. 1104) and "destructive mob behavior" (Citron, 2009, p. 67) taking place within these social media services. Examples would include, among others, cyber-bullying, cyber-harassment, cyber-stalking, and non-consensual posting and distribution of sexually explicit photos and videos online (a practice usually referred to as "revenge porn" (D. E. Bambauer, 2014, p. 2026)).

Third, some scholars (I. Kerr, 2013; MacCarthy, 2011; N. Richards, 2013) were also interested in Facebook's Open Graph and instant personalization technologies, which would link content between this social media and partner websites. For example, Facebook's features would allow: (i) Facebook's partner sites to use data from a Facebook user's profile to personalize their own

websites for that user; (ii) Facebook's users to "Like" a page or content on a developer's site, and make this appear on their news feed, to share with friends what they are up to; and (iii) [s]ervices like Spotify and the Washington Post Social Reader (…) [to] integrate our reading and listening into social networks like Facebook, providing what CEO Mark Zuckerberg calls 'frictionless experiences' of sharing" (N. Richards, 2013, p. 691),

Finally, a few scholars (boyd & Marwick, 2011; Hartzog, 2009) would also be interested in the social media platforms' ability to provide users with a sense of community. Woodrow Hartzog, for example, would consider social networks—as well as the dating websites and online support communities for substance abuse problems—as "online communities," defining them as "websites consisting of users with common interests, the ability to restrict access, and a terms of use agreement" (2009, p. 896). According to him, "[a]t their core, online communities are websites designed to enable communication among users with a common interest and promote shared information through the interconnection of their users" (2009, p. 896). Similarly, danah boyd and Alice Marwick would refer to social network platforms as "networked publics." "Social network sites," boyd & Marwick would point out, "have become the modern-day equivalent of the mall or movie theater, a place where teens can hang out with friends and run into other friends and peers" (boyd & Marwick, 2011, p. 7). Interestingly, almost thirteen years after Jerry Kang's cyber-mall metaphor (1998), the mall would re-emerge again in the sample of scholarship here studied as a helpful figure of speech for conveying meaning in the studied intellectual discourse.

### 1.2. Big Data

With regards to Big Data, in the sample of papers here studied this catchy term appeared for the first time in 2012 (Tene & Polonetsky, 2012b; Yakowitz Bambauer, 2012). From then on, multiple

scholars[60] began to use it, although with various different meanings. On the one hand, the Big Data term would be used by some to simply refer to "vast databases" (Hartzog & Stutzman, 2013b, p. 387) (Birnhack et al., 2014; D. D. Hirsch, 2014a; Yakowitz Bambauer, 2012). On the other hand, most of them would use the term to describe the combination of massive amounts of data, powerful processors, unlimited storage, and—above all—*predictive* models. On this last element, Dennis Hirsch's comment on the matter is illuminating: "Big data also possesses another attribute that is central to the benefits it creates and the threats that it poses. It uses *correlations* to generate accurate and actionable *predictions*" (D. D. Hirsch, 2014b, p. 349).

Thus, instead of using the term by itself, some members of this second group—focused on the combination of massive amount of data and predictive models—would usually introduce it as "big data capabilities" (Tene & Polonetsky, 2013, p. 71), "big data analysis" (Dwork & Mulligan, 2013, p. 36), or "Big Data analytics" (Crawford & Schultz, 2014, p. 93). As examples, they would cite situations such as its use by insurance companies "to predict which insurance applicants are likely to suffer from high blood pressure, depression, or diabetes, and so to identify high-risk applicants" (D. D. Hirsch, 2014b, p. 352); by Google Flu Trends to predict and locate outbreaks of the flu (Tene & Polonetsky, 2012b, p. 64); by firms to analyze consumers' transactions, "spot the places in which consumers deviated from the rational model (…)[,] identifying the factors related to these deviations, (…) [and] watch for those factors to align again and target the consumer when she is vulnerable" (Calo, 2014, p. 1010); or by political actors to "target personalized messages to individual voters by applying predictive modeling techniques to massive troves of voter data" (Rubinstein, 2014, p. 882).

[60] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Birnhack et al., 2014; Calo, 2014; Crawford & Schultz, 2014; Dwork & Mulligan, 2013; Hartzog & Stutzman, 2013b; D. D. Hirsch, 2014b, 2014a; Rubinstein, 2014; Tene & Polonetsky, 2013)

Nevertheless, the most repeated example cited by scholars during these years would be the by now well-known case of the retail giant Target, uncovered in February 2012 by the New York Times Magazine (Calo, 2014; Crawford & Schultz, 2014; D. D. Hirsch, 2014b; Porat & Strahilevitz, 2014; Tene & Polonetsky, 2013). As described by Omer Tene and Jules Polonetsky in 2013,

> Target employed statisticians to sift through buying records of women who had signed up for baby registries. The statisticians discovered latent patterns, such as women's preference for unscented lotion around the beginning of their second trimester or a tendency to buy supplements like calcium, magnesium, and zinc within the first 20 weeks of a pregnancy. They were able to determine a set of products that, when grouped together, allowed Target to accurately *predict* a customer's pregnancy and even her due date. In one case, the New York Times reported that a father of a teenage girl stormed into a Target store to complain that his daughter received coupons and advertisements for baby products. A few days later, he called the store manager to apologize, admitting that, "There's been some activities in my house I haven't been completely aware of. She's due in August." (Tene & Polonetsky, 2013, pp. 66–67)

To be sure, the predictive capabilities of data mining applications had already been spotted in works reviewed in the two previous Chapters (Boehmer, 1992; D. D. Hirsch, 2006; McClurg, 2003; Peek, 2003; D. J. Solove, 2007; D. J. Solove & Hoofnagle, 2006; Reidenberg & Gamet-Pol, 1995; D. J. Steinbock, 2005; Westin, 2003; T. Z. Zarsky, 2003, 2004a, 2004b). However, during those years, scholars had not labelled those practices as "Big Data"; a term that— as some scholars of this period would recognize (D. D. Hirsch, 2014b; Rubinstein, 2014)—is useful to acknowledge three specific characteristics of the data mined (the "three v's"): "volume (the amount of data being created), variety (the range of data types and sources), and velocity (the speed at which data is generated and must be analyzed)" (Rubinstein, 2014, p. 864).

### 1.3. Online behavioral advertising

Finally, when it comes to online behavioral advertising—the particular *use* of analyzed information to which scholars paid special attention during these years, its appearance in this period's literature is vast and sustained.[61] Although in previous studied periods scholars had already focused on targeted advertising (Berman & Mulligan, 1999; Glancy, 1995), online behavioral advertising "involves *a third party*, largely unfamiliar to the user, collecting and processing information about her based on her browsing activity *on various unrelated websites* in order to compile an individual profile, which will be used to facilitate the targeting of ads" (Tene & Polonetsky, 2012a, p. 283). In that sense, as Ryan Calo would point out, "the 'behavioral' in behavioral tracking refers to the previous behavior of the user online, which then serves to sort that user into a particular category for ad-matching purposes" (2014, p. 1016).

Scholars writing during this period would explain how online behavioral advertising "usually involves three parties: a content provider who operates a website or other online service, an ad serving company, and an advertiser who wants to reach a targeted audience with a message" (MacCarthy, 2011, p. 496). As specific examples, some scholars would cite the Beacon online ad system introduced by Facebook in 2007 and "which tracked users' online activities on third-party websites" (Schwartz & Solove, 2011, p. 1846) (Strahilevitz, 2010).

Many scholars would also describe online behavioral advertising as a highly profitable use of data for companies (MacCarthy, 2011; Schwartz & Solove, 2011; Tene & Polonetsky, 2012a; Warner & Sloan, 2012). According to Mark MacCarthy, "[t]he price of a contextual ad or a run of

[61] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Calo, 2014; Hartzog & Stutzman, 2013b; I. Kerr, 2013; MacCarthy, 2011; Schwartz & Solove, 2011; Sloan & Warner, 2014; Strahilevitz, 2010; P. Swire, 2012; Tene & Polonetsky, 2013, 2012a; Warner & Sloan, 2012; Yakowitz Bambauer, 2012).

network online ad will be a fraction of the targeted return rate. For content providers, this creates additional economic support for their services. One study estimates that targeted ads are 50% more effective in generating sales" (2011, p. 497). In a similar fashion, Richard Warner & Robert H. Sloan would contend:

> advertisers are a significant source of revenue for sellers in markets in which buyers provide information and receive advertising in exchange for products and services. As long as buyers are trapped in "seller wins" One-Sided Chicken, large and stable advertising revenues will make sellers unresponsive to demands from small minorities of buyers to change the sellers' information-processing policies. (Warner & Sloan, 2012, p. 78)

Given its sophisticated nature and profitability, this data use would not only appeal to online websites, but also to American privacy law scholars studying online dynamics.

### 1.4. Other less significant technologies and practices

Aside from social networking platforms, Big Data, and online behavioral advertising, three other technologies[62] and practices also called the attention of American privacy law scholars during these years—although to a lesser extent. In terms of technologies, during the years under study some scholars put the spotlight on **self-surveillance or self-tracking technologies** (Kang et al., 2012; Patterson & Nissenbaum, 2013; Peppet, 2012; N. Richards, 2014). According to Jerry Kang and his co-authors,

> [u]sing various existing and emerging technologies, such as GPS-enabled smartphones, *we are beginning to measure ourselves in granular detail*-how long we sleep, where we drive, what we breathe, what we eat, how we spend our time. And we are storing these

[62] Another sociotechnical system that received a mention from some scholars (Calo, 2014; Friedman & Hoffman, 2014; Hoepman, 2014; Patterson & Nissenbaum, 2013; N. Richards, 2014; Tene & Polonetsky, 2013) during these years was what came to be known as the "Internet of Thing5/22/2024 5:27:00 PM," "in which billions of electronic devices will connect to the internet, collecting and relaying unimaginably large amounts of data" (N. Richards, 2014, p. 40). However, except for Allan Friedman & Lance J. Hoffman's account of early IoT applications (2014), the rest of its mentions were in passing, with none of the reviewed authors focusing one of their pieces on digging into its specific implications for privacy.

> data casually, perhaps promiscuously, somewhere in the "cloud" and giving third parties broad access. (2012, p. 812)

As examples of these technologies (or "socio-technological practices," as described by Kang et al.), scholars would mention sensor devices such as Fitbit monitors, BodyMedia's armbands, SleepTracker devices, and web services used to track newborns' habits. According to Heather Patterson and Helen Nissenbaum, in these gadgets consumers were not only encouraged to share their records on their social media networks, but "self-tracking services are selling activity data to users' employers and are partnering with insurance companies to find 'the holy grail' of negative correlations between Fitbit use and doctor visits" (2013, p. 45).

Some other scholars, in turn, would write about the massive proliferation of **mobile devices** (e.g., camera phones, smartphones, tablets), which would usually be location-aware and include cameras (Chander, 2011; J. King, 2012; P. Swire, 2012; Tene & Polonetsky, 2013, 2012a). These authors would emphasize several things about these technologies that made them different. Jennifer King, for example, would highlight how "personal computing has become even more personal as focus shifts from the desktop PC, to laptops, and now smartphones and tablets. Ours and others' research suggests that simply assuming that the smartphone is a smaller scale laptop may be misguided" (2012, p. 12). Omer Tene & Jules Polonetsky, in turn, would add:

> First, users carry their mobile device with them at all times, allowing ad intermediaries to track not only their browsing activity but also their physical location; indeed, few devices store more personal details about their users than mobile phones, including contact numbers, location, and a unique identifying number that cannot be changed or turned off. Second, mobile users consume online services by downloading applications (apps), software programs that allow them to play games, read e-books, or search for restaurants without launching a browser or using a search engine. Mobile apps thus replace browsers and search engines as the main entry gate to the mobile Internet. (2012a, p. 296)

Finally, some scholars writing during this period (Citron, 2008; Citron & Pasquale, 2014; Crawford & Schultz, 2014; Dwork & Mulligan, 2013; N. Richards, 2008; Yakowitz Bambauer, 2012) would start identifying a *use* that would become very popular in American privacy law scholarship in the years to come: **automated decision-making systems**. For Neil Richards, this type of systems was fueling "a vast market for a wide variety of electronic information about individuals" (2008, p. 389). Danielle Keats Citron, however, would go even further. According to her, "[i]n the past, computer systems helped humans apply rules to individual cases. *Now, automated systems have become the primary decision makers*. These systems often take human decision making out of the process of terminating individuals' Medicaid, food stamp, and other welfare benefits" (2008, p. 1252). Similarly, talking about "automated scoring systems" (Citron & Pasquale, 2014, p. 18), Citron and Frank Pasquale would contend:

> Just as concerns about *scoring systems* are more acute, *their human element is diminishing*. Although software engineers initially identify the correlations and inferences programmed into algorithms, *Big Data* promises to *eliminate the human "middleman" at some point in the process*. Once data-mining programs have a range of correlations and inferences, they use them to project new forms of learning. The results of prior rounds of data mining can lead to unexpected correlations in click-through activity. If, for instance, *predictive algorithms* determine not only the types of behavior suggesting loan repayment, but also automate the process of learning which adjustments worked best in the past, the computing process reaches a third level of sophistication: *determining which metrics for measuring past predictive algorithms were effective, and recommending further iterations for testing*. In short, predictive algorithms may evolve to develop an *artificial intelligence (AI)* that guides their evolution. (2014, pp. 5–6)

As pioneers, with these words Citron & Pasquale would touch on a related technology—Artificial Intelligence (AI)—to which many other American privacy law scholars would also devote considerable attention from then to the present day.

## 2. Societal attitudes

As pointed out by Sasha Romanosky, David Hoffman, & Alessandro Acquisti in 2014, "[t]he surge in popularity of social media, e-commerce, and mobile services is proof of the benefits consumers are enjoying from information and communication technologies" (2014, p. 74). As scholars during these years would report, Facebook's monthly active users grew from one million in 2004 to 1.5 billion in 2013 (Warner & Sloan, 2014). Similarly, in 2011 a study from the Pew Research Center would show that "approximately one-quarter of internet users have tracked some aspect of their health online" (Peppet, 2012, p. 81).

Compared to social networking platforms and self-tracking technologies, however, some of the other technological developments mentioned above were not received that well by the American public.

### 2.1. Aversion to online tracking

In 2011, Paul Schwartz and Daniel Solove (2011) would cite a 2010 Gallup poll that concluded that U.S. Internet users were ready to limit online tracking for ads. Similarly, in their articles many scholars (Calo, 2011a; MacCarthy, 2011; D. J. Solove & Hartzog, 2014; Tene & Polonetsky, 2012a) would refer to a 2009 study by Joseph Turow and his collaborators, in order to evidence how Americans rejected online behavioral advertising. According to MacCarthy, for example,

> [w]hatever the possible benefits, polls show that the public does not like the practice of *online behavioral advertising*. When asked, 66% of respondents to a recent poll said they did not like it. The more they knew about the practice the less they liked it. When told how targeted ads were developed through the use of cookies, profiles and data analytics, the percentage of people disapproving rose to 84%. (2011, p. 498)

### 2.2. The "privacy paradox"

Despite this evident aversion, during this period scholars continued to emphasize the societal ambivalent attitudes towards privacy that they had already noticed since the previous two studied periods, and which Patricia A. Norberg, Daniel R. Horne, & David A. Horne came to coin in 2007 as the "privacy paradox" (Norberg et al., 2007). According to Tene & Polonetsky, for example,

> The general public, meanwhile, often expresses in opinion polls an interest in privacy and aversion towards online behavioral tracking. *Yet such results should be tempered against the reality that users consistently refrain from taking any step, no matter how trivial and costless, to prevent tracking*. What does it mean to be "for privacy" or "against tracking," and at the same time unwilling to check a box or pay a single penny to preserve one's rights? Many advocates will suggest that the choices are too confusing or too hard to exercise, but even when the choice is as basic as unchecking a clearly visible tick-box, the default continues to rule the day. And when users perceive a benefit, even if small, they quickly share their data. (2012a, p. 333)

In fact, during these years several authors would report how, "[i]n general, the public has been skeptical about the efficacy of privacy-enhancing technology (…) for protecting information privacy" (Xu et al., 2009, p. 20). According to Ira Rubinstein,

> [o]n the consumer side, *few PETs have proven popular* and *the demand for products and services with strong privacy safeguards seems quite limited*. Reasons include consumers' *lack of knowledge concerning the privacy risks* associated with web surfing, search, social networks, e-commerce, and other daily internet activities and *their limited understanding of how PETs or privacy by design might help reduce these risks*. Further, *cognitive and behavioral biases* may prevent some individuals from acting in accordance with their stated preference for greater privacy. Other consumers *just do not care* very much about privacy. (2011, p. 1412)

MacCarthy, in turn, would add that non sophisticated Internet users would probably not use tools to block adds, clear cookies, or use secure VPNs to anonymize their IP address, "[a]nd they probably cannot be educated into doing them either." According to him, "[i]t is unreasonable to expect ordinary consumers to become experts at hiding information from people who spend most of their working day trying to get at it" (MacCarthy, 2011, p. 511).

Presumibly, the lack of use of some of these self-help technologies was also influenced by the "spectacular, surprising, and embarrassing failures of anonymization" suffered by "sophisticated data handlers— America Online, the state of Massachusetts, and Netflix—" in the previous years (Ohm, 2010, p. 1706). As narrated by some authors during the studied period,[63] in 2006 Netflix released a training data set of more than 100 million ratings from over 480 thousand anonymous customers, challenging computer scientists to beat Netflix's existing recommendation system by at least 10%. However, researchers at the University of Texas used that database, plus public information on movie rentals and preferences (e.g., IMDb), to successfully re-identify some customers with "as few as five personal attributes" (Crawford & Schultz, 2014, p. 99). As a result, in 2010 Paul Ohm would publish an until-today impactful law review article contending that "[c]omputer scientists have recently *undermined our faith in the privacy-protecting power of anonymization*, the name for techniques that protect the privacy of individuals in large databases by deleting information like names and social security numbers" (2010, p. 1701). As will be see, in terms of the intellectual history here traced, this realization of the limitations of anonymization would shape in many ways the course of the intellectual discourse here studied.

### 2.3. Use of (sometimes illusory) self-protective measures

In any case, scholars reviewed during this period would also agree that Internet users "have taken some steps to avoid being tracked. They wish to avoid uses of their data that they experience as harmful (…) as well as the more amorphous costs of a lack of privacy" (Willis, 2014, p. 64). For example, several empirical works presented at PLSC during these years (boyd & Marwick, 2011;

[63] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Crawford & Schultz, 2014; Gratton, 2014; Ohm, 2010, 2013; Romanosky et al., 2014; Rubinstein & Good, 2013; Schwartz & Solove, 2011; Tene & Polonetsky, 2012a; Wu, 2013)

J. King, 2012; Madejski et al., 2012; Patterson & Nissenbaum, 2013) would document how the participants of their studies seemed to care about their privacy and tended to have privacy preserving behaviors.

According to Michelle Madejsk, Maritza Johnson, and Steven M. Bellovin, for example, "our survey data indicate they are concerned with privacy, take steps like untagging or deleting content to protect their privacy, and believe their privacy settings are correct" (2012, p. 344). Similarly, danah boyd and Alice Marwick (2011) would report how teenagers would tend to use structural and social strategies to protect their privacy on social media, such as using Facebook's blocking features, separating social contexts by social tool, posting encoded messages, or even, deactivating their accounts every day or deleting received comments after read or posted.

At the same time, scholars would also call attention to the false or unsupported beliefs of control that Internet users usually had. Citing—among other sources—another study published by Joseph Turow and his collaborators at UC Berkeley's Samuelson Law, Technology, and Public Policy Clinic in 2006, during these years many scholars (Hartzog, 2011; Ohm, 2013; Patterson & Nissenbaum, 2013; N. Richards, 2014; Sloan & Warner, 2014; Tene & Polonetsky, 2012b) would raise that "when users see the term 'privacy policy' on a website, 'they assume that a web site will not share their personal information'" (Hartzog, 2011). Relatedly, in 2012 Jennifer King would evidence how most of her study paticipants "believed that a variety of assurance structures—e.g., obtaining applications only through official stores, or a developer's positive reputation— protected them from privacy violations by applications" (2012, p. 11).

Finally, despite the fact that "[s]ince 2005, an estimated 543 million records ha[d](…) been lost from over 2,800 data breaches, and identity theft caused $13.3 billion in consumer financial loss in 2010" (Romanosky et al., 2014, pp. 74–75), in 2014 Sasha Romanosky, David Hoffman,

& Alessandro Acquisti would report that “the overall federal litigation rate for reported data breaches is only about 4 percent” (2014, p. 100). Thus, the increase in data breaches experienced during these years would not necessarily translate into a greater use of judicial tools to protect people's privacy.

## 3. Legal system

Aside from the data breach notification laws, which by 2011 had already been enacted in forty-five US states (Schwartz & Solove, 2011; Wolf, 2013), during these years the American privacy legislative landscape would continue pretty much unchanged. As Mary J. Culnan would describe in 2011,

> privacy in the U.S. is regulated largely on a sectoral basis. Some industries (e.g. financial services and healthcare) and practices (e.g. telemarketing, online marketing to children, data breaches, video rental records) are regulated by a patchwork of federal and state privacy laws, some of which prohibit certain uses of personal information. (2011, p. 3)

Thus, in spite of several legislative efforts, during the studied period only one privacy-related law passed in Congress, while real action was taken by the FTC, the Obama Administration, and the industry itself.

### 3.1. Mostly unsuccessful legislative efforts

The absence of an American comprenhensive privacy law described by Culnan (2011) would not mean, though, that during these years there were no Congress’s efforts to enact it. According to some of the scholars reviewed during this period (Bamberger & Mulligan, 2011; D. D. Hirsch, 2013; MacCarthy, 2011; Rubinstein & Good, 2013; Schwartz & Solove, 2011; Tene & Polonetsky, 2012a), the privacy bills considered—but not passed—by federal legislators included: (i) the Best

Practices Act (the "Rush bill"), introduced in 2010 (and re-introduced in 2011) by Representatives Bobby Rush and Rick Boucher to "establish national requirements for collecting and sharing personal information, codifying certain fair information principles into law" (Tene & Polonetsky, 2012a, p. 327); (ii) the Consumer Privacy Protection Act (the "the Stearns-Matheson bill"), also introduced in 2010 (and re-introduced in 2011) by Representatives Boucher, Cliff Stearns, and later Jim Matheson; (iii) the Commercial Privacy Bill of Rights Act of 2011, co-sponsored by Senators John Kerry and John McCain; and (iv) the Do Not Track Me Online Act of 2011, introduced by Representatives Jackie Speier, Alcee L. Hastings, and Bob Filner, "directing the FTC to develop standards for a 'do not track' mechanism allowing individuals to opt out of the collection, use or sale of their online activities and requiring covered entities to respect the consumer's choice" (Rubinstein, 2011, p. 1444).

Additionally, Omer Tene and Jules Polonetsky would report how, in October 2011, Congress created a dedicated Senate Sub-Committee on Privacy, Technology, and the Law, headed by Senator Al Franken and in charge of "[o]versight of laws and policies governing the collection, protection, use, and dissemination of commercial information by the private sector, including online behavioral advertising" (2012a, p. 320). Relatedly, "[i]n September 2013, Senate Commerce Committee Chairman Jay Rockefeller announced his committee's investigation of the information collection and sharing practices of top data brokers" (Citron & Pasquale, 2014, p. 32).

Despite these efforts, the only privacy-related law that passed in Congress during this period was an ammendment to the the Video Privacy Protection Act (VPPA) of 1988. According to Neil Richards, this reform was pushed forward by Facebook and Netflix, and "proposed allowing companies to obtain a single, durable consent to automatically and perpetually share all movies viewed on Facebook and other social networks. Despite a feisty committee hearing in the Senate,

the measure ultimately passed, and President Obama signed it into law in early 2013" (2013, p. 690).

Therefore, in these years, real legal action would take place somewhere else: at the FTC and in the Obama Administration (P. Swire, 2012).

### 3.2. The FTC's influential role

As Christopher Wolf would point out in 2013, "[t]he FTC has played an increasingly active role in shaping what privacy protections are expected for all U.S. businesses" (2013, p. 246), acting through two main mechanisms: enforcement actions and guidance.

In terms of FTC's enforcement actions, during these years scholars would refer to the cases pursued by the Commission against the holding company Sears (2009), for failing to disclose the scope of the data collection activities it conducted via a downloadable software application (Bamberger & Mulligan, 2011; MacCarthy, 2011; Schwartz & Solove, 2011; D. J. Solove & Hartzog, 2014); the software development company Echometrix Inc. (2010), for missing to inform parents that children's information would be shared with third-party marketers (Schwartz & Solove, 2011; D. J. Solove & Hartzog, 2014); the social networking service Twitter (2010), for failing to safeguard its users' personal information (Rubinstein & Good, 2013; D. J. Solove & Hartzog, 2014; P. Swire, 2012); Google (2011), for rolling out its Buzz social network on top of its users' existing Gmail contacts (Culnan, 2011; Rubinstein & Good, 2013; D. J. Solove & Hartzog, 2014; P. Swire, 2012; Tene & Polonetsky, 2013); the online behavioral advertising firm Chitika Inc. (2011), for tracking consumers' online activities even after they had opted out (Culnan, 2011; D. J. Solove & Hartzog, 2014); the social networking site Facebook (2011), for failing to keep its privacy promises (Ohm, 2013; Rubinstein & Good, 2013; D. J. Solove &

Hartzog, 2014; P. Swire, 2012); and the social networking platform MySpace (2012), for misrepresenting the privacy protections it offered to its users (Rubinstein & Good, 2013; D. J. Solove & Hartzog, 2014).

Referring to these cases, various scholars would raise the following three important considerations. First, in their 2014 article *The FTC and the New Common Law of Privacy*—already announced in the previous Chapter, Daniel Solove & Woodrow Hartzog would contend: "[d]espite over fifteen years of FTC enforcement, there are hardly any judicial decisions to show for it. The cases have nearly all resulted in settlement agreements. *Nevertheless, companies look to these agreements to guide their decisions regarding privacy practices*" (2014, p. 585). In that way, Solove & Hartzog would shed light to how, in practice, the FTC's privacy jurisprudence had become an influential regulating force in America.

Second, as Wolf would also content,

> The earliest actions focused on holding companies to the promises included in their online privacy policies; violation of a privacy promise constituted a deceptive practice under the FTC Act. *Increasingly, however, the FTC has invoked its authority to affirmatively state what privacy practices are reasonably expected for all companies.* Recent FTC enforcement actions have resulted in settlements whereby the company agrees to implement a comprehensive and auditable privacy program. (2013, p. 246)

Thus, in comparison to the enforcement cases outlined in Chapter III, during these years the FTC would have begun to require the design of specific privacy programs, rather than simply policing companies' fulfillment of their privacy promises. Indeed, Peter Swire would confirm how, compared to previous cases, "[t]he Google and Facebook [and MySpace] consent decrees included the first agreements by companies to establish a 'comprehensive privacy program,' which in part requires that, for the next twenty years, the companies have independent third-party audits every two years to assess their privacy practices" (2012, p. 1383).

Finally, during these years some scholars would also argue that the FTC's enforcement efforts—referred to by Solove & Hartzog as "the FTC's privacy 'common law'" (2014, p. 586)—might be closing the gap between the E.U and the US privacy regulations (D. J. Solove & Hartzog, 2014; Wolf, 2013). As Wolf would argue in 2013, "[t]he differences are largely in form, not substance" (2013, p. 243).

In terms of guidance activities, several privacy scholars would highlight the FTC's publication of two influential reports during these studied years. After a "Behavioral Advertising" Town Hall celebrated in November 2007, FTC staff issued—for public comment—a set of proposed principles to encourage and guide industry self-regulation (MacCarthy, 2011). After receiving more than 60 comments, in February 2009 it published a final report titled *Self-Regulatory Principles for Online Behavioral Advertising: Tracking, Targeting, and Technology* (MacCarthy, 2011; Tene & Polonetsky, 2012a). According to Tene & Polonetsky,

> These principles include: (1) transparency and consumer control (requiring websites that collect personal data to *state that they are doing so* and allow users to *opt-out of collection*); (2) reasonable *security* (commensurate with data sensitivity and the nature of the company's business operations); (3) *limited retention* for consumer data (companies may retain data only as long as is necessary to fulfill a "legitimate business or law enforcement need"); (4) *affirmative express consent* prior to using data in a manner materially different from promises made when the data was collected (protecting users from unexpected changes in the way their information is handled); and (5) *affirmative express consent* for the use of sensitive data (opt-in consent is required for the use of data, not for its collection). (2012a, p. 315)

The second FTC report—*Protecting Consumer Privacy in an Era of Rapid Change*—relevant to the scholars here reviewed was preliminarily released in 2010 and finally published in 2012.

Massively cited by scholars in both its preliminar[64] and final version,[65] this report set forth three "privacy best practices" (Wolf, 2013, p. 247) or "central axes for future regulation of online privacy" (Tene & Polonetsky, 2012a): (i) Privacy by Design ("PbD"), (ii) simplified choice, and (iii) increased transparency of data practices.

Therefore, as described by scholars, the report would promote a greater use of Privacy by Design by companies (Rubinstein, 2011; Rubinstein & Good, 2013; P. Swire, 2012; Tene & Polonetsky, 2012a). Likewise, it would contend that "companies need not provide choice before collecting and using data for 'commonly accepted' practices (…) [and] for practices requiring choice, companies must offer choice at a time and in a context in which the user is making a decision about her data"(Tene & Polonetsky, 2012a, p. 320). Additionally, it would "support a Do Not Track [(DNT)] approach to behavioral advertising, which it defines as 'a more uniform and comprehensive consumer choice mechanism for online behavioral advertising'" (P. Swire, 2012, p. 1401). And, finally, it would also emphasize "companies' obligation to increase the transparency of their data practices" (Schwartz & Solove, 2011, p. 1858) (Citron & Pasquale, 2014; Tene & Polonetsky, 2012a).

In addition to these reports, in several public events cited by the scholars here reviewed the FTC Commissioners would be vocal about the need to protect privacy. According to Tene & Polonetsky, when testifying at the Senate Committee on Commerce, Science and Transportation in July, 2010, "Chairman [Jon] Leibowitz stated that the FTC is calling for an industry-led DNT program" (2012a, p. 324). Ira Rubinstein (2014), in turn, would report that in her Keynote Address

[64] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Culnan, 2011; MacCarthy, 2011; Romanosky et al., 2014; Rubinstein, 2011; Schwartz & Solove, 2011; P. Swire, 2012; Tene & Polonetsky, 2012a; Yakowitz Bambauer, 2012)

[65] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Citron & Pasquale, 2014; Hartzog & Stutzman, 2013b; Rubinstein & Good, 2013; Tene & Polonetsky, 2013; Wolf, 2013; Wu, 2013)

at the Twenty-Third Computers Freedom and Privacy Conference (June, 2013), Commissioner Julie Brill proposed a comprenhensive initiative titled *Reclaim your Name*, to give consumers back some control over their personal data through both knowledge and technology. Likewise, citing Chairwoman Edith Ramirez's Keynote Address at the Technology Policy Institute Aspen Forum (August, 2013), Dennis Hirsch would highlight that the Commissioner was concerned

> that predictive inferences will judge individuals "not because of what they've done, or what they will do in the future, but because *inferences or correlations drawn by algorithms* suggest they may behave in ways that make them poor credit or insurance risks, unsuitable candidates for employment or admission to schools or other institutions, or unlikely to carry out certain functions." (2014b, p. 352)

Against this backdrop, in 2014 Daniel Solove & Woodrow Hartzog would boldly maintain that "the FTC has risen to act as a kind of data protection authority in the United States" (2014, p. 676).

### 3.3. Efforts by the Obama Administration

The FTC was not, however, the only authority pursuing privacy in the country. According to the scholars writing during this studied period, throughout these years the Administration of President Barack Obama, in office since 2009, also took a leadership role in this area. In 2010 the Department of Commerce convened an Internet Policy Task Force, which "begun a 'comprehensive review of the nexus between privacy policy and innovation in the Internet economy'" (Bamberger & Mulligan, 2011, p. 312). As a result, in December of that same year it released a "Green Paper" titled *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, drawing the attention of several scholars (MacCarthy, 2011; Romanosky et al., 2014; Schwartz & Solove, 2011; P. Swire, 2012; Tene & Polonetsky, 2012a). As described by Tene & Polonetsky, besides highlighting the inadequacy of the notice-and-choice system to provide adequately transparent descriptions of personal data use,

> one of the main developments called for in the Department of Commerce Green Paper is *the establishment of a Privacy Policy Office in the Executive Branch*, which would act as a "convener of diverse stakeholders" and work with the FTC to lead efforts to develop voluntary, enforceable codes of conduct. To incentivize online businesses to join the self-regulatory bandwagon, the Green Paper *suggests creating a safe harbor against FTC enforcement for companies that commit and adhere to an appropriate code of conduct*. (2012a, p. 319)

Subsequently, and building on the Green Paper's recommendation, in February, 2012 the White House released its own "White Paper" titled *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy*. Noticed by several scholars writing during this period,[66] this document included seven principles (individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability), which came to be known as President Obama's *Consumer Privacy Bill of Rights*.

According to Wolf, "[t]he Privacy Bill of Rights calls for baseline privacy legislation *largely modeled on the FIPPs* [(Fair Information Practices Principles)]" (2013, p. 234). Similarly, Neil Richards would describe the proposed list of principles as "an enforceable code of conduct for consumer data directly *modeled on the fair information practices tradition*" (2013, p. 719). In contrast, other scholars would offer more nuanced and positive descriptions. For Ira Rubinstein & Nathaniel Good, for example, "the White House framework on consumer data privacy abandons FIPs-lite entirely in favor of a new formulation of FIPs consisting of seven principles, which match up quite well with both the OECD Privacy Guidelines and the E.U. Directive" (2013, p. 1346). Relatedly, Kate Crawford & Jason Schultz would contend that "[a]lthough the FTC and the White

[66] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Crawford & Schultz, 2014; D. D. Hirsch, 2013; Ohm, 2013; N. Richards, 2013; Rubinstein & Good, 2013; Sullivan, 2013; Tene & Polonetsky, 2013; Wolf, 2013; Yakowitz Bambauer, 2012)

House share some FIPPs, the White House's version includes additional approaches to information regulation that attempt to expand the scope of FIPPs, especially in terms of control over the information at issue and with more focus on the data's user and categorization" (2014, p. 108). In any case, during the studied period these efforts would make the Obama Administration stand out as "the first to explicitly support comprehensive privacy legislation in the United States" (P. Swire, 2012, p. 1382).

### 3.4. Relevant industry's self-regulatory initiatives

The government's efforts mentioned aboved—especially those focused on online behavioral advertising, Privacy by Design ("PbD"), and the Do Not Track initiative—prompted the industry to put forward three main types of self-regulatory initiatives: (i) new guidelines and codes of conduct; (ii) online tools; and (iii) the creation of Chief Information Officer (CIO) positions within conmpanies. In terms of guidelines, a number of self-regulatory organizations (e.g., the Wireless Advertising Association (WAA), Direct Marketing Association (DMA), American Association of Advertising Agencies (AAAA), Association of National Advertisers (ANA), TRUSTe, Network Advertising Initiative (NAI), and the Interactive Advertising Bureau (IAB)) developed (or updated) privacy guidelines and codes of conduct partially or fully based on the FIPs, and specifically aimed at behavioral advertising, wireless advertising messaging, email, and location-based services (MacCarthy, 2011; Tene & Polonetsky, 2012a; Xu et al., 2009). Besides, tech companies such as Microsoft, IBM, and HP advanced guidelines and policies "for building privacy into software development and data management" (Rubinstein, 2011, p. 1423) (Rubinstein & Good, 2013).

The industry also developed online tools aimed at providing consumers more transparency and control over the receipt of online behavioral advertising (MacCarthy, 2011; Rubinstein, 2011). These included, for example, Google's Ad Preference Manager and Yahoo's Ad Interest Manager. Likewise, "the release of the FTC's Preliminary Report in December 2010 prompted the major browser makers to engage with the DNT proposal" (Tene & Polonetsky, 2012a, p. 324). According to Richard Warner & Robert H. Sloan, at a Web Tracking and User Privacy Workshop organized by the World Wide Web Consortium (W3C) in 2011, "representatives from BlueKai, Datran Media, Intel, and Microsoft, not only expressed their willingness to incorporate emerging 'do not track' technologies, they emphasized the importance of doing so" (2012, p. 82). And, two years later, the Tracking Protection Working Group of the W3C published the draft of a Do Not Track (DNT) protocol (Dwork & Mulligan, 2013; Tene & Polonetsky, 2013).

Finally, during these years Kenneth A. Bamberger & Deirdre K. Mulligan (2011) and Christopher Wolf (2013) would also highlight the impressive transformation of the corporate privacy management in the United States. Writing in 2013, Wolf would note that:

> the past fifteen years has seen an explosion in companies hiring Chief Privacy Officers (CPOs). In 2000, the few companies that had created CPO positions actually issued press releases announcing their actions. *Now there are thousands of CPO positions at companies across the United States.* The existence of a C-level position focused on privacy elevated corporate America's focus on privacy and resulted in *substantial increases in time and resources devoted to privacy protections*. (2013, p. 248)

According to Bamberger & Mulligan as well as Omer Tene & Jules Polonetsky, these changes were being accompanied by: (i) the enhancement of the privacy profession through the International Association of Privacy Professionals (IAPP), which had been created since 2000; and (ii) the rise of a vigorous privacy law practice to service "in-house" professionals (Bamberger &

Mulligan, 2011; Tene & Polonetsky, 2012a; Wolf, 2013). As Bamberger & Mulligan would report in 2011,

> the International Association of Privacy Professionals (IAPP) (…) quickly *went about formalizing educational programs and undertaking studies to understand the needs and activities of this new profession*. By 2003, IAPP claimed one thousand overall members. In 2004, the association launched a certification program in corporate privacy compliance, which certified 350 professionals within a year. And today [(2001)], IAPP boasts more than seven thousand members from businesses, governments, and academic institutions across fifty-two countries, runs a credentialing program in information privacy, the Certified Information Privacy Professional (CIPP), and runs a wide range of educational and professional conferences. (2011, p. 262)

***

This overview of technological, societal, and legal changes suggests that the most significant events of this period occurred both in the techno-legal domains. From the popularization of social network platforms, the sustained use of behavioral advertising, and the Big Data revolution to the multiple privacy-related interventions advanced by the FTC, the Obama Administration, and the industry itself, these years could be considered some of the most eventful in this intellectual history so far. In particular, in what had to do with behavioral advertising, which seemed to rise to the top of the American privacy policy agenda during these years.

In contrast, it is striking to note that, regardless of the techno-legal context, the societal attitudes toward privacy registered by scholars have not changed much over the three periods examined thus far. In particular, irrespective of revolutionary technological changes (such as the advent of the commercial Internet or the Big Data revolution) or less perceptible technological advancements (such as the shift from transactional data to clickstream data), American society's attitudes towards privacy have consistently remained ambivalent: expressing both concerns about information privacy and willingness to constantly share personal information. If anything, what has been unveiled in this domain over the years is the individuals' lack of knowledge about the complexity

of the information ecosystem, and the reach and scope of the tracking capabilities of technologies used by them.

## B. American privacy law scholars' response

In the context of this eventful background, the number of harms detected by the privacy law scholars here reviewed increased greatly between 2008 and 2014. Although scholars would continue to highlight old harms, during this period they added new ones such as discrimination and the erosion of due process rights. Considering these novel harms, scholars would begin to turn their back to many of the privacy tools they themselves had proposed up until now. A radical contrast to their previous trajectory—which, as said in the previous Chapter, had been described by Paul M. Schwartz & William Michael Treanor as the "new privacy"—scholars would gradually begin to distance themselves from most of the FIPs-based solutions. Thus, during these years only a small minority of still FIPs adherents would continue proposing to implement them fully, but through Privacy by Design ("PbD") instead of traditional statutes.

### 1. Identified harms

In the same vein as previous years, several scholars writing during this period (Matwyshyn, 2012; Rubinstein, 2014; Sloan & Warner, 2014; Tene & Polonetsky, 2012b; Warner & Sloan, 2012) would underscore the **diminishing ability of individuals to maintain control over their personal information** as an important privacy harm. Nonetheless, a set of additional traditional and new harms would specially draw the attention of scholars during this period.

### 1.1. Traditional harms

Although not necessarily raised by scholars during the past two examined periods, between 2008 and 2014 the scholars here reviewed would regularly refer to four harms which "have a long history of recognition" (Solove & Citron, 2022, p. 837) as related to privacy.

First, as Jane Bambauer would highlight in 2012, in the wake of the proliferation of abusive online conducts on social media, "**[r]eputational harm and shame** (…) [were] among the most commonly cited privacy harms. The information age has undeniably increased the availability of reputation-damaging content" (Yakowitz Bambauer, 2012). In fact, during the years under review, most authors studying cyber-bullying, cyber-harassment, stalking, and revenge porn conducts (D. E. Bambauer, 2014; Chander, 2011; Citron, 2009; Lipton, 2012) would refer to embarrassment, shame, and humiliation as preponderant harms—although not necessarily described as privacy ones.

Another "unwelcome mental state(…)" (Calo, 2011, p. 1133), that scholars would also refer to during these years was the by-then already known **"chilling effect."** According to several scholars, when faced with unconsented disclosure of personal information on the Internet (D. E. Bambauer, 2014; Chander, 2011; Citron, 2009), and the increased sense of being surveilled (Calo, 2010; D. D. Hirsch, 2006; MacCarthy, 2011; Ohm, 2013; Peek, 2009; N. Richards, 2008, 2013; Wu, 2013), individuals would commonly "change their behavior in the individual instance, or refrain entirely from engaging in certain behavior for fear of retribution or judgment" (Calo, 2010, p. 35). In practice, that would mean going offline (Citron, 2009; MacCarthy, 2011; Rubinstein, 2014), forgoing the leaked activity altogether (D. E. Bambauer, 2014), abstaining from reading or researching new things (N. Richards, 2008, 2013), or becoming "more likely to conform, and less

likely to experiment, explore, and so to find and become who we want or need to be" (D. D. Hirsch, 2014a, pp. 380–381).

A third traditional privacy harm would be the **physical harms** (e.g., rape, murder) caused by the disclosure and un-authorized publishing of personal information (Citron, 2009; Gratton, 2014; Lipton, 2012; MacCarthy, 2011; Rubinstein, 2011). For instance, scholars would argue that "individuals may become a victim of a crime against their person, in the event that their information (home or work address) are used by criminals such as stalkers and rapists" (Gratton, 2014, p. 73). These harms had been recognized by the American society since at least 1989, when the murder of actress Rebecca Shaefer by a stalker who had had access to her drivers' records led to passage of the Drivers' Privacy Protection Act.

Finally, some scholars would also focus on the **financial harms** resulting from identity theft or identity fraud.[67] Given the spate of Internet privacy incidents that had been occurring since 2005 (Calo, 2011a; Gratton, 2014; D. D. Hirsch, 2014a; Ponemon, 2010; Romanosky et al., 2014; Rubinstein, 2011, 2014; Rubinstein & Good, 2013), during the years under review scholars would highlight how, "as the amount of data an organization generates and collects has increased, so has the risk the organization faces of losing data and experiencing security breaches" (Ponemon, 2010, p. 1).

Interestingly, though, not every scholar would equate data breaches with a privacy harm. On the one hand, MacCarthy would for example contend that "[e]xtra risk of harm is also a harm. (…) The increased risk of identity theft is a measurable harm. Greater exposure to the loss of property and monetary damage are tangible harms" (2011, p. 481). In contrast, on the other side of the

[67] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Citron, 2009; Culnan, 2011; Gratton, 2014; D. D. Hirsch, 2013, 2014a; MacCarthy, 2011; Patterson & Nissenbaum, 2013; Romanosky et al., 2014; Rubinstein, 2011, 2014; Willis, 2014; Wolf, 2013; Wu, 2013)

spectrum Ryan Calo (2011) would argue that a data breach only classifies as a privacy harm if the data is used (objective privacy harm) or if the consumer is notified that that their personal information has leaked (subjective privacy harm).

## 1.2. New harms

### 1.2.1. Discrimination

One of the relatively new harms identified by scholars between 2008 and 2014 was discrimination. To be clear, during the previous studied period (2000-2008) scholars had already raised alarms on the possibility of using personal data to discriminate data subjects (DeVries, 2003; Evans, 2007; Gostin & Hodge, Jr., 2002; Hildner, 2006; Kim, 2002; Koops & Leenes, 2005; Phillips, 2003; Schwartz, 2000b; Solove, 2002a; Zarsky, 2004a). Yet, during the period under review the scholars' approach to addressing this harm would be new in two ways. First, unlike the 2000-2008 period, when scholars had only referred to price, invidious, and genetic discrimination, during these years scholars would explore a wide variety of avenues through which data-based discrimination could take place. [68] Additionally, during these years, discussions would also be held regarding the nature of discrimination as a privacy harm.

#### 1.2.1.1. Price discrimination

Like Michael Froomkin (2000b) and Tal Zarsky (2003, 2004a), during the period under study a few scholars (Gratton, 2014; MacCarthy, 2011; Rubinstein, 2011; Willis, 2014) would keep

[68] This, in spite of a few scholars who even during this period would keep referring to discrimination as a possible harm without digging into its reach and scope (Ohm, 2010; Patterson & Nissenbaum, 2013; Tene & Polonetsky, 2012a, 2012b; Wu, 2013).

mentioning price discrimination as a specific harm. Not all of them, however, would consider it to be a *privacy* harm. For MacCarthy, for instance,

> Price discrimination occurs when firms charge different consumers different prices for access to the same good or service. Economists distinguish first-, second- and third-degree price discrimination. In first-degree price discrimination, the firm gathers as much information as possible about potential customers in order to assess demand. They are seeking to determine how valuable the good or service they sell is to these potential buyers so as to charge them the highest possible price they are willing to pay. *This clearly involves extensive information gathering and profiling of specific individuals and is the form of price discrimination that raises the most questions about privacy harms*. (2011, pp. 462–463)

Nevertheless, he would also point out:

> *But this description of the privacy harm is entirely circular*. The gathering and aggregating of data about potential customers violates privacy rights, goes the argument, because it leads to price discrimination, which for the sake of the argument is assumed to be injurious. But then the argument turns on its tail and declares that price discrimination is injurious because it rests on the privacy harm of gathering and aggregating data about potential customers.
>
> It is important to be clear about what the cause is and what the effect is in the privacy harm connected to price discrimination. *The harm in this case is the price discrimination that results in a net loss of social welfare*. As we have seen, it is sometimes hard to determine when a price discriminatory practice is harmful. Economic theory is not a reliable guide in this area. *But even if the information gathered for the discriminatory pricing has been gathered with full notice and consent, the harm can occur.* As we have seen in other cases, information gathering and analytic techniques can produce information about one set of data subjects that is derived from another set. Informed consent cannot protect against this kind of information leakage. *When there is a privacy harm resulting from price discrimination, it can be an external harm created by the leaky character of information*. (MacCarthy, 2011, pp. 467–468)

In this way, MacCarthy would question whether the injurious harm can be located in the gathering and aggregating of data about potential customers or in the implementation of price discrimination. For him, the loss of social welfare that can result from price discrimination is not a privacy harm *per se*.

#### 1.2.1.2. Invidious discrimination

In the same manner as between 2000 and 2007 (Chapter III), during this period several scholars (Crawford & Schultz, 2014; MacCarthy, 2011; N. Richards, 2014; Sweeney, 2013) would also refer to invidious discrimination—"discrimination against a protected class" (D. D. Hirsch, 2014b, p. 351)—as another privacy harm. Yet, during this covered period most of the scholars would expand the scope of this type of harm, to cover situations where companies would not explicitly use attributes such as race or gender to classify individuals, but would still rely on proxies. In 2014, for example, when talking about discriminatory housing practices, Kate Crawford & Jason Schultz would point out:

> The use of Big Data may allow landlords and real estate companies to shift away from general advertising in media outlets and circumvent anti-discrimination enforcement mechanisms *by isolating correlative attributes that they can use as a proxy for traits such as race or gender*. Such predictive practices already occur in other industries with the power of Big Data. (2014, p. 100)

Other scholars, like Dennis Hirsch, would also refer to discriminatory acts against a protected class (invidious discrimination), but would not consider them as a privacy harm. In Hirsch's words,

> Such practices can threaten both privacy *and* equal opportunity. *They injure privacy when*, without notice to or the consent of the individuals concerned, they infer and potentially reveal sensitive information such as pregnancy status, sexual orientation, political and religious views, or drug use. *They can result in unfair discrimination when* the disfavored attributes further correlate to a particular race, religion, gender or other protected class so that the model ends up denying important life opportunities to people in these vulnerable groups. (2014b, p. 346)

Thus, in a similar way to Similar to MacCarthy Hirsch would only consider the existence of a privacy harms when the data used to discriminate was collected in violation of the subject's rights to notice and consent.

Finally, in 2011 Paul M. Schwartz & Daniel J. Solove would consider that the classification of individuals according to their membership in certain groups was not an information privacy harm and should not be addressed by privacy law. According to these authors,

> Of course, *certain types of aggregate data can be used in harmful ways*. For example, banks might draw on a statistical indication that a certain demographic group has a much higher default rate to deny loans to members of this group or to charge them higher rates. In addition, actuarial data from insurance companies affects coverage and rate decisions. *These decisions can be harmful, and information does play a role in these harms. Nonetheless, this category of harm is far broader than the category of information privacy harms*. As a policy matter, these issues raise questions that predominately sound in civil rights, discrimination, and insurance law. At least as far as the analysis of aggregate data is concerned, *the critical issues in these areas are not those of information privacy law*. (2011, p. 1869)

As the next Chapter will show, though, if the "critical issues" here analyzed by Schwartz & Solove were read today through the lens of "the relational character of data" approach—which would be raised first by Mark MacCarthy (2011) (see below) and then by several scholars writing between 2015 and 2020—many scholars, including Solove himself, would likely include them nowadays as part of "the category of information privacy harms" (Solove & Schwartz, 2011, p. 1869).

#### 1.2.1.3. Novel spotted types of discrimination

Aside from price and invidious discrimination, during the reviewed period scholars would highlight three other novel ways in which discrimination could occur. First, Hirsch would explore the possibility of encountering harms in **cases where companies sort individuals without discriminating against a particular racial group or other protected class**. According to him,

> Denying employment, loans, housing, insurance, or other important opportunities and goods to those deemed to be at greater risk of a heart attack *would not constitute invidious discrimination* since these individuals would not fit the legal definition of "disabled" and so would not be members of a protected class. *But would it be harmful?* This is not an easy question to answer. Clearly, withholding jobs, loans, insurance, or housing imposes

> a significant cost on those denied access to them. Moreover, it seems unjust to deny these vital life opportunities to people who may never experience a heart attack and may even take steps to prevent one. From the perspective of the business, however, this sorting produces benefits. Assuming that they can identify those with a greater chance of a heart attack, and that these individuals really do perform less well as employees, borrowers, tenants, and life insurance customers, a company could justifiably be worried about transacting with them. (2014b, p. 352)

In the next and last studied period (2015-2020), many more scholars would join Hirsch in raising concerns about this sui generis and complex type of discrimination, which is usually based on innocuous characteristics.

Cynthia Dwork & Deirdre K. Mulligan (2013) and Danielle Keats Citron & Frank Pasquale (2014) would consider a second way in which discrimination would occur, namely, **instances where human biases are embedded in the technological tools used to sort people**. "[C]lassification systems are neither neutral nor objective, but are biased toward their purposes," Dwork & Mulligan would contend. "They reflect the explicit and implicit values of their designers. Few designers 'see them as artifacts embodying moral and aesthetic choices' or recognize the powerful role they play in crafting 'people's identities, aspirations, and dignity.' But increasingly, the subjects of classification, as well as regulators, do" (Dwork & Mulligan, 2013). Similarly, Citron & Pasquale would pose: "Because human beings program predictive algorithms, their biases and values are embedded into the software's instructions, known as the source code and predictive algorithms. Scoring systems mine datasets containing inaccurate and biased information provided by people" (2014, p. 4). However, similar to Hirsch, both couples of authors would consider these discriminatory outcomes as separate from privacy harms.

Finally, Citron & Pasquale (2014), as well as most authors studying abusive online conducts (D. E. Bambauer, 2014; Citron, 2009; Lipton, 2012) would emphasize a third type of discrimination: **the disparate impact of** these **abusive conducts**—and of **biased predictive**

**algorithms**, in the case of Citron & Pasquale—**on historically subjugated groups**. According to Citron, "[a]lthough in theory anonymous online mobs could attack anyone, in practice they overwhelmingly target members of traditionally subordinated groups, particularly women" (2009, p. 65). In a similar fashion, Derek E. Bambauer would contend that, "while rigorous data are not yet available, nonconsensual distribution appears to be *a gendered problem*. It seems to target women disproportionately" (2014, p. 2044).

During these years scholars would also refer to a harm greatly related to (or derived from) discrimination, being it **the denial of life opportunities such as employment, insurance, or housing**. Having been spotted by various scholars since the previous reviewed period (2000-2007), during these years several scholars[69] would keep emphasizing the problematic character of these decisions. In addition, taking into account "the merciless memory of digital recorders" (Chander, 2011, p. 116), some scholars (Chander, 2011; Crawford & Schultz, 2014; Matwyshyn, 2012; Yakowitz Bambauer, 2012) would raise concerns around the possibility that those decisions could be based in past actions of a younger self.

### 1.2.2. The erosion of due process guarantees

Another objective harm that began to be highlighted by a few scholars (Citron, 2008; Citron & Pasquale, 2014; I. Kerr, 2013) during this period was the dismantling of critical procedural safeguards by automated decision-making systems. Writing in 2008, Danielle Keats Citron would point out that "automation erodes the due process guarantees of notice and an opportunity to be heard. It assesses the myriad ways automation strips procedural integrity from administrative

[69] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (D. E. Bambauer, 2014; Gratton, 2014; D. D. Hirsch, 2014b; MacCarthy, 2011; Patterson & Nissenbaum, 2013; Rubinstein, 2014; Tene & Polonetsky, 2012a; Willis, 2014)

rulemaking, including the elimination of notice-and-comment participation, transparency, and political accountability" (2008, p. 1258). Similarly, Ian Kerr would emphasize how "predictive technologies threaten due process by enabling a dangerous new philosophy of preemption" (I. Kerr, 2013, p. 92). Interestingly, these scholars writing about procedural injustice would not explicitly frame it as a privacy harm, but simply as a harm to due process.

### 1.3. Sparse but visionary references to other harms/circumstances

Finally, two remaining harms—manipulation (Calo, 2014; N. Richards, 2014) and diminished exposure to differing perspectives (Dwork & Mulligan, 2013; MacCarthy, 2011)—were not mentioned widely during these years. Nonetheless, given the relevance that they would receive in the last period reviewed (Chapter V), it is worthwhile to trace their roots in this sample.

Joining Joel Reidenberg (1995), Dorothy J. Glancy (1995), Helen Nissenbaum (1997), and Tal Zarsky (2003, 2004a, 2004b), in 2014 Ryan Calo would also refer to **manipulation** as a harm to consumer autonomy. However, unlike previous authors, he would be the first one to dig deeper into the *modus operandi* of this harm. According to Calo, thanks to the digitization of commerce, firms have the ability to exploit consumers' irrationality, defined by him as "the measurable departures from the self-interested course that autonomous subjects generally follow" (2014, pp. 1032–1033). In turn, in terms of **the narrowing of perspectives**, Cynthia Dwork & Deirdre K. Mulligan would denounce the "the social fragmentation of 'filter bubbles' that create feedback loops reaffirming and narrowing individuals' worldviews" (Dwork & Mulligan, 2013, p. 37).

Interestingly, both Calo and Dwork & Mulligan would place these harms outside of the privacy sphere. Thus, while Calo would present the harm to autonomy as a separate harm from the harm to privacy, Dwork & Mulligan would explicitly state that "[t]he decreased exposure to differing

perspectives, reduced individual autonomy, and loss of serendipity that all result from classifications that shackle users to profiles used to frame their 'relevant' experience, *are not privacy problems*" (2013, p. 37).

Finally, during the studied period Mark MacCarthy would point to a characteristic of harms that, although poorly explored by then, would become very important in the reviewed scholarship during the years to come. In 2011 MacCarthy raised the concept of "**negative privacy externalities**," "where one person's decision to share information can adversely affect others who choose o remain silent. The idea is that disclosure of information by some people can reveal information about other people, to their detriment" (MacCarthy, 2011, p. 429). As will be seen un Chapter V, starting in 2015 this characteristic would become massively spotted by scholars.

## 2. Proposed privacy tools

In striking contrast with the first years of the twenty first century (Chapter III), and to many of the FIPs-based proposals that had finally come to be suggested by the US governments in the form of FTC and White House reports, during the first seven years of PLSC an increasing number of scholars would begin to identify several limitations of various of the FIPs principles to cope with the Information Age. Consequently, they would either propose to adapt some of their key concepts and principles to the Digital Age (e.g., notice and consent mechanisms, the concepts of sensitive data or PII), suggest both old (i.e., Tort law) and innovative alternatives (e.g., social norms, co-regulatory arrangements) to them, or resort to other areas of law (e.g., Tort law, Intellectual Property law, Contract Law, Consumer Protection law, Environmental law) for inspiration. Finally, piggybacking on one of the FTC reports cited above, a remaining group of FIPs adherents

would propose implementing them not through statutes, but rather through Privacy by Design ("PbD").

If the scholars' previous overwhelming claims about the necessity of FIPs-based legislation had marked a second turning point in the American scholarly discussion about regulatory techniques to protect information privacy, this new change of direction would represent a third and last turning point.

### 2.1. Backlash against the FIPs

In contrast to the 2000-2007 period, where scholars' faith on comprehensive FIPPs-based federal privacy laws grew exponentially, during the years under study several scholars would begin to refer to the limitations of many of the FIPs principles against the framework of the Information Age.

Among these scholars, most of them[70] would highlight the useless character of the *notice and choice principles*, also questioning the "voluntary" and "informed" character of consent. According to Omer Tene and Jules Polonetsky, for example,

> [b]y emphasizing "transparency and user consent," in European data protection terms, or "notice and choice," in United States parlance, the current legal framework *imposes a burden on business and users that both parties struggle to lift*. Users are ill placed to make responsible decisions about their online data—given, on the one hand, their *cognitive biases and low stake in each data- (or datum-) transaction* and, on the other hand, the *increasing complexity of the online information ecosystem*. Indeed, even many privacy professionals would be hard pressed to explain the inner-workings of the online market for personal information, the parties involved, and the actual or potential uses of information. *Imposing this burden on users places them at an inherent disadvantage and ultimately compromises their rights*. It is tantamount to imposing the burden of health care decisions on patients instead of doctors. (2012a, p. 285)

[70] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Crawford & Schultz, 2014; Culnan, 2011; D. D. Hirsch, 2014a; Peppet, 2012; Sloan & Warner, 2014; D. J. Solove & Hartzog, 2014; Tene & Polonetsky, 2013, 2012a; Warner & Sloan, 2012; Willis, 2014)

Thus, building on what they had been identifying around the so-called "privacy paradox," scholars would begin to frame the "consent" as a burden imposed over subjects who lacked the knowledge necessary to make informed and objective decisions about their personal data.

In addition, scholars would also criticize the principles of *data minimization*[71] (Swire, 2012; Tene & Polonetsky, 2012b) and *purpose limitation* (Bambauer, 2012; Hirsch, 2014a) as anachronic. With regards to the first one, Peter Swire would for example argue:

> the idea of data minimization serves as a useful reminder, for those who process personal information, that data should not be collected, used, or retained where it can cause harm and is not needed. *We live in an information age, however. The goal simply cannot be to minimize and protect against uses of data*. Data empowers individuals as well as risks the possibility of harm. Other stakeholders will push for access to personal data, such as corporations targeting advertisements, the state doing law enforcement, and medical and other researchers trying to make new discoveries. Those of us who have participated in privacy debates are familiar with these stakeholders and their usually utilitarian arguments for acquiring the data. The additional point here is *that individuals themselves have the tension between data minimization and data empowerment*. Regulators and advocates who focus on outcomes for the individual face difficult questions about when either empowerment or minimization will favor the individual. The tension within each of us is a tension facing regulators as well. *I believe considerable further debate and research is needed to clarify the conditions under which data minimization and data protection are the correct concepts going forward, and when instead to consider explicitly the benefits to the individual from data empowerment*. (2012, p. 1414)

And referring to the principle of *purpose limitation*, Dennis Hirsch would argue that "[p]urpose limitations *create a direct conflict with Big Data*, the value of which lies in continuously re-purposing massive data sets and finding new and unanticipated uses for them" (2014a, p. 391). Similarly, Jane Bambauer would contend:

[71] As described by Ira Rubinstein in 2014, this principle was a new addition to the original list of FIPs proposed by the U.S. Department of Health, Education, and Welfare (HEW). According to Rubinstein "[o]ver the years, these five core HEW principles have been expanded, contracted, codified, and critiqued. Among the more important additions to the HEW principles are data minimization, limits on data retention, and accountability" (Rubinstein, 2014, pp. 888–889).

> Consider, for example, the purpose limitations of FIPs, which constrain a holder of data from using it for any purpose other than that for which it was collected. *This rule allows privacy interests to trump other important societal values.* Imaginative repurposing of data is now common practice for public health and security, sports and entertainment, and even core political activities, (…). (2012, pp. 219–220).

Even, Kate Crawford & Jason Schultz would question the utility of the concept of *personally identifiable information (PII)*, central to the FIPs-type laws. According to these authors,

> Even the anchoring concept of most modern privacy regulations— PII—may fail to provide a sufficient nexus for future Big Data privacy regulation. *Big Data's analytics are simply too dynamic and unpredictable to determine if and when particular information or analyses will become or generate PII*. Instead, one may only observe the problem in hindsight, such as with predictive policing or in the Target pregnancy case. (2014, p. 107)

Hence, between 2008 and 2014, many of the scholars here studied would begin to identify foundational elements and principles of the FIPs that would be at odds with the Information Age and the Big Data revolution.

### 2.2. Proposed adaptations to key elements of the FIPs

As a consequence of the identified FIPs' limitations, during these years many scholars would suggest certain adaptations to some of the FIPs' key elements. For example, acknowledging that "when sensitive data are involved, stronger procedural protections are warranted" (2013, p. 720), Neil Richards would propose to extend the concept of *sensitive information* to cover reader records.

Similarly, when it comes to the concept of *PII*, several alterations would be proposed between 2008 and 2014. In 2010, in the face of the demise of robust anonymization and the fact that by then, almost any piece of data could be related to some identifiable individual, Paul Ohm would suggest a radical solution: "we must abandon the pervasively held idea that we can protect privacy

by simply removing personally identifiable information (PII). This is now a discredited approach. Even if we continue to follow it in marginal, special cases, we must chart a new course in general" (Ohm, 2010, p. 1742). What would that new course look like? Ohm would propose a five-factors test "to assess the risks of reidentification and carefully balance these risks against countervailing values" (2010, p. 1776). Thus, "[i]f the risk is very low, regulators might choose to do nothing. If the risk is very high, regulators should feel inclined to act, imposing new restrictions on data collection, use, processing, or disclosure, and requiring specific data safe-handling procedures" (2010, p. 1768). The latter, through sectoral FIPs-type laws with targeted, enhanced obligations.

Considering Ohm's proposal too radical and a threat to privacy law's regulatory boundaries, in 2011 Paul Schwartz & Daniel Solove would suggest an alternative to abandoning the PII concept: develop a new conception, PII 2.0, which would be based on two different categories of PII—"identified" and "identifiable" data, each of which would be treated differently. Thus, drawing on a standard-based approach, "this approach allows for legal safeguards for both identified and identifiable information-safeguards that permit tailored FIPs built around varying levels of risk to individuals" (2011, p. 1877).

Finally, although referring to the concept of *personal information* instead of PII, in 2013 Eloise Gratton would propose "*a new method of interpreting the notion of personal information*, one which takes into account the ultimate purpose behind the adoption of [Data Protection Laws] DPLs which was to protect individuals against a risk of harm which may take place upon organizations collecting, using or disclosing their personal information" (2014, p. 6).

However, not everyone would agree with intervening the concept of PII. Felix T. Wu, for example, would question the bases of this whole discussion about PII. According to him, "[o]ne cannot talk about the success or failure of anonymization in the abstract. Anonymization

encompasses a set of technical tools that are effective for some purposes, but not others. What matters is how well those purposes match the law and policy goals society wants to achieve" (2013, p. 1126).

Besides sensitive information and PII, another key element of the FIPs intervened by scholars writing about privacy during this period would be the *privacy notices* and *consent mechanisms*. Central to the notice and choice principles, these figures would receive a lot of attention by scholars during the years under study. One possible reason for this increased attention could be a study published by Carnegie Mellon researchers Aleecia M. McDonald & Lorrie Faith Cranor in 2008 and highly cited by American privacy law scholars (Bamberger & Mulligan, 2011; Hartzog & Stutzman, 2013a; MacCarthy, 2011; Ohm, 2013; N. Richards, 2014; Tene & Polonetsky, 2012a) during this period. According to this study's results, "an average person would expend 81 to 293 hours per year were they to skim the privacy policy at each website visited, and 181 to 304 hours if she actually read them" (Bamberger & Mulligan, 2011, p. 297). Another possible reason, in turn, could also be the FTC's support to the Do Not Track (DNT) approach to behavioral advertising.

For whatever reason, during these years scholars would propose several ideas to improve the privacy notices and consent mechanisms. As in previous years, some scholars would keep grappling with the opt-in/opt-out dichotomy (MacCarthy, 2011; N. Richards, 2013; Rubinstein, 2014; Tene & Polonetsky, 2012a, 2012b; Warner & Sloan, 2012; Willis, 2014). However, unlike prior proposals, many of these articles would look for option combinations and creative alternatives. For example, instead of a binary choice between opt-in and opt-out, Mark MacCarthy would propose a continuum of choice regimes. According to him,

> Notice and opt-out would be an appropriate policy response *when the information practice in question is closer to the public benefit use*. Notice and opt-in would be the appropriate policy *when the information practice is riskier, closer to the harmful uses*. Easy opt-in choice is especially problematic when an information practice has substantial

> external information effects that spread the harmful effects beyond those who have chosen to participate in it. (2011, p. 475)

In a similar fashion, Tene & Polonetsky would claim that "[s]ome activities are value creating, socially desirable, and minimally intrusive; they should be permitted to exist as default options. Other activities are privacy intrusive, socially menacing, and may inflict real harm on users; they should be prohibited absent users' informed, explicit, opt-in consent" (2012a, p. 341). For them, the debate about a DNT mechanism disguised a more fundamental normative discussion about the desirability of allowing behavioral advertising, and more generally, about the type of practices that a society would consider desirable. In fact, in a parallel article they would even explore the possibility of allowing certain "legitimate" uses without consent. In that sense, they would

> call for the development of *a model where the benefits of data for businesses and researchers are balanced against individual privacy rights*. Such a model would help determine whether processing can be justified based on legitimate business interest or only subject to individual consent, and whether consent must be structured as opt-in or opt-out. (2012b, p. 69).

Besides this defaults' discussion, other scholars would be even more innovative with regards to modifying the privacy notices. In 2010, for example, Ryan Calo would propose to rely on anthropomorphic design to provide "visceral notices." According to him, "placing an apparent agent at the site of data collection can help line up user expectations about how data will be used with the actual practices of the entity collecting that data" (2010, p. 7).

### 2.3. Alternatives to the FIPs

As had also happened in previous years, scholars would also propose alternatives to the FIPs. While some of them would keep going back to Tort law, other innovative alternatives would

include a focus on social norms, co-regulatory configurations, and other two proposals that although not widely spread at the time, would become widely popular over the years.

### 2.3.1. An old known alternative: Tort law

Between 2008 and 2014 a reduced number of scholars (Chander, 2011; Peek, 2009; Strahilevitz, 2010; Yakowitz Bambauer, 2012) would keep proposing a—by then—old alternative: a return to privacy's American origin—Tort law. For Marcy Peek, "the values of information privacy law embodied in the four traditional privacy torts (and essentially conceived in the late nineteenth century in a fundamentally different world) might be reconstrued" (2009, p. 64). Similarly, Lior Jacob Strahilevitz would argue for a reunification within privacy tort law itself and for the consequent establishment of a "unified tort with three essential elements—privacy, highly offensiveness, and negative effects on social welfare—" (2010, p. 2011).

Within this same trend, other authors would focus their attention on specific privacy torts. Anupam Chander (2011) would recommend judges to reinvigorate the tort of *public disclosure of private facts* to respond to the unconsented dissemination of nude photographs and videos online. Jane Bambauer (2012), in turn, would highlight the tort of *intrusion upon seclusion* as the best avenue to intervene the stage of information flow commonly known as observation, by imposing liability for conduct-offensive observations. According to Bambauer, "[i]ntrusion has great, untapped potential to address privacy harms created by advances in information technology. Though the tort is associated with conduct in real space, its principles apply just as well to operations in the era of Big Data" (2012, p. 207).

### 2.3.2. Innovative alternatives

Despite the constant re-emergence of this old alternative approach, the period under study could generally be characterized as one of high innovation in terms of alternative solutions. In particular, four proposed tools stood out during these years.

#### 2.3.2.1. Social norms

First, scholars opened the door for the remaining "constraint" proposed by Lawrence Lessig (1999) since 1999, which unlike the law, technology, and the market, had still not been proposed, namely, social norms. While this was the first reviewed period in which there was little discussion of market solutions, social norms for the first time played an important role in American privacy law scholarship during these years. Since 1998, Helen Nissenbaum (1998, 2004) had been urging scholars to understand privacy through the concept of "contextual integrity." However, it was with the publication of her 2009 book *Privacy in Context*—and with the incorporation of the "respect for context" principle into President Obama's proposed Consumer Privacy Bill of Rights in 2012—that the role of social norms became preponderant in scholarship.

For Nissenbaum (2009), a privacy violation occurs when a given practice violates context-dependent social norms, therefore threatening "contextual integrity." Thus, the appropriateness of information flows depends on whether they respect informational norms present in specific contexts. Several scholars writing between 2010 and 2014[72] would borrow from this idea to: (i)

[72] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Bamberger & Mulligan, 2011; boyd & Marwick, 2011; Brandimarte et al., 2013; Culnan, 2011; Fan, 2011; Hartzog, 2014; I. Kerr, 2013; J. King, 2012; Madejski et al., 2012; Ohm, 2010; Patterson & Nissenbaum, 2013; N. Richards, 2014; Rubinstein, 2014; Rubinstein & Good, 2013; Schwartz & Solove, 2011; Sloan & Warner, 2014; D. J. Solove & Hartzog, 2014; Tene & Polonetsky, 2013, 2012b, 2012a; Warner & Sloan, 2012; Wu, 2013)

argue that the privacy implications of a given use of personal information is contextual; and/or (ii) propose their own context-based solutions.

In 2011, for instance, danah boyd and Alice Marwick would "discuss the implications of teens' practices, revealing the importance of social norms as a regulatory force" (2011, p. 2). According to them,

> Fundamentally, privacy is a social norm. Legal regulation is legislated to protect individuals from harm. The market competes in opposite directions, trying to "win" both by enhancing privacy and leveraging opportunities to invade people's privacy for financial gains. Likewise, technologies will be built both to protect and erode privacy. But when it comes to social privacy, *the biggest battles will be around the social norms that regulate it. In other words, what is socially appropriate in networked publics?* How are norms signaled and violations recognized? What social sanctions can be used to curb violations? There are no clear answers to this, but *what is clear is that teenagers are working hard to bring social norms into the equation*. They're developing strategies for managing privacy in public spaces as they try to assert control over social situations. They may not always be successful, and they may consistently face violations of their privacy, but they are not discarding privacy as a result. (2011, p. 26)

Similarly, in 2012 Michelle Madejski, Maritza Johnson, and Steven M. Bellovin would suggest:

> One of the largest culprits for privacy flaws is Facebook's reliance on data types (e.g., photos, events, and status updates) for defining privacy settings. These data types are misrepresentative of the real world that Facebook attempts to model. Outside of a social network, an individual does not determine visibility of personal data by its format but instead *by the context of its information*. *A key improvement would be to automatically categorize information with a predicted context, and define privacy settings per context that reflect the user's intent*. (2012, p. 344)

In a similar fashion, in three consecutive articles Richard Warner & Robert H. Sloan would recommend creating value-optimal, role-appropriate informational norms (Sloan & Warner, 2014; Warner & Sloan, 2012, 2014). Likewise, in 2013 Tene & Polonetsky would invite policymakers to "recognize that *social norms* are rarely established by regulatory fiat, and that laws that fail to reflect techno-social reality may not fare well in the real world. Whether legislating or encouraging

self-regulation, *understanding how social norms are evolving* is essential in order to avoid crude or heavy-handed interventions." (2013, p. 101). Additionally, another related context-based solution also proposed by Tene & Polonetsky (2012a) would be to go back to normative questions, identifying the social norms that underlie discussions about a given technology. Similarly, when referring to the re-identification debate mentioned above, Tene & Polonetsky would once again contend: "the seemingly technical discussion concerning the scope of information viewed as personally identifiable masks a fundamental *normative question*. Policymakers should engage with this normative question, consider which activities are *socially acceptable, and spell out the default norms accordingly*" (2012b, p. 66).

#### 2.3.2.2. Co-regulation

A bigger group of scholars (Bamberger & Mulligan, 2011, 2013; Culnan, 2011; D. D. Hirsch, 2013; Rubinstein, 2011; Tene & Polonetsky, 2012a) would in turn propose to explore different forms of co-regulation. In contrast to command-and-control governance, the principal ideas of the co-regulatory approaches proposed by these scholars are: (i) to prioritize regulatory flexibility; and (ii) adjudicating some type of responsibility to companies.

By studying corporate privacy management—also referred to as "privacy in the ground"—as well as the FTC's "'soft' regulatory tools" (2011, p. 295) and its "entrepreneurial use of its enforcement powers" (2011, p. 279), in 2011 Kenneth A. Bamberger & Deirdre K. Mulligan would conclude that

> [f]raming legal mandates broadly leaves space for *discretion* in implementation. By permitting heterogeneous and flexible methods of compliance in individual firm contexts, such framing provides a means for *enlisting the judgment of firm decisionmakers*, drawing on their superior knowledge both about the ways risks manifest themselves in individual firm behaviors and business lines and about available risk-management capacities and processes. It further accords regulators *continuing flexibility in the face of uncertainty* as

> to how public goals should be furthered in diverse and heterogeneous contexts and quickly shifting landscapes over time. (2011, pp. 304–305)

In a similar fashion, in her 2011 article Mary J. Culnan would propose "augmenting the current approach with new regulations based on accountability where *firms are delegated responsibility* to develop risk management programs for privacy tailored to their individual circumstances" (2011, p. 15). That same year, Ira Rubinstein (2011) would propose different strategies for privacy regulatory innovation, such as a program for the FTC to negotiate agreements with individual companies to modify or relax existing regulatory requirements in exchange for the adoption of privacy-friendly PETs; negotiated rulemaking to tackle the DNT discussions; and a co-regulatory approach to rulemaking. Similarly, taking inspiration from Dutch privacy regulation, in 2013 Dennis Hirsch would support the idea of implementing "collaborative governance"—a term drawn from regulatory theorists. According to Hirsch,

> "collaborative governance" [is] a hybrid form of regulation in which government, industry, and, potentially, other stakeholders *collaborate on the drafting and/or enforcement of rules*. The proponents of collaborative governance claim that it can combine *the flexibility and business savvy* of industry self- regulation with the *accountability and public-spiritedness* of government rules. Such a blended approach might provide a way to transcend the current political impasse and pass comprehensive legislation to protect individual privacy in the digital economy. (2013, p. 88).

#### 2.3.2.3. Other innovative alternatives

During these years, two other innovative solutions were proposed as alternatives to the FIPs. Although less popular at the time compared to social norms and co-regulation, its reception by scholars would significantly grow in the years to come. First would be Latanya Sweeney (2013) and Cynthia Dwork & Deirdre K. Mulligan's (2013) idea to **rely on Computer Science and employ technical tools to tackle unfairness**. In Sweeney's view,

> The good news is that we can use the mechanics and legal criteria described earlier to *build technology that distinguishes between desirable and undesirable discrimination* in ad delivery. Key components are: (1) identifying affected groups; (2) specifying the scope of ads to assess; (3) determining ad sentiment; and (4) testing for adverse impact. (Sweeney, 2013, p. 16)

Likewise, Dwork and Mulligan consider that besides of privacy and transparency, the classifications and segmentation produced by big data analysis should be tackled through computer science's proven strategies. According to them,

> In computer science and statistics, the literature addressing bias in classification comprises: testing for statistical evidence of bias; training unbiased classifiers using biased historical data; a statistical approach to situation testing in historical data; a method for maximizing utility subject to any context-specific notion of fairness; an approach to fair affirmative action; and work on learning fair representations with the goal of enabling fair classification of future, not yet seen, individuals.
> Drawing from existing approaches, a system could place the task of *constructing a metric*—defining who must be treated similarly—*outside the system*, creating a path for external stakeholders—policymakers, for example—to have greater influence over, and comfort with, the fairness of classifications. *Test files* could be used to ensure outcomes comport with this predetermined similarity metric. While incomplete, this suggests that there are opportunities to address concerns about discrimination and disadvantage.

The second less generalized but still innovative alternative would be to establish **substantive standards and prohibitions**. Following the steps of Julie Cohen (2003), during these years a small group of scholars (D. D. Hirsch, 2014b; MacCarthy, 2011; Ohm, 2010) would begin to suggest this approach as an alternative to the simple procedural safeguards at the base of the FIPs. For Paul Ohm, for example, "[i]f the costs significantly outweigh the benefits of information flow, regulators might *completely ban* the dissemination or storage of a particular type of information" (2010, p. 1769). Relatedly, both Mark MacCarthy (2011) and Hirsch (2014b) would propose the use of an unfairness framework to identify—among other possibilities—impermissible collection and/or uses.

### 2.4. Tools based on other areas of law

Finally, and also probably as a result of the limitations identified in some of the FIPs, between 2008 and 2014 American privacy law scholars would increasingly draw from other areas of law for inspiration. A first area—**Fiduciary law**—had been already explored by Ian Kerr (2001) in the previous period. However, it would only be until these studied years when several scholars would start to look into what a fiduciary duty—mainly the duty of confidentiality—could look like in relation to data.

For example, looking to protect intellectual privacy in the digital age, both in 2008 and 2013 Neil Richards would propose that search engines, online bookstores, ISPs, and providers of physical and streamed video be treated as information fiduciaries, being therefore subject to meaningful requirements of confidentiality (N. Richards, 2008, 2013). Similarly, in the wake of self-surveillance technologies, Jerry Kang, Katie Shilton, Deborah Estrin, & Jeff Burke would recommend the creation of the Privacy Data Guardians (PDGs), a new kind of professionals who would have a fiduciary relationship with data subjects. According to Kang and his co-authors,

> The PDG would embrace a professional identity of expertise and service, as has been done by other professionals such as lawyers, accountants, financial planners, and librarians. Their role ideology would include the core idea of acting as trustworthy confidantes on behalf of their clients (vis-a-vis third-party snoops, subpoenas, and government surveillance), zealous advocates who negotiate for best informational terms vis-a-vis third-party application service providers (3P-ASPs), and wise counselors to their individual clients about their decisions regarding self-surveillance data. (2012, pp. 828–229)

Relatedly, in 2014 Woodrow Hartzog would provide courts with a decision-making framework to impose implied obligations of confidentiality to members of certain online communities. In Hartzog's words,

> Confidentiality, which is, according to one definition, "the state of having the dissemination of certain information restricted," focuses not on the nature of the

> information as public or private but rather on the nature of the relationship or agreement between parties. Even if self-disclosed information is not "private," it could be disclosed in confidence. Under the law of confidentiality, courts can largely *avoid the difficult question of whether information was private or offensive and focus instead on whether a trust was breached*. (2014, p. 768)

In fact, as had already happened in the previous studied period (2000-2007), during these years the concept of trust would also be highlighted by some scholars. For example, among his five proposed factors for assessing the risk of privacy harm, Paul Ohm would include trust. According to him, "[r]egulators should try to craft mechanisms for instilling or building upon trust in people or institutions. (…) We might, for example, conclude that we trust academic researchers implicitly, government data miners less, and third-party advertisers not at all, and we can build these conclusions into law and regulation" (2010, pp. 1768–1769). In a similar fashion, in 2011 Bamberger & Mulligan would find that within corporations, "[p]rivacy was portrayed as an expansive concept: privacy 'equates to trust,' 'is a strategic initiative,' and is 'a core value associated with trust, primarily, and integrity and respect for people'" (2011, p. 280)

However, not everyone would agree with relying on trust relationships and consequent duties of confidentiality to protect privacy. In 2012, for example, Bambauer would contend that "[s]ome existing privacy laws unwisely create confidentiality duties for relationships with only marginal amounts of trust" (2012, p. 265) According to her, "[f]or sectors that do not have a quasi-fiduciary responsibility with the consumer, *assigning a duty of confidentiality unduly encumbers relationships that are not ones of unusual trust.* In addition to lost information, the public would bear the costs of administering a strong privacy system. These costs are considerable" (2012, p. 264).

A second area of law explored by various scholars was that of **Administrative law**. Worried about the procedural injustices that would derive from the application of automated decision-

making systems, some scholars would agree on the necessity of protecting what Danielle Keats Citron would coin as "technological due process." "This technological due process provides new mechanisms to replace the procedural regimes that automation endangers," Citron would argue. "In certain instances, surrogate rules can be used to protect the transparency, accountability, and fairness of rulemaking and adjudication. In others, new standards can be implemented to prevent trick procedurally defective rulemaking and arbitrary government decision making" (2008, p. 1258). According to her, legal principles for today's automated systems could include meaningful notice, protections for hearings, public source codes of systems, testing of systems' software, participation in the building of automated decision systems, and non-automation of interpretative rules and policy statements.

Following suit, but in light of predictive technologies, Big Data, and automated scoring systems used in the private sector, Ian Kerr (2013), Kate Crawford & Jason Schultz (2014), and Citron & Frank Pasquale (2014) would nevertheless depart from Administrative law, proposing to expand these procedural data due process principles and safeguards—and others, such as independent review/oversight (Citron & Pasquale, 2014; Crawford & Schultz, 2014), licensing and audit requirements, and risk assessment reports (Citron & Pasquale, 2014)—to address automated decision-making systems employed in private companies.

Finally, other areas of law explored by a few scholars during these years include: (i) **Civil Rights law** to respond to online mobs (Citron, 2009) ; (ii) **Intellectual Property law** to fix information-quality problems during privacy lurches—through Trademark law (Ohm, 2013)—and regulate the production and distribution of intimate photos and videos online—through Copyright law (D. E. Bambauer, 2014)—; (iii) **Contract law** to protect confidentiality in online communities (through the doctrine of promissory estoppel) and enforce website features and design as code-

based promises (Hartzog, 2009, 2011); (iv) **Consumer Protection law** to align corporate incentives with those of consumers in the context of digital market manipulation (Calo, 2014); and **Environmental law**, as a model to identify specific policies, legal doctrines, and government environmental investments from which analogy could be drawn to protect privacy from "data spills" and "the glass house effect," in which layer upon layer of personal information "give (…) each of us the sense that we are living in a glass house" (Hirsch, 2014a, p. 376). Right at the start of the next studied period (2015-2020), Michael Froomkin (2015) would similarly join Dennis Hirsch in analyzing Privacy Impact Notices ("PINs") in light of the already known Environmental Impact Statements ("EIS") and calling for the regulation of mass surveillance as privacy pollution.

### 2.5. Privacy By Design

Lastly, while other scholars would keep having faith in the power of the FIPs, they would prefer to implement them through technology/architecture instead of law. Although scholars' focus on architecture, and more concretely Privacy Enhancing Technologies ("PETs"), was not new at this point in time, the FTC's inclusion of Privacy by Design ("PbD") as one of the central axes for future regulation of online privacy in its report *Protecting Consumer Privacy in an Era of Rapid Change* could probably have influenced these scholars' renovated approach to "code is law."

Even before the release of the FTC's preliminary report in 2010, some scholars had already been talking about building privacy protections into technology. Following Julie Cohen's pioneer approach (2003), in 2008 Danielle Keats Citron would also claim that "[a]utomated systems must be designed with transparency and accountability as their primary objectives, so as to prevent inadvertent and procedurally defective rulemaking" (2008, p. 1308). However, it was not until

2011 that the concept of Privacy by Design was formally introduced into the sample of articles here reviewed.

Although proposed by several scholars between 2011 and 2014,[73] Ira Rubinstein, Nathaniel Good, Woodrow Hartzog, and Frederic Stutzman seem to have provided the most comprenhensive approaches to PbD during this period. In 2011, Rubistein published an article titled *Regulating Privacy by Design,* intended to "clarify the meaning of privacy by design and to suggest how privacy officials might develop appropriate regulatory incentives that offset the certain economic costs and somewhat uncertain privacy benefits of this new approach" (2011, p. 1413). According to him, unlike PETs, "privacy by design is not a specific technology or product but a systematic approach to designing any technology that embeds privacy into the underlying specifications or architecture" (2011, pp. 1411–1412). In his view, both if Congress finally enacted a privacy law and authorized FTC rulemaking, or if it failed but the FTC continued to play an activist role in defining comprehensive privacy programs through enforcement actions, the FTC may be able to require commercial firms to implement PbD. As Rubinstein himself would explain,

> In the absence of new legislation, the FTC may continue to pursue strategic enforcement actions and, on its own or in conjunction with the DOC, convene experts from industry, advocacy groups, and academia to develop best practices for privacy by design. Alternatively, new legislation may authorize FTC-supervised experimentation with innovative regulatory approaches that relax one-size-fits-all requirements in exchange for better privacy results, negotiated solutions to emerging regulatory challenges such as how best to implement a "do not track" rule, and/or the use of safe harbor programs that permit flexible self-regulatory arrangements for implementing CIPPs subject to FTC oversight and enforcement. (2011, p. 1453)

[73] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Bamberger & Mulligan, 2013; Hartzog & Stutzman, 2013b; Hoepman, 2014; J. King, 2012; Rubinstein, 2011; Rubinstein & Good, 2013; D. J. Solove & Hartzog, 2014; P. Swire, 2012; Tene & Polonetsky, 2013, 2012a)

In 2013, in turn, Woodrow Hartzog & Frederic Stutzman published their article *Obscurity by Design*. Building on their previous piece *The Case for Online Obscurity*, in this article Hartzog & Stutzman looked to address how designers should approach the implementation of Privacy by Design in social technologies. In their view,

> [t]he current goal of design solutions is "privacy," which is too broad and opaque to provide meaningful guidance in designing social technologies. (…) This Article *recommends looking to the related concept of obscurity*. Empirical evidence demonstrates that Internet users aim to produce and rely upon obscurity to protect their social interaction online. The concept of online "obscurity," defined here as a context in which information is relatively difficult to find or understand, is a much more defined and attainable goal for social technology designers. Obscurity is more flexible than some conceptualizations of privacy and also more feasible to implement. Moreover, obscurity involves more than prohibitions on conduct; internet users can actively produce obscurity themselves. (2013b, p. 388)

Finally, that same year Rubinstein & Nathaniel Good would publish another article titled *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*. Using recent privacy incidents involving Google and Facebook as examples, in this article Rubinstein & Good looked to

> analyze privacy by design from two complementary perspectives: privacy engineering, which refers to the design and implementation of software that facilitates privacy, and usable privacy design, which refers to design tasks involving human-computer interaction ("HCI"). The former focuses on building software *to satisfy the abstract privacy requirements embodied in the FIPs* (in some cases overlapping with security engineering), the latter on ensuring that users understand and benefit from well-engineered privacy controls. (2013, p. 1342)

No matter their different approaches, almost all scholars writing about Privacy by Design during this period would stress two main ideas: (i) the necessity to develop concrete ways to translate the FIPs into engineering principles and practices; and (ii) the need for policymakers to provide incentives to target the market failures that impede the adoption of Privacy by Design strategies in the private sector.

***

Several reflections can be drawn from this Chapter. In a sense, this period could have been characterized as "business as usual" for privacy law scholars if, during these years, they had limited themselves to identifying traditional privacy harms, including lack of control over one's personal information, reputational harms, "the chilling effect," and physical and financial harms. Yet, scholars approached the eventful techno-legal context described in Section A not only with newly identified harms, but also with a nascent different approach to addressing them.

The new harms raised by scholars—discrimination and the erosion of due process guarantees—stand out for two reasons. First, both harms can be characterized as *objective* or *consequential*. According to Ryan Calo, "[t]he objective category of privacy harm is the unanticipated or coerced *use of information* concerning a person *against that person*. These are *negative, external actions justified by reference to personal information*" (2011a, p. 1133). Relatedly, Ignacio Cofone has offered the concept of "consequential harms" to refer to those "[h]arms that *are enabled by a loss of privacy*;" "they are harms that are external to privacy interests but *occur as a consequence of privacy violations*" (2022, p. 1396).

Therefore, unlike subjective harms such as reputational harms or the "chilling effect"—which are "unwelcome mental states (…) that accompany the belief that one is or will be watched or monitored" (Calo, 2011a, p. 1133)— , discrimination and erosion of due process guarantees take place outside of the individuals' subjectivities, as a negative externality or downstream consequence of a previous or concomitant loss of privacy. As a result, instead of being identified in psychological or dignitary effects, they are usually seen as tangible consequences (e.g., an opportunity loss).

Interestingly, the tangible character of these newly identified harms can be seen, in particular, when contrasted with the type of harms discussed in Chapter III. During the period there studied (2000-2007), scholars were mostly concerned about the lack of control over one's own life and the reduction of the individual to a set of data points. While these harms are clearly related to metaphysical and dignitary matters, which revolve around an individual's own sense of worth and ownership, discrimination and the erosion of due process protections go beyond the individual's psyche and reflect on tangible, material effects.

Second, in contrast to the other objective harms also identified during this period (e.g., physical and financial harms), discrimination and erosion of due process guarantees usually result from the *actual processing phase* of the data cycle. Thus, even though the physical and financial harms also identified by scholars can happen after the simple collection of personal data (e.g., access to a bank account's routing number or to a residential address), the harms of discrimination and erosion of due process guarantees here described often need of the application of the different data analysis techniques identified by this community of scholars over the years.

Similarly, the privacy tools proposed by the scholars during these years are noteworthy, for their departure from the path taken by this intellectual community over the previous seventeen years. While between 1990 and 2007 scholars had been steadily increasing their support for FIPs-based solutions, gradually walking towards a "new privacy" (Schwartz & Treanor, 2003), during the period under review many of them would begin to consider the shortcomings or limitations of those proposals. As a result, and similar to what happened in the first period covered in Chapter II, what we can witness through this Chapter are years of much regulatory innovation by these scholars, resulting in a state of flux very similar to the one initially reported in Chapter II.

Lastly, the scholars' criticism of the FIPs contrasts sharply with the FTC's and the White House's demonstrated interest in implementing these principles. At the same time, it is also interesting to observe how, many of the alternative proposals made by the scholars over these years would also begin to be reflected in the Executive branch's reports issued in this period. In particular, the following examples of cross-pollination or "co-production" should not be overlooked: (i) the resonance already observed above between the FTC's recommendation to use Privacy by Design and the scholars' increasing interest in this approach; (ii) a shared interest between the FTC, the Obama Administration, and many scholars in improving privacy notices and consent mechanisms as a result of the widely recognized failure of the "notice and choice" approach; (iii) the scholars' idea that the FTC might play a key role in the co-regulatory arrangements envisioned by many of them; and (iv) the inclusion of a Contextual Integrity principle in President Obama's Consumer Privacy Bill of Rights.

## V. 2015-2020: An Algorithmic Turn for an Age of Algorithms

By focusing on the last six years (2015-2020) of the period covered in this study, the present Chapter concludes the intellectual history of privacy's algorithmic turn here presented.

In the next few pages, I hope to illustrate how the Internet of Things ("IoT") and AI-powered algorithmic decision-making systems flourished during the years covered in this Chapter. As scholars observed these developments, they would also be closely following a rapidly changing legal system, which would seek to update both its hard and soft law instruments to adapt to these and previous socio-technical developments. During these years, the European Union would approve its General Data Protection Regulation ("GDPR"). Both the US–EU Safe Harbor Agreement and the subsequent EU–US Privacy Shield framework would be invalidated. Meanwhile, in the United States, Congress, the FTC, the States, and for some time the White House, would introduce unsuccessful federal bills, lead enforcement actions against companies with data-based business models, issue new reports on the most pressing technologies and practices, and adopt the first set of State comprehensive privacy laws. Society, in turn, would react with increasing animosity toward Big Tech companies' scandals, resulting in the phenomenon known as the "techlash."

Strangely enough, scholars would not interpret these events through the lens of entirely new harms. While continuing to develop the harms already identified as new in the previous period, scholars would also turn into dominant the harms that had been sparsely discussed in this scholarship over the past 25 years—manipulation, diminished exposure to divergent perspectives, and subordination/oppression. In order to address these harms, they would continue to reject the FIPs (and the individual privacy rights they implicate) as insufficient or inadequate for the Age of

Algorithms, exploring instead a great variety of existing and novel approaches. By the end of the period, several scholars would seem to coalesce again, but this time around a hands-on set of substantive requirements, duties, and prohibitions intended to intervene tech companies' data-extractive business models, the practices of system design, the corporate structure and business incentives, and even data externalities.

This Chapter follows the following structure. I use Section A to offer an overview of the sociotechnical and techno-legal context of the 2015-2020 period, *as seen through the lens of the scholars studied here*. As a result, I provide information regarding the most significant technological advances of the period, the societal attitudes that developed around them, and the legal responses of the US and the European Union to these developments. In Section B, in turn, I present the harms that would become the most prominent in the sample of American privacy law scholarship here reviewed, as well as the different alternatives explored by scholars during these years in order to replace the FIPs. Finally, in Section C I will wrap up the intellectual history here presented by answering the first research question of this dissertation, namely, how did privacy's algorithmic turn actually happen?

## A. Context

This Section looks to place the reader in the technological, social, and legal context in which the American privacy law scholars reviewed for this study were writing between 2015 and 2020. For this purpose, here I offer an account of the main information technologies and practices of this period, the most salient societal attitudes developed in response to them, and the legal frameworks that were in place or being discussed in the United States and the European Union during those

years. As a result, this Section constitutes a general overview of the multiple sociotechnical and techno-legal factors which may have influenced these scholars' thinking during the covered years.

As in the previous three Chapters, it is important to emphasize that the account described here is presented *through the lens of the scholars reviewed for this study*, and therefore, does not necessarily guarantee the accuracy of their forecasts, perceptions, and asseverations.

### 1. Information technologies and practices

As in previous years, between 2015 and 2020 American privacy law scholars would continue to refer to the ubiquitous, pervasive, endless, and—in many cases—surreptitious collection of personal data, which allows public and private entities to amass massive amounts of information.[74] In that sense, during this period Big Data would keep being extremely popular among scholars.[75] As Solon Barocas & Andrew D. Selbst would claim in 2016, "'Big Data' is the buzzword of the decade" (2016, p. 673). Thus, even by the end of the studied years, scholars would still use the term in expressions like "today's age of Big Data" (Katyal, 2019, p. 59), "[t]oday's 'big data' culture" (Lev-Aretz, 2019, p. 1496), and "our brave, big data world" (Bellovin et al., 2019, p. 11).

Additionally, following suit from previous years, some scholars would also continue to raise how these large-scale datasets would either be commercialized by data brokers (Ford, 2019; N. M. Richards & Hartzog, 2016; van Hoboken, 2016) or used to profile individuals (Bronfman, 2015;

[74] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Bronfman, 2015; Coen et al., 2016; Ford, 2016; Lev-Aretz, 2019; Lev-Aretz & Strandburg, 2020; Nissenbaum, 2015; Ohm, 2015; J. Reidenberg, 2015; Sloan & Warner, 2016).

[75] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Barocas & Selbst, 2016; Bellovin et al., 2019; Birnhack, 2019; Bruening & Culnan, 2016, 2016; Coen et al., 2016; I. N. Cofone & Strandburg, 2019; Desai & Kroll, 2017; Fluitt et al., 2019; Ford & Price II, 2016; Hartzog & Solove, 2015; Hiller & Blanke, 2017; Hu, 2017; Jones, 2015; Katyal, 2019; Lev-Aretz, 2019; MacCarthy, 2017; Madden et al., 2017; Marwick et al., 2017; Newman, 2017; Paterson, 2018; Regan, 2020; N. M. Richards & Hartzog, 2016; Samaha & Strahilevitz, 2015; Selbst, 2017; Stark, 2016; van der Sloot, 2017; van Hoboken, 2016; Wachter & Mittelstadt, 2019; T. Z. Zarsky, 2015).

J. Reidenberg, 2015; N. M. Richards & Hartzog, 2016; Sloan & Warner, 2016) and consequently provide them with personalized content (Coen et al., 2016; Kim, 2020; Sax et al., 2018) and/or targeted online advertisement.[76]

Finally, during this period scholars would also continue highlighting the relevance of social media platforms in the information ecosystem (Bietti, 2023; Brayne et al., 2022; Casilli, 2015; Cohen, 2016; Kim, 2020; McKenna et al., 2019; Wachter & Mittelstadt, 2019; Zarsky, 2015). Interestingly, though, during these last studied years it would become common to see scholars that instead of focusing on digital platforms as places or things,[77] would begin to understand them as concepts and logics (Bietti, 2023; Cohen, 2016). The following quote from Eletra Bietti's article *A Genealogy of Digital Platform Regulation* (2023) (in which she in turn cites Julie Cohen) rightly exemplifies this emerging approach: "I adopt Cohen's definition of the platform as *a versatile information intermediary* that gives rise to *specific social, political, technical, and economic affordances*" (Bietti, 2023, p. 23).

As well as not being new—since all of the technologies and practices mentioned above were already discussed in previous Chapters, referring to only Big Data, profiling, personalization, targeted advertising, and social media platforms as the sole information technologies and practices of this period would be misleading. In particular, it would overlook an understanding that many scholars seem to have reached during the period under study. Chris Hoofnagle's eloquence on this

[76] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Bronfman, 2015; I. N. Cofone, 2017; Cohen, 2016; Ford, 2019; Hull, 2021; Kim, 2020; Marotta et al., 2016; Martin & Shilton, 2016; Sax et al., 2018; Shilton & Greene, 2019; van Hoboken, 2016; Veale & Zuiderveen Borgesius, 2022; Wilka, 2018).

[77] As a reference of this earlier use, is worth recalling danah boyd's & Alice Marwick's reference to "social network sites," as "the modern-day equivalent of *the mall or movie theater*, *a place* where teens can hang out with friends and run into other friends and peers" (2011, p. 7).

insight warrants an extended quotation from his 2016 book's Conclusion chapter (workshopped at PLSC 2015):

> Whether *advertising* is harmful has dominated the debate about privacy online. This is a misleading lens to view the problems presented by online advertising.
> Online advertising has both enabled and justified a *massive surveillance regime*. Additionally, online advertising's logic assumes a world with individually targeted marketing. This logic provides no outer bound to surveillance activities, and, indeed, one plan of *the Internet of Things* is to embed devices into the home, such as "smart" televisions and thermostats, which monitor people for advertising purposes. Any kind of personal information, including medical information, and any kind of observable behavior are fodder for more perfectly targeted advertising. Consumer advocates can do little to push back against the demand for more monitoring. Pro-online advertising arguments of funding free content and the idea that advertising does not cause harm trump pro-privacy arguments.
> The online advertising frame also misdirects the public and policy-makers from consideration of the more serious implications of surveillance. Commentators may quip, "what's the harm, it's only advertising?" In so doing, they miss the point that the surveillance systems being built for marketing have other, unforeseen uses. These surveillance systems may even have other purposes, as Shoshana Zuboff has explained. For companies such as Google, a company that rode to victory in search by critiquing the influence of advertising on search results, online tracking is just an instrument for grasping the yet-unrealized dream of *artificial intelligence*. In the shorter run, advertising systems are training *algorithmic decision-making systems*, the very systems that are undermining existing consumer protections (…)." (Hoofnagle, 2016, pp. 347–348)

Thus, either through this or other reasoning, between 2015 and 2020 most American privacy law scholars saw the importance of also paying attention to: (i) a novel and encompassing practice used to *collect* information (the Internet of Things ("IoT")) and (ii) a pervasive way of both *analyzing* data and *using* processed information (algorithmic decision-making systems).[78] As will be seen, although this latter use was already referred to in the previous period as automated

[78] Other sociotechnical systems that received brief mentions from some of the reviewed scholars during these years were robots (Brennan-Marquez & Henderson, 2019; Hartzog & Richards, 2020; A. E. Waldman, 2018b), drones (Bennett & Raab, 2020; Hartzog, 2018a), and the computing cloud (Bennett & Raab, 2020; Friedman & Hoffman, 2014; Gürses & Van Hoboken, 2017; Polonetsky & Tene, 2015; J. Reidenberg, 2015; Yoo, 2015; Zeide, 2016). However, except for Kiel Brennan-Marquez & Stephen Henderson (2019), who focused a 2019 article on the implications of robots occupying democratic decision-making roles, the mentions of these technologies were generally in passing, and none of the reviewed articles explored their specific implications for privacy in greater depth.

decision-making, the implementation of Artificial Intelligence ("AI") (and in particular, Machine Learning ("ML") algorithms) during this studied years sparked the interest of many more scholars in the field.

### 1.1. The Internet of Things

Paula J. Bruening & Mary J. Culnan would describe the Internet of Things as "the ability of everyday objects to connect to the Internet and to send and receive data. This can include automobiles, home appliances, or wearable fitness devices among other 'smart devices'" (2016, p. 565). Unlike the previous reviewed period, where only a few scholars referred to this phenomenon and mostly in passing, between 2015 and 2020 a large number of scholars grappled with the implications of the IoT (Bronfman, 2015; Bruening & Culnan, 2016; Casilli, 2015; Hartzog, 2018a; Hiller & Blanke, 2017; Paterson, 2018; N. M. Richards & Hartzog, 2016; Stark & Levy, 2018).

In 2015, Antonio A. Casilli would forecast: "[t]he capture of data emitted by meters, electronics, and smart appliances installed in private homes, as well as by public transports and ambient components of urban infrastructure (sensors, cameras, etc.), is already a part of our everyday lives. However, it is destined to reach a critical point (…)" (2015, pp. 12–13). As the decade advanced, the presence of smart phones, mobile apps, sensors, wearables, smart power devices, and "'smart' everything'" (Bennett & Raab, 2020, p. 448) devices connected to the Internet would indeed become part of the societal infrastructure. Writing in 2018, Woodrow Hartzog would contend: "[w]e have become drunk on our ability to give anything Wi-Fi access. Barbie dolls, baby monitors, coffee makers, refrigerators, clothes, watches, and cars—we have connected it all. Each new device in this Internet of Things (…)" (Hartzog, 2018a, p. 3).

To be sure, scholars would not necessarily focus on the IoT revolution as a whole but, rather, on one or more subsets of it. Jillisa Bronfman (2015), for instance, would focus on home monitoring technologies (which include devices, services, and applications). Relatedly, Luke Stark & Karen Levy (2018) would delve into the smart devices used at home, in care settings, and to surveil service work. Anne Toomey McKenna and her colleagues (2019), in turn, would explore the combination of smart devices and satellite-based information systems. While Brett Frischmann & Evan Selinger would study "the mind-extending technologies of our emerging smart world" (2018, p. 96), Andrea M. Matwyshyn would dig into the "Internet of Bodies" (IoB), describing it as "a hybrid society where computer code and human corpora blend and where the human body is the new technology platform" (2019, p. 81). Similarly, Charlotte A. Tschider would use the term "Internet of Health Things" (IoHT) to refer to a technology that connects to the Internet physical medical devices such as "connected pacemakers, (…) mobile device-connected insulin pumps, Internet-connected X-Ray machines, and fitness trackers" (2018, p. 1508). Finally, a group of scholars (Hiller & Blanke, 2017; Rubinstein, 2018; Rubinstein & Petkova, 2020; Sanfilippo & Shvartzshnaider, 2023) would zoom in on "smart cities." As described by Ira Rubinstein,

> [c]ity agencies use a variety of means, including city web sites and Internet of Things (IoT) devices, to collect data related to infrastructure, traffic, utilities, tourism, education, child welfare, housing, and healthcare. So-called "smart cities" analyze these massive datasets to enable more efficient and effective monitoring and coordination of maintenance, mobility, environmental management, visitor movements, social services, and neighborhood sentiment. They are also starting to deploy mobile apps to make such services more readily accessible to city residents. And many cities now make these datasets freely available to the wider public through open data programs that publish all sorts of government data that anyone can use, analyze, or redistribute as they wish for a range of beneficial purposes. (2018, p. 1965)

Before addressing the use of algorithmic decision-making systems—as the second relevant practice of this period, it seems important to highlight how, the combination of the IoT and other

information technologies also noticed by scholars over the previous years (e.g. CCTV cameras, biometrics, GPS systems, RFID tags, online social networks), would drive many of them to emphasize the current state of massive digital surveillance.

To be clear, since the mid-90's and early 2000's, scholars who make up the reviewed sample were already talking about how "the decentralization of information processing ha[d] made *omnipresent surveillance* possible by organizations and even individuals" (J. R. Reidenberg & Gamet-Pol, 1995, p. 111), constantly referring to "the reality of rapidly *increasing surveillance* by both public and private bodies" (Froomkin, 2000b, p. 1539).[79] Yet, between 2015 and 2020 several scholars would take a step further and typify this surveillance.

Some scholars would characterize it as *"participatory"* (Ajunwa et al., 2017; Casilli, 2015; Cohen, 2016). For them, participatory surveillance relies on "the intentional, agonistic disclosure of personal information by users of digital services, mobile applications and online platforms" (Casilli, 2015, p. 3), while "workers are expected to aid employer surveillance by using productivity applications and wellness programs" (Ajunwa et al., 2017, p. 739). According to Julie Cohen, for instance, "[o]ver the last several decades, surveillance has become increasingly privatized and commercialized—and also increasingly *participatory*. This shift has challenged initial conceptualizations of surveillance as discipline and control by the state" (2016, p. 207). In her view, in order to incentivize user participation in this new model of surveillance, commercial actors use techniques of "gamification," open access projects, and a discursive strategy that positions privacy and innovation as opposed. Thanks to this latter strategy, which results in a "surveillance–innovation complex," "participation is framed as the result of uncoordinated,

[79] In fact, although not part of this sample, in 1994 David Lyon would publish his book *The Electronic Eye: The Rise of Surveillance Society* (1994).

autonomous, inherently democratic choices made by free-market actors, even as participation and commodification are inextricably entwined" (2016, p. 208).

Relatedly, Mary Anne Franks would characterize the surveillance of the epoch as *"democratic,"* capable of affecting everyone. For Franks, "[t]he rise of government surveillance and the rapid pace of technological progress have given the more privileged classes of society a glimpse of the longstanding experiences of the less privileged classes" (Franks, 2017, p. 430). Robert H. Sloan & Richard Warner, in turn, would describe contemporary surveillance as *"observational"* and *"predictive"* (2016, p. 225), giving private and public entities a massive capacity to both observe a person's past and predict the future.

Finally, several scholars would complicate the traditional top-down and bottom-up models of surveillance, identifying different variations prevalent during these years. Luke Stark & Karen Levy (2018), for example, propose the concept of the "surveillant-consumer," who operates sometimes as an observer, supervising intimate relations, and sometimes as a manager, inspecting the execution of a contracted services. Relatedly, Sarah Braynel, Sarah Lageson, & Karen Levy would use the term "surveillance deputies" to refer to ordinary people who "use their labor and economic resources to engage in surveillance activities on behalf of the state" (2023, p. 463).

### 1.2. Algorithmic decision-making systems, Machine Learning, and Artificial Intelligence

Besides the IoT, the use of algorithmic decision-making systems was the other practice relevant to scholars writing during these years. Between 2015 and 2020, an overwhelming amount of

American privacy law scholars[80] showed interest in how "[d]ecisions based on machine learning algorithms [were] (…) supplementing or replacing human decision-making in vastly different aspects of society, including consumer finance, employment, housing, healthcare, and sentencing, among others" (Selbst, 2017, p. 113).

As described in Chapter IV, since at least 2008 some American privacy law scholars were already focusing on the use of automated decision-making systems to make relevant decisions about individuals' lives (Citron, 2008; Citron & Pasquale, 2014; Crawford & Schultz, 2014; Dwork & Mulligan, 2013; N. Richards, 2008; Yakowitz Bambauer, 2012). However, as Lilian Edwards & Michael Veale would eloquently explain in 2017,

> [p]rogress in automated decision-making and decision support systems was initially held back by a lack of large-scale data and algorithmic architectures that could leverage them, restraining systems to the relatively simplistic problems. *In recent years*, technologies capable of coping with more input data and highly non-linear correlations have been developed, allowing the modelling of social phenomena at a level of accuracy that is considerably more operationally useful. For a large part, this has been due to *the move away from manually specified rule-based algorithms* (such as the early legal systems noted above) *to ML [(Machine Learning)]*. In rule-based systems, explicitly defined logics turn input variables, such as credit card transaction information, into output variables, such as a flag for fraud. Complex ML algorithms are different: output variables and input variables together are fed into an algorithm theoretically demonstrated to be able to "learn" from data. *This process trains a model exhibiting implicit, rather than explicit, logics, usually not optimised for human-understanding as rule-based systems are.* The learning algorithms that make this possible are often not blazingly new, many dating from the '70s, '80s and '90s. But *we now have comparatively huge volumes of data that can be stored and processed cheaply, such that the performance of and ability to further research ML systems has greatly increased*. (Edwards & Veale, 2017, p. 25)

[80] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Ajunwa, 2020, 2021; J. Bambauer & Zarsky, 2018; Barocas & Selbst, 2016; Brennan-Marquez & Henderson, 2019; R. Calo & Citron, 2021; Cohen, 2019b; Desai & Kroll, 2017; Doshi-Velez et al., 2017; Edwards & Veale, 2017; Fluitt et al., 2019; Gerards & Zuiderveen Borgesius, 2022; Hartzog & Richards, 2020; D. Hirsch et al., 2019; D. Hirsch, 2020; Hoofnagle, 2016; Hu, 2017; Kaminski, 2019; Katyal, 2019; Kim, 2017, 2020; Madden et al., 2017; Mulligan et al., 2016; Ohm & Frankle, 2018; Paterson, 2018; Selbst, 2017, 2021; Selbst & Barocas, 2018; Tene & Polonetsky, 2017; Wachter et al., 2018, 2021; Wachter & Mittelstadt, 2019; A. Waldman & Martin, 2022; Wang, 2022; Wilka, 2018; Zeide, 2016, 2017)

A similar transition would be described by Deven R. Desai & Joshua A. Kroll too. According to these scholars,

> A consistent theme is that unaccountable machines have taken center stage and now "are used to make decisions for us, about us, or with us," in sensitive and subjective areas such as healthcare, employment, credit, national security, networked devices, news, and more. *A more recent fear is that the rise of large data sets combined with machine learning ("ML")* (an area of computer science that *uses the automated discovery of correlations and patterns to define decision policies*) might allow those who use such techniques to wield power in ways society prohibits or should disfavor, but *which society would not be able to detect*. (Desai & Kroll, 2017, pp. 3–4)

Thus, what specially drew the attention of scholars writing between 2015 and 2020 was the rising implementation of *ML algorithms* by public and privacy entities to make automated decisions. Unlike *rule-based algorithms*, *ML algorithms* work with implicit logics that are: (i) self-"learned" through the automated discovery of correlations and patterns from huge volumes of data; (ii) not always optimized for human-understanding; and (iii) often based on statistical relationships that defy human intuition. While some scholars writing during this period would conflate these two latter elements into the by-then well-known "black-boxed" nature of ML algorithms (Desai & Kroll, 2017; Ford & Price II, 2016; Ohm & Frankle, 2018; Wang, 2022), others would be more specific about their differences (Selbst & Barocas, 2018; Wachtera et al., 2021). According to Andrew Selbst & Solon Barocas, for example,

> What sets machine learning models apart from other decision-making mechanisms are their inscrutability and nonintuitiveness. (…) Inscrutability and nonintuitiveness have been conflated in the past: where the property of *inscrutability* suggests that models available for direct inspection may defy understanding, *nonintuitiveness* suggests that even where models are understandable, they may rest on apparent statistical relationships that defy intuition. (Selbst & Barocas, 2018, pp. 1090–1091)

Similarly, although referring to algorithms in general, Sandra Wachtera, Brent Mittelstadt, & Chris Russell would contend that, "[c]ompared to human decision-making, algorithms are *not*

*similarly intuitive*; they operate at speeds, scale and levels of complexity that *defy human understanding*, [and] group and act upon classes of people that need not resemble historically protected groups (…)" (Wachter et al., 2021, p. 3).

When talking about ML algorithms and related concepts, a few of the scholars writing during this period would look to be precise in delimiting these concepts. According to Janneke Gerards & Frederik Zuiderveen Borgesius, for example,

> A concept closely related to *algorithmic decision-making* is artificial intelligence. *AI* can be described as "[t]he theory and development of computer systems able to perform tasks normally requiring human intelligence." AI can be divided into two broad categories: (i) rule-based AI, and (ii) machine learning. For *rule-based, or knowledge-based, AI*, usually "explicit facts and rules about some activity are explicitly programmed into software, harnessing the knowledge of domain experts about how some system or activity operates." *Machine learning* can be described as "an automated process of discovering correlations (sometimes alternatively referred to as relationships or patterns) between variables in a dataset, often to make predictions or estimates of some outcome." One could also say that machine learning is "statistics on steroids". *Machine learning has become the most successful type of AI*. In fact, machine learning is so successful that AI is often used as a synonym for machine learning now. For ease of reading, we will mostly speak of AI in this paper. (Gerards & Zuiderveen Borgesius, 2022, pp. 5–6)

In a less technical but also cautious way, in her 2020 article *The Paradox of Automation as Anti-Bias Intervention*, Ifeoma Ajunwa would explain: "the definition of the term 'artificial intelligence' (AI) varies in legal literature and in popular media, and thus, in this Article, in lieu of 'AI,' I employ the more precise terms of 'algorithms' and 'machine learning algorithms'" (2020, p. 1684). Yet, efforts like these ones to clarify the use of the different concepts would be an exception rather than the rule. In most of the reviewed sample of articles, terms such as algorithms, ML, "Big Data analytics," "predictive analytics," and AI would tend to be interchangeably used when referring to algorithmic decision-making systems.

Finally, most scholars in the sample of articles reviewed would cite examples of algorithmic decision-making systems being used in a variety of different contexts. Nevertheless, a considerable

group of them would specifically place their attention on their application in the following three domains: (i) education (Rubel & Jones, 2017; Zeide, 2016, 2017), where data analytics are used, for example, to "create a list of 'red flag' conditions that are correlated with a decreased likelihood of a student graduating," "identify students likely to drop out, and encourage[e] (…) them to leave early (i.e., before they would count in the retention measures)" (Rubel & Jones, 2017, p. 26), and make pedagogical decisions; (ii) the workplace (Ajunwa, 2020, 2021; Kim, 2017, 2020; Newman, 2017), where algorithms are employed, for instance, to "make personnel decisions, thereby affecting who gets interviewed, hired, or promoted" (Kim, 2017, p. 860), and "decide how to systematically weed out people who might agitate on behalf of all employees for higher wages" (Newman, 2017, p. 697); and (iii) the administrative state (R. Calo & Citron, 2021; Hu, 2017), where algorithmic decision-making systems are used, among other things, for "big data blacklisting" (Hu, 2017), as well as "to evaluate public school teachers in Texas, to assess and terminate unemployment benefits in Michigan, and to evaluate the risks posed by criminal defendants in D.C., Wisconsin, and elsewhere" (R. Calo & Citron, 2021, p. 801).

## 2. Societal attitudes

During the studied period, scholars would report how public concerns about privacy—also reported by them in the previous years—would continue to increase. At the same time, a portion of them would start to make more nuanced claims about these reported concerns, making clear how their presence and magnitude would depend on different variables. In any case, the high-profile cases involving data leaks or private and public entities engaged in questionable collection, aggregation, processing, use, and dissemination of personal data would lead American society, would generate among Americans growing public animosity toward Big Tech companies. As a

result, more and more individuals would be reported by scholars to be using self-help technologies to protect their privacy.

Finally, during these years scholars would, for the first time in the covered thirty years, start to question the rhetoric surrounding the "privacy paradox" theory.

### 2.1. Increased public concern about privacy

As in previous periods, between 2015 and 2020 several scholars (Bruening & Culnan, 2016; Casilli, 2015; J. King, 2015; Nissenbaum, 2015; Regan, 2015; Wilka, 2018) would note an increase in public concern about the collection, processing, and use of personal data as well as about algorithmic decision-making.

"[U]sers are making increasingly insistent demands for autonomy and personal and collective empowerment," Antonio A. Casilli would contend. "They are not remaining passive in the face of widespread complicity between businesses and governments, scandals surrounding the passing of draconian laws and the lack of legal and technical means to protect the integrity and confidentiality of personal data" (2015, p. 5). Citing a national public opinion survey conducted by the National Cyber Security Alliance, Paula J. Bruening & Mary J. Culnan would similarly claim that by 2015, "eighty-seven percent of individuals were concerned about the sharing of their information with others without their knowledge and consent" (2016, p. 573).

In a similar fashion, Priscilla Regan would cite "[t]he pull and tug between Facebook the company, in its quest for more information and transparency of users' activities, and Facebook users, who realize they value privacy once they concretely see or experience changes in the flow of information" (2015, pp. 58–59), as proof of the importance that the user community would give to privacy. Additionally, she would argue that even in the context of government data collection,

where 9/11 initially generated widespread public acceptance of surveillance, support had waned. According to Regan,

> support became somewhat tempered by concern over the intrusiveness of some techniques, debate over their effectiveness and questions over accountability and due process – all of which sprung in part from shared perceptions that the "national security state" had intruded too far into the kind of privacy protections society valued and needed to be pulled back into a less aggressive and more carefully regulated stance. (2015, p. 59)

Yet, no all scholars would support these claims about the existence of wide public concern. Rather, some of them would make more nuanced claims about society's public worries. According to these scholars, people's distrust and judgments about commercial surveillance would depend on elements as varied as the type of information collected and the use purpose (Coen et al., 2016; Poort & Zuiderveen Borgesius, 2019), the presence of cues of trust/distrust (Mourey & Waldman, 2018), decision importance and the type of governance regime applied (A. Waldman & Martin, 2022), as well as the context where information wold be used (Hull, 2021; Martin & Nissenbaum, 2017). Relatedly, Omer Tene & Jules Polonetsky would argue that consumers' suspicion towards companies would be contingent to whether they saw them as an information fiduciary (e.g., Amazon) or as actors "pursuing their own agenda, setting algorithms to maximize ad inventory value, and monetizing with little apparent value for consumers" (2017, p. 141) (e.g., ad tech companies).

### 2.2. Scandals and consequent "techlash"

Between 2015 and 2020 society became awash with high-profile cases involving private and public entities that engaged in questionable collection, aggregation, processing, use, and dissemination of personal data. In the first place, large-scale unauthorized access to personal information became more common every day. As reported by Rachel Wilka in 2018,

> Over the course of 2014, 47% of U.S. adults, or 110 million individuals, had their personal data stolen. By 2017, approximately the same proportion of Americans were affected by the Equifax hack alone. Outside of data breaches, companies argue that data distributed to partners is anonymized, but in the Human Genome Project, a respected medical study, between 84–97% of participants could be re-identified (i.e., their names could be connected to their individual "anonymized" data). (2018, p. 66)

Second, several scandals of data misuse would also significantly impact the public's perceptions during these years. Among them, three would be repeatedly cited by scholars: the Snowden leaks (Franks, 2017; Martin & Nissenbaum, 2017; Paterson, 2018; J. Penney, 2022; Regan, 2015; J. Reidenberg, 2015; Schwartz & Peifer, 2017; Stark, 2016), Facebook's emotion manipulation experiment on users (Martin, 2015; N. M. Richards & Hartzog, 2016; Stark, 2016), and the Cambridge Analytica scandal.[81]

In June 2013, Edward Snowden leaked information that revealed "the breadth and detail of the National Security Agency (NSA) surveillance activities in the USA and abroad" (Regan, 2020, p. 52). In the second case, Facebook's researchers "manipulated Facebook's news feed by, among other things, showing fewer positive posts to some users to see if they would lead to greater user expressions of sadness" (N. M. Richards & Hartzog, 2016, p. 470). Finally, it emerged in 2018 that,

> Facebook allowed a researcher, Alexander Kogan, to contact Facebook users about downloading a personality quiz application. Around 270,000 users responded. The application collected not only their data but also harvested the information of all their friends, giving access to the profiles of an estimated 50–70 million people. Kogan then sold this information to a company called Cambridge Analytica, a political data firm that offered to identify the preferences of voters based on their personality traits, friend networks, and Facebook "likes" to influence their behavior with targeted election advertisements. President Trump's 2016 election campaign thereafter hired Cambridge Analytica to gain access to these voter profiles, as did the Brexit campaign. The ensuing

[81] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Barocas & Levy, 2020; Barrett, 2018; Chander et al., 2021; Fathaigh et al., 2019; D. Hirsch, 2020; Kaminski, 2019; Katyal, 2019; Kim, 2020; Lev-Aretz, 2019; Lev-Aretz & Strandburg, 2020; Mathur et al., 2021; J. Penney, 2022; Regan, 2020; N. M. Richards & Hartzog, 2021; Rubinstein & Petkova, 2020; Susser et al., 2019).

> scandal gained notoriety precisely because of the number of people affected and the fact that they were voters with political interests, and not merely shoppers with consumer interests. (Rubinstein & Petkova, 2020, p. 782)

Evidently, these infamous privacy failures provoked public outrage and alarm among all kinds of stakeholders. As a result, in 2020 Woodrow Hartzog & Neil Richards would describe how "[t]he Financial Times proclaimed that all of 2018 could be summarized by the word 'techlash,' which they defined as '[t]he growing *public animosity towards large Silicon Valley platform technology companies and their Chinese equivalents*'" (2020, p. 1691).

### 2.3. Use of self-help tools

Probably as a consequence of this animosity toward Big Tech companies, individuals would use different forms of "self-help" (Hazel, 2021, p. 305) and "privacy-protecting strategies" (Marwick et al., 2017, p. 4) to protect their information privacy (Casilli, 2015; Hazel, 2021; O. S. Kerr & Schneier, 2018; J. King, 2015; Martin, 2015; Marwick et al., 2017). These strategies include, for example, employing Virtual Private Networks (VPNs), encrypted messaging apps broadly available (e.g., Whatsapp), and anonymous networks such as TOR. As Casilli would eloquently state, "[r]ather than a smooth, linear transition from a world where privacy plays a central role to one where it has supposedly lost its raison d'être, we are today engaged in *a full-fledged culture war over confidentiality, anonymity, and secrecy*" (2015, p. 6).

### 2.4. Questioning the "privacy paradox"

Unlike previous periods, during these years several scholars (Barrett, 2018; Bhatia & Breaux, 2018; J. King, 2015; D. J. Solove, 2021) would start questioning the rhetoric surrounding the

"privacy paradox" theory. For Jennifer King, for instance, the assumption that consumers trade off their privacy *despite* knowing about the risks is short-sighted. According to her,

> In fact, *many technology users do not understand what is at stake* when they download an app or visit a website. But more fundamentally, this argument misses the fact that *we act as humans first and technology users second*. Disclosure is often a reasonable, and even rational, response to so many of the decisions that we face, even those with detrimental privacy consequences. It's similar to the impulse that has us reaching for our smartphones to check to see who just texted us, despite the fact we are navigating a vehicle down a freeway at seventy miles per hour. The technology has been overlaid upon our existing social structures, but with none of the limitations inherent to our cognitive capacities. (2015, p. 3)

Similarly, for Jaspreet Bhatia & Travis D. Breaux, "[a]n alternative explanation for why users exhibit conflicting behaviors when sharing their personal information is that users perceive privacy harms in terms of a cost-benefit tradeoff, wherein *the risk of a privacy harm is reduced when users perceive an increase in the benefits of sharing their personal information with a service*" (2018, p. 2). Similarly, Lindsay Barret would comment on the benefits of empirical research to understand "the limits of asking someone broad questions about how they value their privacy writ large," as well as the risks of "conflating preferences and expectations, assuming the respondent is deeply informed about the internet ecosystem, or divorcing broad privacy value statements from situational context" (2018, p. 38).

Daniel Solove, in turn, would go a step further in his critique to the "privacy paradox" theory. In his view, the privacy paradox is actually a myth, because, in reality, "behavior and attitudes about privacy are not out of alignment" (2021, p. 4). In other words, "[a]ttitudes and behavior only *appear* to be in conflict; they actually involve different things. *The behavior in the privacy paradox involves people making decisions about risk in very specific contexts. In contrast, people's attitudes about their privacy concerns or how much they value privacy are much more general in nature*" (2021, p. 4).

## 3. Legal system

"Privacy law seems stuck. *Congress has not enacted any meaningful new privacy laws or overhauled any old laws in at least a decade*, with one important but narrow exception relating to genetic information" (2015, p. 1127), would denounce Paul Ohm in 2015. In a similar note, in 2016 Bilyana Petkova would complain:

> [D]ata-privacy law is in flux in the United States. *It is surprising, however, how little the debate has progressed over the years*. As noted by Professor Hoofnagle, the conversation on data privacy has changed strikingly little since the 1973 landmark report of the U.S. Department of Health, Education, and Welfare (HEW) published the Fair Information Practice Principles (FIPPs) that were to become the backbone of privacy laws worldwide. Yet, the United States—where as far back as 1890, Warren and Brandeis proclaimed a "right to be left alone" and where the FIPPs originated in the influential HEW report—*has hesitated to take a decisive stance on data privacy since then*. (2016, p. 596)

By 2020, this diagnosis would remain pretty much the same (Gilman & Green, 2018; Rubinstein, 2018). As in the previous period, however, the absence of new statutes did not mean that legislative proposals as well as other governmental efforts had not occurred.

### 3.1. Congressional unsuccessful efforts

According to Anupam Chander, Margot E. Kaminski, and William McGeveran, whose article was published in 2021, "[i]n the past year, (…) eleven comprehensive federal privacy bills were introduced in Congress" (2021, p. 1734). Among them, most scholars would particularly highlight: (i) the Consumer Privacy Bill of Rights Act, a 2015 White House legislative initiative based on the 2012 White House report mentioned above, which among other things, looked "to address this issue of 'disparate impact' resulting from data analysis and targeted use" (Bronfman, 2015, p. 218); (ii) the Data Care Act of 2018, introduced by Senator Brian Schatz to impose relational duties of care, loyalty, and confidentiality (Chander et al., 2021; MacCarthy, 2021; N. M. Richards &

Hartzog, 2021; A. E. Waldman, 2020); (iii) the Deceptive Experiences to Online Users Reduction (DETOUR) Act, introduced by Senators Mark Warner and Deb Fischer to target "user interfaces that attempt to manipulate users into making decisions they would not otherwise do or are in ways adverse to their interests," also known as "dark patterns" (Hartzog & Richards, 2020, p. 1716) (Luguri & Strahilevitz, 2021; Mathur et al., 2021); (iv) the Algorithmic Accountability Act, introduced in 2019 to "direct the Federal Trade Commission to develop regulations regarding the use of automated decision" (Kim, 2020, pp. 932–933) (J. R. Bambauer et al., 2022); and (v) the Consumer Online Privacy Rights Act, introduced in 2019 by Senator Maria Cantwell and which would also include a duty of loyalty (Chander et al., 2021; N. M. Richards & Hartzog, 2021).

Moreover, a draft of the Consumer Data Protection Act was circulated by Senator Ron Wyden, who aimed "to tackle automated decision systems and hold executives personally liable for certain privacy lapses" (Hartzog & Richards, 2020, p. 1716). Similarly, in 2018 Senator Mark Warner issued the White Paper *Potential Policy Proposals for Regulation of Social Media and Technology Firms,* "proposing a number of policy options including one to label certain services, such as Google, as 'essential services,' a designation that would require internet platforms to provide access to these services on 'fair, reasonable and non-discriminatory' terms (…) and prevent them from 'engaging in self-dealing or preferential conduct'" (Regan, 2020, p. 500).

In the education domain, "[b]ills proposed by Senators Edward J. Markey and Orrin Hatch, Senator David Vitter, and Representatives Todd Rokita and Marcia Fudge could amend FERPA. Two other bills, sponsored by Representative Messer and Senator Blumenthal, respectively, propose to regulate entities that receive information from educational institutions and agencies" (Zeide, 2016, p. 379).

Additionally, scholars would also report that in 2017 Representatives John Delaney and Pete Olsen launched a bipartisan Artificial Intelligence Caucus, which in turn introduced the FUTURE of Artificial Intelligence Act of 2017 to address concerns over bias and privacy risks associated with AI. As Lindsey Barrett would highlight in 2018, "members of both the House and Senate have shown interest in the both the benefits and risks of artificial intelligence, and privacy writ large is even more of an established issue on the Hill" (2018, p. 59).

Despite these numerous but unfruitful federal legislative efforts, scholars would locate action in the States (including local governments (Rubinstein, 2018)) and in the Executive branch.

### 3.2. States would be starting to act

As scholars writing during this period would report, in 2011 California had already enacted the California Reader Privacy Act, to extend privacy protection to e-books. Similarly, "[i]n 2013, Arizona explicitly added e-book protection to their library records statute" (Kaminski & Witnov, 2015, p. 515). As reported by Elana Zeide, "[a]s of July 2, 2015, 'forty-six states considered 182 bills addressing student data privacy' and twelve passed twenty-four new laws" (2016, p. 379). Yet, when it came to comprehensive privacy laws, California would almost unanimously be seen as a frontrunner (Petkova, 2016). In June 2018, California's Consumer Privacy Act (CCPA) was enacted.[82] According to Anupam Chander and his co-authors,

> *U.S. privacy law can be periodized as pre-CCPA and post-CCPA.* Until the CCPA, no state or federal statute in the United States imposed privacy protections across all industry sectors and technologies in the manner that European data protection law had done for decades. Ever since the CCPA, Congress and state legislatures across the country have been considering huge numbers of data privacy proposals of that scope. (Chander et al., 2021, pp. 1738–1739).

[82] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Chander et al., 2021; Habib et al., 2019; Han et al., 2019; Hartzog & Richards, 2020; Lev-Aretz & Strandburg, 2020; Regan, 2020; D. J. Solove, 2021; P. Swire, 2022).

As a result, in 2021 Neil Richards & Woodrow Hartzog (2021) would report the enactment of additional comprehensive state privacy laws in Virginia and Colorado.

### 3.3. Efforts coming from the Executive branch

Regarding the Executive branch, in 2015 Helen Nissenbaum would explain how,

> *governmental bodies in the US have kept citizens' privacy on the active agenda*, pursuing cases against specific activities (e.g. Google Inc. v. Joffee et al. 2014; FTC v. Wyndham Worldwide Corporation, et al. 2014; re: Netflix Privacy Litigation 2012). They have conducted studies, public hearings, and multistakeholder deliberations on specific practices, such as commercial uses of facial recognition systems, surreptitious uses of personal information by mobile apps, and applications of big data (National Telecommunications and Information Administration (NTIA) 2013a). (2015, p. 2)

In particular, actions taken by the FTC and the White House would be specially noticed by scholars writing during these years.

#### 3.3.1. The FTC's continued efforts

Between 2015 and 2020 many scholars would keep pointing to the Federal Trade Commission ("FTC") as "the de facto data protection authority of the United States and its chief privacy ambassador to the outside world" (R. Calo, 2015, p. 682) (Hartzog & Solove, 2015; van Hoboken, 2016). As explained by Ryan Calo,

> [t]he Commission interprets its authority to stamp out "deceptive" practices to also encompass false or misleading statements about privacy, privacy being an exogenous consumer preference. *Yet the agency's role has extended well beyond enforcing the statements companies make in privacy policies*. The agency routinely holds workshops and publishes guidance on matters related to privacy and security of emerging technology in general wherein participants and the Commission recognize a diverse array of complex privacy values. And in its burgeoning role as a de facto privacy regulator, *the Commission has relied more and more on its authority to stamp out not only deception but "unfairness."* For instance, the Commission pursues inadequate security around the

> personal information of consumers even in the absence of a promise to keep it safe, as well as sudden or invasive changes to the use and collection of information that have been technically disclosed to the consumer. (2015, pp. 683–684)

Thus, in a similar way to the previous period (Chapter IV), during these years scholars would highlight the multiple different ways that the FTC had found over the years to stretch its relatively restricted powers to protect information privacy. Nonetheless, due probably to this same stretching efforts, in 2015 Woodrow Hartzog & Daniel Solove (2015) would also discuss how in *FTC v. Wyndham Worldwide Corp*. and *LabMD, Inc. v. FTC* the FTC's authority in consumer privacy matters would for the first time have been called into question.

In terms of the FTC's guidance activities, scholars would refer to several staff reports published during these years on topics such as data brokers, the Internet of Things ("IoT"), Big Data, and the sharing economy.

First was the 2014 report *Data Brokers: A Call for Transparency and Accountability*, where the FTC recommended Congress to "enact legislation to regulate the data broker industry so that consumers would know about the industry's activities and have access to information held about them by data brokers" (Madden et al., 2017, p. 122). Second, the *Internet of Things: Privacy & Security in a Connected World* report, published by the agency in 2015, after having organized a meeting to hear comments in November 2013 (Bronfman, 2015; Bruening & Culnan, 2016). Among various elements, the report "suggested some alternatives to traditional web privacy notices for the IoT such as QR codes, choices at the point of sale, or choices during setup of the device" (Bruening & Culnan, 2016, p. 565). Similarly, various scholars writing during these years would allude to the report *Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues*, published in 2016 (N. M. Richards & Hartzog, 2016; Tene & Polonetsky, 2017). In this document, "[t]he Federal Trade Commission ("FTC") asserted companies must correct for biases that could

be incorporated into automated processes at both the collection and analytic stages, and 'balance the predictive value of the model with fairness considerations'" (Tene & Polonetsky, 2017, pp. 134–135). In fourth place, Ryan Calo & Alex Rosenblat would refer to "*The 'Sharing' Economy: Issues Facing Platforms, Participants & Regulators* report, a 2016 document resulting from a 2015 day-long workshop, in which the FTC "describes at a high level of generality what makes for a successful sharing economy platform and engages in sustained discussion of the competition issues that sharing economy platforms may generate" (2017, p. 1677).

Regarding the FTC's enforcement activities, scholars would report how, during these years, the agency pursued enforcement actions against several commercial actors, including Snapchat (2015) (Fathaigh et al., 2019; Zimmeck et al., 2017), Uber (2017) (R. Calo & Rosenblat, 2017), Equifax (2019) (Rubinstein & Petkova, 2020), and Facebook Inc. (2019) (Fathaigh et al., 2019; Rubinstein & Petkova, 2020). This last one, due in part to the Cambridge Analytica scandal described above. Writing in 2022, Peter Swire would report: "Many of the largest platforms have signed consent decrees with the Federal Trade Commission ('FTC'), and Facebook paid a record $5 billion fine in 2019 to settle FTC charges that it violated its consent decree" (P. Swire, 2022, p. 62).

Finally, in February 2019 the FTC launched a Task Force to Monitor Technology Markets (Van Loo, 2019). At the same time, throughout these years scholars would also frequently call attention to the lack of resources of the agency to meet its mission (Hoofnagle, 2016; McGeveran, 2016; A. E. Waldman, 2018b). According to Chris Hoofnagle, for example,

> [t]he Agency is also limited in resources. The FTC's budget is only $300 million. Consider that the Food and Drug Administration's budget is over $4 billion and the newly created Consumer Financial Protection Bureau's is over $400 million. Almost half of the FTC's budget is devoted to competition matters. The FTC's Bureau of Consumer Protection is modest in size (about 638 employees), and just a fraction of its staff handle privacy matters (the FTC estimates 57 employees). (2016, p. 335)

### 3.3.2. The White House's ambivalent initiatives

Similar to the FTC (and even earlier), in 2014 the Obama-era White House also released a report on Big Data—*Big Data: Seizing Opportunities, Preserving Values*, which was widely cited by scholars.[83] Also known as the Podesta Report, this document "hinted at the discriminatory potential of big data (…) [and] suggests that there may be unintended discriminatory effects from data mining but does not detail how they might come about" (Barocas & Selbst, 2016, p. 674).

In contrast, scholars would also report with concern how, after Donald Trump was elected as the US President in 2017, he issued an Executive Order—*Protecting the Nation from Foreign Terrorist Entry into the United States*—ordering the implementation of screening and vetting standards—increasingly algorithm and Big Data-based—for "barring the entry of travelers and refugees from specific Muslim-majority countries into the United States" (Hu, 2017). Relatedly, "in March 2018, Secretary of Commerce Wilbur Ross announced that he would add the citizenship question to the Census for 2020 to assist the Department of Justice (DOJ) in enforcing the Voting Rights Act (VRA)" (Rubinstein & Petkova, 2020, p. 777). This initiative, however, was later blocked by a judge.

Thus, as scholars would argue, the White House's role as a key privacy player would be greatly diminished with the change of government.

## 3.4. The European Union's regulatory landscape

Although finally blocked by a judge, these and similar moves by President Trump were not well received by the international community. According to Paul M. Schwartz & Karl-Nikolaus Peifer,

[83] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Barocas & Selbst, 2016; Hiller & Blanke, 2017; Jones, 2015; Katyal, 2019; Polonetsky & Tene, 2015; N. M. Richards & Hartzog, 2016; T. Z. Zarsky, 2015).

"there are indications of a potential negative 'Trump Effect' in privacy law that will divide the United States and EU in the area" (2017, p. 120). It should be noted, however, that the fracture of this relationship had begun even earlier. As pointed out by Joel Reidenberg in 2015, "in the wake of the Snowden disclosures, the European Parliament challenged the viability of the Safe Harbor" (2015, p. 461). As a result,

> [i]n late 2015, an E.U. court case invalidated the U.S.–E.U. Safe Harbor Agreement, a legal mechanism used by over 4,500 U.S. companies to transfer personal data from the E.U. to the United States—potentially subjecting many more of them to E.U. enforcement. A replacement mechanism, known as the "Privacy Shield," went into effect in mid-2016. (McGeveran, 2016, p. 962)

As this was happening, the European Union was also considering replacing the European Data Protection Directive with a regulatory framework administered by the European Commission. Writing in 2016, Julie Cohen would highlight how "American regulators and diplomats have worked to soften the European Commission's proposed new data protection regulation. Consistent with the interests of the powerful U.S. information industry, in U.S. interventions overseas the theme of innovation is uppermost" (2016, p. 219). That same year, the European Union's General Data Protection Regulation (GDPR) was finally adopted.[84] According to Mary Madden and her co-authors, besides endorsing Privacy by Design (Bhatia & Breaux, 2018) and including a right to data portability (P. Swire, 2022), the GDPR

> provides *even stronger privacy protections*, including a "right to be forgotten," *strict consent requirements* that place the burden of proof on the collector, and *increased sanctions for violations.* The Regulation also *tightens restrictions on the processing of particularly sensitive information*, such as race, political opinions, and religion. In addition, the Regulation gives people *the right not to be subject to decisions solely based*

[84] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Bennett & Raab, 2020; Bhatia & Breaux, 2018; Chander et al., 2021; Davis & Marotta-Wurgler, 2019; Doshi-Velez et al., 2017; Edwards & Veale, 2017; Fathaigh et al., 2019; Hartzog & Richards, 2020; Helberger et al., 2017; Hyman & Kovacic, 2019; Lev-Aretz & Strandburg, 2020; Madden et al., 2017; McGeveran, 2016; Petkova, 2016; Regan, 2020; Schwartz & Peifer, 2017; P. Swire, 2022; van Hoboken, 2016; A. E. Waldman, 2020; Yakovleva & Irion, 2020a).

> *on algorithms, including profiling, and to contest such decisions*. (Madden et al., 2017, pp. 120–121)

As a result, in 2016 William McGeveran would valorate the Regulation in the following terms: "[t]he revisions move European statutory law even further from the U.S. approach and create enormous new potential fines—but leave most day-to-day power in the hands of the same national regulators as before" (2016, p. 963). At the same time, this new framework "led many global technology companies [based in the US] to comply with GDPR requirements firm-wide" (Hartzog & Richards, 2020, p. 1689).

Finally, by 2018 a few scholars (Fathaigh et al., 2019; Wachter & Mittelstadt, 2019; F. J. Zuiderveen Borgesius & Steenbruggen, 2019) would also start grappling with the possibility of the European Union passing an ePrivacy Regulation to protect the confidentiality of electronic communications. And, while only mentioned by one of the scholars here reviewed (Yakovleva, 2020c), in July 2020 the Court of Justice of the European Union (CJEU) invalidated the EU–US Privacy Shield framework in the so-called Schrems II case.

***

Information privacy-wise, significant events seem to have occurred in all three technological, social, and legal domains between 2015 and 2020, turning these years into another of the most agitated studied periods. In the technological domain, the re-emergence of Machine Learning algorithms put previous automated decision-making systems on asteroids, finally bringing into life today's famously known Artificial Intelligence ("AI") systems. In the social domain, in turn, during this period the American societal attitudes about information privacy reported by scholars would finally undergo a significant change. In particular, famous Silicon Valley misconducts such as Facebook's emotion manipulation experiment on users and the Cambridge Analytica scandal

would eventually lead American society to what journalists would refer to as the "techlash": a growing public animosity towards the Big Tech companies. And, when interpreting these societal attitudes, scholars would for the first time start to question the "privacy paradox" theory, which many of them had pushed forward in the past.

Lastly, during these years the American legal system would be significantly shacked by the approval of the European Union's GDPR and the invalidation of both the US–EU Safe Harbor Agreement and the subsequent EU–US Privacy Shield framework. Meanwhile, in the United States, Congress, the FTC, the States, and for some time the White House would be busy trying to update their hard and soft law instruments to respond to many of the technologies and practices described in this intellectual history (e.g., data brokers, Big Data, the IoT).

### B. American privacy law scholars' response

In contrast to this agitated sociotechnical and techno-legal context, and to the previous studied period, between 2015 and 2020 American privacy law scholars would raise no new harms. Yet, the harms panorama of the period would still considerably change during these years, since the scholars' conceptions of discrimination and the harm to due process guarantees would evolve over time. Likewise, three other harms that had been mentioned sparsely by them over the past 25 years (i.e., manipulation, diminished exposure to differing perspectives, and subordination/oppression) would finally become dominant in their scholarship during this period. In parallel, scholars would continue to reject the FIPs as insufficient or inadequate for the Age of Algorithms, while exploring a great variety of existing and novel alternatives.

## 1. Identified harms

Between 2015 and 2020, the American privacy law scholars here reviewed would keep bringing up traditional harms, while also continuing to develop the harms identified as "new" in the prior period. In addition, many of the harms mentioned sparsely by them over the past 25 years, such as manipulation, diminished exposure to differing perspectives, and subordination/oppression, would finally acquire dominance in their scholarship during this period.

### 1.1. Traditional harms

#### 1.1.1. Data-breach harms

As in the previous fifteen years, between 2015 and 2020 American privacy law scholars (Bodie, 2022; Brensinger, 2023; Bronfman, 2015; Ford & Price II, 2016; Hartzog & Solove, 2015; McGeveran, 2019; Paterson, 2018; D. J. Solove & Citron, 2018; D. J. Solove & Hartzog, 2022; Yakovleva, 2020c) would keep raising alarms about data-breach related harms. In practice, these harms could range from **financial harms**, such as identity theft and fraud due to misappropriated information, to **emotional distress, anxiety, and the harm to interpersonal trust** caused by a data breach.

As a result of conflicting caselaw, during this period Daniel Solove and his two separate co-authors (Woodrow Hartzog and Danielle Citron) as well as some others (A. E. Waldman, 2018b) would repeatedly emphasize the need for data security breaches—and the associated *risk* of identity theft—to be considered as harms in and of themselves (Hartzog & Solove, 2015; D. J. Solove & Citron, 2018; D. J. Solove & Hartzog, 2022).

### 1.1.2. Chilling effects

During these years, scholars would also keep raising alarms about the **"chilling effects"** of data collection and processing activities[85] and their consequent **detrimental effects on self-governance and democracy** (Green, 2020; Kaminski & Witnov, 2015; Matwyshyn, 2019; Paterson, 2018; J. Reidenberg, 2015; Sandfuchs & Kapsner, 2016; Stark & Levy, 2018). Compared to previous periods, however, during these years some of the analysis of the "chilling effect" harm would be more sophisticated and nuanced.

In particular, in 2015 Margot E. Kaminski & Shane Witnov would use social science research to empirically prove the intuited effects of surveillance on First Amendment activity. According to their findings, "beyond merely causing people to stop speaking when they know they are being watched" (2015, p. 467), surveillance also prevents the development of minority ideas. Thus, besides a chilling effect on speech, an even more pernicious element—labeled by them as the "conformity effect"—is also at play. According to Kaminski & Witnov,

> [i]f the First Amendment serves to encourage democratic self-governance, surveillance thwarts this purpose as well. Surveillance discourages individuals with unformed ideas from deviating from majority political views. And if the First Amendment is intended to allow the fullest development of the autonomous self, surveillance interferes with autonomy. Surveillance encourages individuals to follow what they think others expect of them and conform to perceived norms instead of engaging in unhampered self-development. (2015, p. 467)

Relatedly, in two different articles published in 2017 and 2022, Jonathon W. Penney also provided empirical evidence of the nature and extent of chilling effects. In particular, in his 2017 article Penney "discussed the results of a new and original survey-based case study that offer strong

[85] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Kaminski & Witnov, 2015; Koops et al., 2018; J. Penney, 2022; J. W. Penney, 2017; Perri & Thaw, 2017; Polonetsky & Tene, 2015; Sloan & Warner, 2016; Vagle, 2016; van Hoboken, 2016; Wachter & Mittelstadt, 2019; Zeide, 2017)

support for the suggestion that state and non-state action, such as laws, regulations, or state actions like surveillance, can, and do, have a chilling effect on people's activities online" (2017, p. 22). Further, in *Understanding Chilling Effects* (2022) Penney would also rely on social science fields to propose a "social conformity theory" of chilling effects. In this article, workshopped at PLSC 2020, he would challenge the conventional understanding of chilling effects as deterrence and self-censorship, highlighting instead the productive side of chilling effects: "chilling effects involve not just an absence—a lack of speaking or doing—but also shape behavior" (2022, p. 1455).

Furthermore, a few other scholars (Birnhack, 2019; Ford & Price II, 2016; MacCarthy, 2017; Sloan & Warner, 2016; Zubrzycki, 2021) would introduce a related harm—"harm to a social context", which Mark MacCarthy would define as "when people *withdraw* from the context in order to protect themselves. This can take place, for instance, when people do not go to a doctor, lawyer, or priest or do not disclose information fully in order to avoid having the information divulged in other contexts and used against them" (2017, p. 403).

Like scholars writing in the 1990s about the harm to individual autonomy and its consequent effect on social participation and democracy (Kang, 1998; Reiman, 1995; Schwartz, 1999), these authors would similarly highlight how the harm to a social context impacts not only individual but also collective values. "When contexts are harmed, the harm is not purely personal. The loss is not just financial, physical or psychological harm to specific people. Instead, *the cost is social*," MacCarthy would contend. "In the example of the loss of confessional confidentiality, a certain religious practice ceases to exist as certainly as if it had been declared illegal" (2017, pp. 403–404). Similarly, when referring to the growth of black-box medicine, Roger Allan Ford & W. Nicholson Price II would claim: "[p]rivacy creates environments that foster cooperation, trust, and

confidence; without privacy, people are likely to be far more guarded in their interactions, or to avoid interactions that would benefit society" (2016, p. 28).

Importantly, these claims about the social value of privacy—and which had been going on since the 1990s—should not be confused with the claims explained later (see Sub-section 1.2.6) around the relational character of privacy. Unlike the social value of privacy here reviewed, which evidences itself when individual harms affect also *social values* such as democracy, creativity, or innovation, the relational character of data refers to cases when people's inherent connections to each other turn an individual harm into a *group harm*.

### 1.1.3. Strictly privacy harms

In third place, several scholars[86] would also point out to strictly privacy concerns that emerge from the combination of enhanced data collection and the use of Big Data analytics. In particular, they would refer to the **threats to individual autonomy, dignity, and the ability to communicate anonymously** that derive from the following practices: (i) the fact that "*new and unexpected insights are inferred* from data that individuals have intentionally disclosed" (Mulligan et al., 2016, p. 2); (ii) the fact that *sensitive information can be derived* from apparently innocuous pieces of data or even from non-personal information; and (iii) "the *use of data in ways that could not have been anticipated* and therefore, would not have been included in a privacy notice" (Bruening & Culnan, 2016, p. 563). Lilian Edwards & Michael Veale would expand on this latter practice as follows:

[86] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Bellovin et al., 2019; Birnhack, 2019; Bronfman, 2015; Bruening & Culnan, 2016; I. N. Cofone, 2017; Edwards & Veale, 2017; Fluitt et al., 2019; Froomkin, 2017; Hiller & Blanke, 2017; D. Hirsch et al., 2019; Kaminski, 2019; Mulligan et al., 2016; Paterson, 2018; Polonetsky & Tene, 2015; Sloan & Warner, 2016; Slomovic, 2017; Wachter & Mittelstadt, 2019)

> ML and big data analytics in general are fundamentally based around the idea of repurposing data, which is in principle contrary to the data protection principle that data should be collected for named and specific purposes. (…) Connected problems are that "big data" systems encourage limitless retention of data and the collection of "all the data" rather than merely a statistically significant sample (…). (2017, p. 32)

### 1.2. Dominant harms

Despite the importance of the discussion of the aforementioned traditional harms, during this period five other harms *dominated* the sample of American privacy law scholarship here reviewed, becoming even intertwined in many instances. Although the five of them had already been addressed to a greater or lesser extent in previous periods, the last three would only become dominant during this period.

#### 1.2.1. Procedural injustice (threat to algorithmic accountability)

The first harm that dominated the discourse during these years is procedural injustice or the harm to due process. Since at least 2008, the dismantling of critical procedural safeguards by automated decision-making systems had become an issue in the privacy legal scholarship (Citron, 2008; Citron & Pasquale, 2014; I. Kerr, 2013). At that time, Danielle Keats Citron would highlight the erosion of due process guarantees like "notice-and-comment participation, transparency, and political accountability" (2008, p. 1258).

Building on this idea, in 2015 Margaret Hu would contend that the government's Big Data blacklisting programs did not only breach procedural but also substantive due process rights. In her view, "big data blacklisting systems create an administrative and noncriminal 'guilty until proven innocent' concern for the digitally blacklisted. The process of big data blacklisting and the digital suspicion it creates are an infringement upon a fundamental liberty interest" (2015, p. 1742).

Similarly, Dennis Hirsch and his co-authors (D. Hirsch, 2020; D. Hirsch et al., 2019) would include procedural unfairness as one of the potential harms identified by their interviewees.

However, between 2015 and 2020 this harm to due process quickly evolved to what would become a threat to algorithmic accountability.[87] This development was indeed described by Woodrow Hartzog and Neil Richards in the following way: "Citron has argued for a 'technological due process' that is ensured in these systems. *The modern discourse around this topic* has centered around algorithmic fairness, transparency, and accountability" (2020, p. 1758). But what would this re-packaged harm specifically entail? According to Lilian Edwards & Michael Veale,

> [h]opes of feeling in control of these systems are dashed by *their hiddenness, their ubiquity, their opacity, and the lack of an obvious means to challenge them* when they produce unexpected, damaging, unfair or discriminatory results. Once, people talked in hushed tones about "the market" and how its "invisible hand" governed and judged their lives in impenetrable ways: now it is observable that there is similar talk about "the algorithm," as in: "I don't know why the algorithm sent me these adverts" or "I hate that algorithm." (2017, p. 19)

Therefore, in the framework of Frank Pasquale's book *The Black Box Society: The Secret Algorithms That Control Money and Information* (2015),[88] many of the authors would raise the "black-box" character of algorithms as the main cause of this threat to rule-of-law values (Desai & Kroll, 2017; Ford & Price II, 2016). In Deven R. Desai & Joshua A. Kroll's view, "[o]ften the claim is that society cannot understand or govern these outcomes because *the decision process is a black box*. A consistent theme is that *unaccountable machines* have taken center stage (…)" (2017, p. 3). Additionally, a related but distinct claim would be posed by Ryan Calo & Citron, who in 2021 would highlight how "automation by agencies threatens to erode long-standing

[87] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Edwards & Veale, 2017; Gürses & Van Hoboken, 2017; Hartzog & Richards, 2020; Kaminski, 2019; Katyal, 2019; Regan, 2020; Selbst & Barocas, 2018; Wachter & Mittelstadt, 2019; A. Waldman & Martin, 2022; Zeide, 2017).
[88] Which was not part of the studied sample.

justifications for having agencies at all" (2021, p. 803), namely, "their ability to accrue expertise and the prospect of flexible and nimble responses to complex problems" (2021, p. 804).

### 1.2.2. Algorithmic discrimination (unfairness)

During this period, an overwhelming number of scholars would also refer to the harm of unfairness and algorithmic discrimination. According to these scholars, however, this harm can manifest in at least four entangled but still different ways.

First, some scholars would talk about data-driven discrimination "in decisionmaking contexts that are covered by antidiscrimination law, such as housing, employment, and credit" (Coen et al., 2016) (Ajunwa et al., 2017; Ford & Price II, 2016; Sloan & Warner, 2016; van Hoboken, 2016). Relatedly, several other scholars would refer to discrimination against members of historically disadvantaged groups—commonly referred to as invidious discrimination.[89] Following Kate Crawford & Jason Schultz (2014), who had already wrote about this in the previous period, these scholars would not only talk about the use of algorithmic decision-making systems that include legally protected classes as part of their variables, but also proxies of these classes.

Following Dennis Hirsch (2014b), another group of scholars (Ajunwa et al., 2017; J. R. Bambauer et al., 2022; Gerards & Zuiderveen Borgesius, 2022; Hu, 2017; Kim, 2017; Wachter et al., 2021) would refer to the use of innocuous variables to discriminate. Thus, unlike cases of invidious discrimination, in these cases—described by Janneke Gerards & Frederik Zuiderveen Borgesius with the term "unfair differentiation" (2022, p. 5)—automated decisions are made based

[89] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Ajunwa, 2020, 2021; Ajunwa et al., 2017; J. R. Bambauer et al., 2022; I. Cofone, 2019; I. N. Cofone, 2017; Gerards & Zuiderveen Borgesius, 2022; D. Hirsch et al., 2019; Polonetsky & Tene, 2015; Tene & Polonetsky, 2017; A. Waldman & Martin, 2022; Wang, 2022; Zeide, 2017).

on non-traditional and counter-intuitive categories, such as patterns of social media behavior or type of web browser used. Thus, as Jane R. Bambauer, Tal Zarsky, & Jonathan Mayer (2022) would describe in *When a Small Change Makes a Big Difference: Algorithmic Fairness Among Similar Individuals* (2022), in these cases small odd binary inputs, such as the use of Mac or PC, have outsize effects on a decision-making process's output. In that sense, for these cases "[a] certain type of proxy might not ring 'alarm bells' like other data would have. We know that income can act as proxy for gender, for example, but how do browsing behaviour, likes on Facebook, or clicks on webpages correlate with protected attributes?" (Wachter et al., 2021, p. 29). As explained by Margaret Hu,

> disparate treatment stemming from cybersurveillance and dataveillance *may not be characterized as traditional discrimination*: discrimination on the basis of a historically protected class, for instance, race, color, ethnicity, national origin, and sex. This type of identity-management, technology-based discrimination may, therefore, *fall outside current interpretations of the scope of the Fourteenth Amendment's Equal Protection Clause* and outside the reach of the protection of civil rights statutes. (Hu, 2017, p. 695)

In fourth place, instead of highlighting the type of activity or group impacted, another group of scholars would tend to focus on the effect of these discriminatory activities (Ajunwa, 2020; Barocas & Selbst, 2016; Benthall & Viljoen, 2021; Bodie, 2022; Edwards & Veale, 2017; Kaminski, 2019; Katyal, 2019; Kim, 2020; Selbst, 2017). For these scholars, algorithmic decisions based on observations of past human behaviors can reinforce or exacerbate existing patterns of discrimination, inequality, and disadvantage. In consequence, many of these scholars would use their scholarship to explain the different technical ways through which these discriminatory harms could be reproduced by automated decision-making systems. In 2016, for example, Solon Barocas & Andrew Selbst developed a taxonomy of five mechanisms by which these disproportionately adverse outcomes might occur. According to them,

> [d]ata mining can go wrong in any number of ways. It can choose a target variable that correlates to protected class more than others would, reproduce the prejudice exhibited in the training examples, draw adverse lessons about protected classes from an unrepresentative sample, choose too small a feature set, or not dive deep enough into each feature. Each of these potential errors is marked by two facts: the errors may generate a manifest disparate impact, and they may be the result of entirely innocent choices made by data miners. (2016, p. 729)

Finally, several scholars would follow suit from Danielle Keats Citron & Frank Pasquale (2014) and from various authors studying abusive online conducts (D. E. Bambauer, 2014; Citron, 2009; Lipton, 2012), who between 2008 and 2014 had started to highlight the discriminatory or disparate impact of certain abusive conducts on historically subjugated groups. Between 2015 and 2020, an overwhelming number of scholars would similarly denounce the disparate burden of surveillance (Brayne et al., 2023; Bronfman, 2015; Franks, 2017; Madden et al., 2017; Mir et al., 2018; Skinner-Thompson, 2017; Stark et al., 2020; A. Waldman, 2019), hate crimes (Citron, 2014), and other privacy abuses (Hartzog & Richards, 2020) on marginalized populations. Mary Ann Franks, for intance, would propose the concept of "intersectional surveillance" to describe "how those subjected to multiple sources of subordination are also subjected to multiple sources of surveillance" (2017, p. 431). Relatedly, others would refer to how conducts such as identity theft (Brensinger, 2023) have a different and more perjudicial effect on them, or to how "information inequality" can also discriminate against marginalized populations who inhabit the "surveillance gap" (Gilman & Green, 2018).

### 1.2.3. Online manipulation

Another harm prominently discussed by American privacy law scholars writing between 2015 and 2020 is online manipulation. Following Ryan Calo (2014), as well as sparse mentions to manipulation indentified in Chapters II to IV, during this period an overwhelming number of

scholars[90] would refer to how firms apply the insights of behavioral science and take advantage of their users' cognitive vulnerabilities and biases to manipulate them "in both commercial and political fields" (Wang, 2022, p. 69). In the political context,

> [p]ersonal data can be used to drive friendly voters to the polls, to nudge unfriendly ones to stay home, or to influence voters in others ways, whether by the Obama campaign's data scientists in 2012, or by Cambridge Analytica to influence the outcome of the Brexit Referendum and the 2016 Presidential Election. (Hartzog & Richards, 2020, p. 1759)

In the commercial sphere, when talking about the sharing economy firms, in 2017 Calo & Alex Rosenblat would claim: "Increasingly, firms use what they know about consumers not only to match them to content they might prefer but also *to nudge consumers to pay more, to work for less, and to behave in other ways that advantage the firm*" (2017, p. 1650). Similarly, when referring to mHealth apps, Marijn Sax, Natali Helberger, & Nadine Bol would explain:

> As it becomes possible to personalize nudges and continually adjust their timing and content on the basis of the personal characteristics and circumstances of the nudgee, the potential to manipulate people into forming certain desires or displaying certain behaviours also grows. Hypernudges could, for instance, *be used to target people with personalized communications exactly at those moments they are most susceptible to being influenced*. (2018, p. 106)

In parallel, several scholars[91] would begin to refer to what is now commonly known as dark patterns: "user interface designs that researchers deem problematic" (Mathur et al., 2021, p. 1). Initially coined by user experience designer Harry Brignull in 2010, this concept would become widely used by PLSC scholars during this period. Through these design-based tactics, information-

[90] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (R. Calo & Rosenblat, 2017; Desai & Kroll, 2017; Hartzog & Richards, 2020; Hartzog & Solove, 2015; D. Hirsch, 2020; D. Hirsch et al., 2019; Hull, 2021; Jones, 2015; Kaminski, 2019; Kim, 2020; N. M. Richards & Hartzog, 2016, 2021; Rubinstein & Hartzog, 2016; Sax et al., 2018; Slomovic, 2017; Susser et al., 2019; Tene & Polonetsky, 2017; Wachter & Mittelstadt, 2019; Wang, 2022)

[91] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Cohen, 2019b; Edwards & Veale, 2017; Hartzog, 2018a; Luguri & Strahilevitz, 2021; Mathur et al., 2021; N. M. Richards & Hartzog, 2021; A. Waldman, 2019; A. E. Waldman, 2022a, 2018a)

intensive companies intervene online contexts, interfaces, and choice architectures to manipulate users in different ways, including causing them to disclose more personal information. As explained by Ari Waldman, "[i]n much the same way that the design of public spaces can influence behavior, website design can discourage us from reading privacy notices, make them transparent, or coerce us into mismanaging our privacy contrary to our true intentions" (2018a, p. 133). However, "[u]nlike brick-and-mortar manipulation, dark patterns are hiding in plain sight, operate on a massive scale, and are relatively easy to detect" (Luguri & Strahilevitz, 2021, p. 48).

### 1.2.4. Diminished exposure to differing perspectives

A fourth harm of this list of dominant harms is diminished exposure to differing perspectives. Also referred to as "narrowcasting and filter bubbles" (Polonetsky & Tene, 2015, p. 982), Cynthia Dwork & Deirdre K. Mulligan (2013) had initially brought up this harm in 2013 (see Chapter IV), and during this last period of study a number of scholars would add to it (Kaminski, 2019; Katyal, 2019; Kim, 2020; Polonetsky & Tene, 2015; Regan, 2020; Sandfuchs & Kapsner, 2016).

In the context of classrooms and schools, for example, Jules Polonetsky & Omer Tene would cite Joseph Turow's research to raise how "by 'pigeonholing' individuals into pre-determined categories, automated decision making *compartmentalizes society into pockets, or 'echo chambers,' of like-minded individuals*. The ability to amass granular information regarding individuals' viewing habits and target specially tailored content at them raises concerns over siloization and narrowcasting" (2015, pp. 982–983). Going even further, both Sonia K. Katyal (2019) and Priscilla Regan (2020) would add how the "[s]egmentation and the targeting of political messages to selected subgroups of the population" (Regan, 2020, p. 492) contribute to the spread of misinformation and fake news. For Katyal, for instance, "[s]ince algorithms tend to show users

content that can affirm their existing interests and beliefs, within these filter bubbles, fake news flourished, perhaps affecting the results of the 2016 U.S. election" (2019, p. 57).

### 1.2.5. Subordination, oppression, exploitation, and social inequality

The last dominant harm could be described with a variety of terms such as subordination, oppression, exploitation, and social inequality (Hartzog, 2018a; Paterson, 2018; Stark & Levy, 2018; Viljoen, 2021; A. E. Waldman, 2022a). Following pioneer Marcy Peek (2003), the main point of the authors talking about this harm is that consumer surveillance deepens social inequalities, materializing new forms of oppression and subordination. In Moira Paterson's view, for example, "[t]he danger lies in the use of surveillance as a basis for automated decision-making and the *oppressiveness* that this can create in contexts where the individual is unaware of what is being collected and of the potential consequences that might follow" (2018, pp. 9–10). Relatedly, Dennis Hirsch and his collegues would explain: "Advanced analytics can use predictive attributes in order to allocate social goods such as loans, jobs or college admissions. Insofar as more privileged classes tend to possess these attributes to a disproportionately greater extent than others, analytics can entrench *social inequalities and divisions*" (2019, p. 4). However, one of the most popular accounts of this harm was proposed by Salomé Viljoen in 2021. According to her,

> [d]atafication (or, more precisely, data production) is wrongful if and when it materializes *unjust social relations* along either the vertical or horizontal axis. These unjust social relations may take the form of *exploitative data relations* that generate unfair wealth distributions, as well as data relations that materialize forms of *group oppression* like racism, sexism, and xenophobia. (2021, p. 631)

### 1.2.6. Transversal trends

As a final note, two transversal trends can be identified across many of the descriptions of these five dominant harms: (i) the relational character of data; and (ii) constant worries about the *exacerbation* of power asymmetries.

Building on Mark MacCarthy's concept of "negative privacy externalities" (2011) (see Chapter IV), between 2015 and 2020 an overwhelming number of American privacy law scholars[92] would highlight how, "[d]ecisions to consent to data collection are never purely personal decisions. Instead, one person's decision to consent to sharing their information frequently implicates others sharing some sort of connection with them" (Waldman, 2022, p. 93). Consequently, during these years more and more scholars would come to realize the way in which the harms mentioned above affect not only individuals but social groups. According to these authors, "[a]mongst the most challenging may be the fact that the personal data of others may be as significant as one's own data" (van Hoboken, 2016, p. 252). In that sense, "many of the problems with algorithms are more problems for groups than for individuals" (Edwards & Veale, 2017, p. 83), "[b]ecause these harms operate *by reducing opportunities for members of a group as a whole*" (Kim, 2017, p. 901).

Drawing from the article *The Networked Nature of Algorithmic Discrimination (2014),* published by danah boyd, Karen Levy & Alice Marwick in 2014 and not included in this sample of articles, some scholars would refer to this **relational character of data** by using expressions such as "networked privacy harms," "in which users are simultaneously held liable for their own behavior and the actions of those in their networks" (Madden et al., 2017, p. 56). Writing in 2017, Alice Marwick and danah boyd themselves (along with Claire Fontaine) would add:

[92] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Barocas & Levy, 2020; Edwards & Veale, 2017; Hartzog & Richards, 2020; Jia & Xu, 2016; Kim, 2017, 2020; Kroll, 2018; Madden et al., 2017; Marwick et al., 2017; van der Sloot, 2017; van Hoboken, 2016; A. E. Waldman, 2022a)

"[c]onceptualizing privacy as networked suggests that individual control over personal privacy is impossible, as people's inherent connections to each other, and the contextual nature of information, are explicitly made visible through both data-driven technologies and social media" (2017, p. 10). Solon Barocas & Karen Levy, in turn, would term this phenomenon as "privacy dependencies." For them, "individuals' privacy always depends on others' discretion" (2020, p. 558). More recently, Salomé Viljoen would refer to it as "data's relationality." In Viljoen's view,

> Prior to the widespread availability of large-dataset computing technology, data about a data subject like Adam may have been valuable because it helped businesses, employers, the government, and insurers know things about Adam. And to some extent, this is still what makes data about Adam valuable.
> But what makes data about Adam particularly and distinctly valuable for the contemporary digital economy is *its capacity to help companies make predictions or change the behaviors of others based on relevant population features they share with Adam*—in other words, on the basis of at-scale population-level horizontal data relations. It is this relational value of data that drives much of the imperatives to data access, processing, and use. (2021, pp. 610–611)

Finally, during these years the aformentioned dominant harms would also tend to be associated with concerns about **the *exacerbation* of power asymmetries**. As pointed in Chapter II, since mid-1990s scholars where already referring to the existance of power imbalances (Froomkin, 1996a; J. R. Reidenberg, 1995; Schwartz, 1999). Likewise, in the years 2000 through 2007 (Chapter III) Daniel Solove (2001, 2007, 2002b, 2002a) and others (Cuijpers, 2007; Nehf, 2003; Nissenbaum, 2004; Phillips, 2003; Schwartz, 2000a) alluded to the power asymmetry between individuals and bureaucratic institutions.

Yet, between 2015 and 2020 many scholars would point to the *worsening* of these asymmetrical relationships (J. Bambauer & Zarsky, 2018; Gürses & Van Hoboken, 2017; Hartzog, 2018a; Hartzog & Richards, 2020; Newman, 2017; Regan, 2020; Stark & Levy, 2018; van Hoboken, 2016). For them, the rise of Big Data and sophisticated data analytics, design, and

consumer self-surveillance activities, among others, have vested data-extractive firms with an unparalleled power, while making individuals and social groups more vulnerable.

***

To be sure, the five dominant harms mentioned above would not always be considered by scholars as privacy harms *per se*. Although sometimes explicitly introduced as privacy harms/problems (I. Cofone, 2019; Regan, 2020), in many other cases privacy law scholars would present them *along* privacy harms (Katyal, 2019), as *consequences* of the lack of privacy (Regan, 2020), as "risks to the *fundamental interests linked to* privacy, such as equality, autonomy, and intellectual freedom" (Barrett, 2018, p. 3), as "broader concerns *intertwined with* privacy" (Rubinstein & Petkova, 2020, p. 760), or as "harms in *areas well beyond* privacy" (D. Hirsch et al., 2019). Other times—especially in the case of the harm to due process and algorithmic accountability, privacy would not even be considered in addressing them.

As pointed out by Ryan Calo and myself in *Distinguishing Privacy Law: A Critique of Privacy as Social Taxonomy* (2024), other than the social recognition criterion proposed by Daniel Solove (2006a) in his 2006 taxonomy and employed again by him and Danielle Keats Citron in a 2022 privacy typology, during these years a clear "limiting principle" and a "rule of recognition" (Calo, 2011a, p. 1134) for privacy harms did not seem to exist. Therefore, even when it was unclear whether all of these harms could be classified as privacy harms, many of these scholars would in many cases recommend addressing them through so-called privacy tools.

## 2. Proposed privacy tools

Between 2015 and 2020, the scholars here reviewed would continue to walk down the path they had begun in the previous period of separating themselves from the FIPs-based approaches. In

addition to exploring additional reasons to justify the FIPs' unsuitability for addressing the harms mentioned above, throughout these years many American privacy law scholars would specifically criticize the individual privacy rights approach implied in the FIPs. Furthermore, while some scholars would continue to try to update the FIPs, the majority of them would build on previous efforts (e.g., collaborative governance mechanisms) or add new alternatives (e.g., algorithmic accountability, risk-based proposals) to their already wide array of regulatory proposals. By the end of the period, however, many of the scholars reviewed here would start to coincide around what could be considered a more hands-on batch of alternative solutions.

### 2.1. Increased criticism of the FIPs (and their implied individual privacy rights approach)

Even more than in the previous studied period (Chapter IV), between 2015 and 2020 a massive number of American privacy law scholars would criticize the Fair Information Practices (FIPs) as ill-suited for the Age of Algorithms.[93] As highlighted by Meg Leta Jones since the beginning of this period, "the more pressing rationale is a movement away from the process FIPPs prescribes" (2015, p. 257). From education (Zeide, 2016) to smart cities (Hiller & Blanke, 2017), scholars would explain the shortcomings of the process-based and individual rights approach "in the electronic, mobile, and social media environment" (Hiller & Blanke, 2017, p. 330). Even, Ari Waldman would come to describe individual privacy rights as "traps" which "will do additional harm to privacy" (2022, p. 90).

[93] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Bennett & Raab, 2020; Birnhack, 2019; Cohen, 2019b; Ford & Price II, 2016; Hartzog & Richards, 2020; Hiller & Blanke, 2017; D. Hirsch et al., 2019; D. Hirsch, 2020; Hull, 2021; Paterson, 2018; Regan, 2020; N. M. Richards & Hartzog, 2021; A. E. Waldman, 2022a; Zeide, 2016)

Among other reasons for criticism, scholars would pinpoint to the fact that the FIPs rely on the artificial character of notice and consent (Barrett, 2018; Birnhack, 2019; Hartzog & Richards, 2020; D. Hirsch, 2020; Hull, 2021; Paterson, 2018; A. E. Waldman, 2022a); the lack of use of the right to access data (Birnhack, 2019); the increasingly blurry concept of Personally Identifiable Information (PII) (Paterson, 2018); the FIPs' failure "to account for data externalities such as environmental harm, attention theft, and degradation of social interaction" (Hartzog & Richards, 2020, p. 1695); their "complete disregard for how an inherently social, inference-based economy actually functions" (A. E. Waldman, 2022a, p. 94); and the general incompatibility of predictive analytics with the control paradigm (Cohen, 2019b; D. Hirsch, 2020), as evidence of their unfitness. According to Dennis Hirsch, for example,

> Today, however, *companies can use this surface data to infer additional, latent information that may be far more sensitive than that which the person thought they were sharing*. For example, Target used purchase histories to infer pregnancy status; Cambridge Analytica took Facebook "likes" and inferred psychological type. In such a world, individuals cannot understand what information they are really disclosing and, as a consequence, cannot make a meaningful choice about whether or not to share the information in the first place. This is not a trivial shift. (…) *individuals cannot use the tools that privacy law has provided them—notice, choice, and purpose limitation—to protect themselves from these threats*. (2020, pp. 445–446)

Similarly, in 2022 Ari Waldman would argue:

> In the privacy space, individual rights look good on paper. Legislators will throw some rights at a political and economic problem, point to the bill they passed, and say, "Look what we did!" When, inevitably, *the data-extractive economy makes headlines for its privacy invasions, manipulative tactics, and violations of civil rights—none of which are limited by individual rights*—conservative and neoliberal policymakers will claim that too much regulation stifles innovation, insist they addressed the problem, and go home. *Individual rights leave extractive business models wholly intact*. (2022, p. 103)

### 2.2. Proposals to update the FIPs

Nevertheless, as happened between 2008 and 2015, during the first years of this period some of the scholars here reviewed would still keep some faith on this procedural approach, suggesting different ways to update the FIPs. In 2016, for example, Neil Richards & Woodrow Hartzog would propose

> *their rejuvenation* from a procedural means of manufacturing consent into a substantive system of regulating the processing of personal data in the interests of all. Trust can provide the source of that rejuvenation, allowing us to *rethink the FIPs* in ways that are positive, substantive, and inspiring, rather than pessimistic, procedural, and depressing. *When viewed through the lens of trust-building the existing FIPs of Confidentiality, Transparency, and Security* become the substantive obligations of Discretion, Honesty, and Protection. Even more importantly, when we thinking about privacy in terms of trust suggests *the adoption of a new Fair Information Practice: Loyalty*. (2016, p. 458)

Relatedly, looking to reconcile data philanthropy with the *purpose specification* and *use limitation principles*, in 2019 Yafit Lev-Aretz would propose an exception to the FIPs, which would rely on a "three-tiered review process for determining the appropriate balance between privacy protections and social benefit in any given case" (2019, p. 1492).

In turn, same as in the previous period, other scholars kept exploring the possibility of improving the *consent mechanisms* and *privacy notices*, as key components of the FIPs.[94] In terms of consent mechanisms, Ignacio Cofone would suggest, for example, targeting web browsers instead of websites, treating different kinds of cookies in a different way, and preferring an opt-in/active choice system "in which there is no default and people must choose between neutrally presented options" (2017, p. 48). Similarly, in the context of healthcare, Charlotte A. Tschider

[94] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Bronfman, 2015; Bruening & Culnan, 2016; I. N. Cofone, 2017; Cohen, 2019b; Cranor et al., 2016; Habib et al., 2019; Martin, 2015; Tschider, 2018; A. Waldman, 2019; A. E. Waldman, 2018a; F. Zuiderveen Borgesius & Poort, 2017).

would propose a "Choice-First Model" that "enables an individual to make discretionary, contextual decisions about their personal information in a prior and continuous model" (2018, p. 1535).

Regarding privacy notices, Jillisa Bronfman (2015), for instance, would suggest designers and developers to rely on Americans with Disabilities Act ("ADA") standards when designing privacy notices for devices and platforms used by the older populations. Relatedly, in addition to the existence of traditional privacy policies, Lorrie Faith Cranor, Pedro Giovanni Leon, & Blase Ur (2016) as well as Hana Habib and her co-authors (2019) would recommend providing online privacy notices in a standardized format. According to Cranor et al., "[b]ecause the same information is located in the same place on each standardized notice, consumers can directly compare two or more institutions' privacy practices by placing these institutions' standardized notices next to each other" (2016, p. 26).

Ari Waldman (2019; 2018a), in turn, would suggest intervening the "design, aesthetics, and presentation" of privacy notices (2018a, p. 131). Finally, Paula J. Bruening & Mary J. Culnan (2016), Frederik Zuiderveen Borgesius & Joost Poort (2017), and Julie Cohen (2019b) would go even further, asking for privacy notices to be accompanied with mandated transparency and a requirement of meaningful disclosures "about the automated logics involved in processing personal information" (Cohen, 2019b, p. 7)[95]. In Bruening & Culnan's view,

[95] Notably, Cohen would accompany the requirement of meaningful disclosure with the following additional conditions:

> If a requirement of meaningful disclosure is to have any teeth, moreover, it needs to be accompanied by *skepticism toward broad trade secrecy claims* that would shield key information about logics and consequences from disclosure. Additionally, a requirement of meaningful disclosure can function as a regulatory lever only if it is backstopped by *robust consumer protection laws guaranteeing individual consumers meaningful access to goods and services on acceptable terms even after they decline to provide certain items of personal information*. (2019b, p. 8)

> [t]o achieve the openness required by the first fair information practice principle, data protection and privacy should *move from a "notice" model to one of "transparency."* It also asserts that the terms "notice" and "transparency" are not synonymous and that different definitions apply to each. It also defines notice as the posted articulation of a company's privacy practices and policies. In contrast, *transparency is a condition of disclosure and openness jointly created by companies and policy makers through the use of a variety of approaches, including notice*. (2016, p. 521)

### 2.3. Algorithmic accountability tools

Linked to this last suggested intervention to privacy notices—mandated transparency—is a broader tool, which seems to move even further away from the FIPs: algorithmic accountability. To a great extent, the algorithmic accountability approaches of this period would be inspired by previous work done by legal scholars such as Danielle Keats Citron (2008), Ian Kerr (2013), Kate Crawford & Jason Schultz (2014), and Citron & Frank Pasquale (2014). Yet, a significant influence on them would also come from "the budding field of algorithmic fairness, accountability, transparency, and ethics (commonly referred to as "FATE")" (J. R. Bambauer et al., 2022, p. 2340). While initially separated from the field of Privacy law, between 2015 and 2020 an overwhelming number of American privacy law scholars would draw from and contribute to this emerging field, to address the harms referred to above as harm to due process and algorithmic accountability, and algorithmic discrimination. In that sense, during these years a large portion of the reviewed literature would grapple with tools such as **transparency** and **explainability**.

Transparency proposals[96] would include requiring all types of disclosures, including transparency of data practices and information flows, disclosure of the fact of the system's

[96] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Benthall & Viljoen, 2021; Helberger et al., 2017; Hu, 2015; Katyal, 2019; Kim, 2020; Paterson, 2018; Polonetsky & Tene, 2015; Poort & Zuiderveen Borgesius, 2019; N. M. Richards & Hartzog, 2016; Rubinstein, 2018; Tene & Polonetsky, 2017; A. E. Waldman, 2022a; Zeide, 2016, 2017; F. Zuiderveen Borgesius & Poort, 2017)

existence, transparency of source codes or training data, transparency of algorithms' inner working and/or algorithmic editing practices, as well as whistleblower protections.

Regarding explainability, in the wake of the GDPR scholars within this community began to explore the reach and scope of the so-called "right to an explanation" (Doshi-Velez et al., 2017; Sloan & Warner, 2019; Wachter et al., 2018). Specifically, they would discuss about the kind of questions that "legally-operative explanations" (Doshi-Velez et al., 2017, p. 2) should respond to while still respecting trade secrets and predictive performance, "why and when explanations are useful enough to outweigh the cost" (Doshi-Velez et al., 2017, p. 12), and the aims that explanations should have (namely, assist affected data subjects to act, instead of simply understand the internal workings of complex technical systems) (Wachter et al., 2018).

For Sandra Wachter, Brent Mittelstadt, & Chris Russell, for instance, an unconditional counterfactual explanation "provides data subjects with meaningful explanations to understand a given decision, grounds to contest it, and advice on how the data subject can change his or her behaviour or situation to possibly receive a desired decision (e.g. loan approval) in the future" (2018, p. 844). Later on, Wachter and her co-author Brent Mittelstadt (2019) would complement this ex-post remedy with a right to reasonable inferences.

Still, a significant number of scholars writing during this period would disagree on the effectiveness of transparency and explainability. Ira Rubinstein & Woodrow Hartzog (2016), for example, would consider approaches that focus on transparency and disclosures as ineffective for responding to the failure of anonymization mentioned above. Roger Allan Ford, in turn, would show himself skeptical about the benefits of the transparency of data collection and processing activities. According to him,

> [i]ncreasing the transparency of information collection, use, and disclosure, and increasing the control that individuals have, would surely reduce some of the costs of

> exercising that control. *But it would not reduce those costs enough to allow individuals to exercise meaningful privacy choices for each and every potential privacy loss in their lives—every collection, use, and disclosure of information about an individual*. (…) Some contexts are better suited than others for strategies that aim to make information flows more transparent and give information subjects the power to control how information about them is collected, used, and disseminated. Such strategies may be more likely to work, for instance, when the underlying information flows are unusually important to the information subject, since in those circumstances it will be more worthwhile to spend the time and make affirmative privacy choices. But trying to extend those strategies to the myriad contexts in which information about individuals is collected, used, and disseminated is very likely a hopeless task. (2016, pp. 1113–1115)

And with regards to *algorithmic* transparency in particular, several scholars (Edwards & Veale, 2017; Kim, 2017; N. M. Richards & Hartzog, 2021; Wachter & Mittelstadt, 2019; A. Waldman & Martin, 2022; Wang, 2022), would challenge the merits of traditional transparency solutions as a mechanism for legal-political accountability. According to Deven R. Desai & Joshua A. Kroll, for example,

> transparency is a powerful concept and has its place. After all, who can argue against sunlight? And yet, to an extent, we do exactly that, because from a technical perspective, general calls to expose algorithms to the sun or to conduct audits will not only fail to deliver critics' desired results but also *may create the illusion of clarity in cases where clarity is not possible.* For example, as discussed infra, fundamental limitations on the analysis of software meaningfully limit the interpretability of even full disclosures of software source code. (2017, p. 5)

In fact, Hao Wang would go even further, framing algorithmic transparency as a disciplinary technique. "[W]hat if algorithmic transparency itself is a form of manipulation? What if some algorithm deployers intentionally disclose the workings of their algorithms in order to operate its power of control and to only meet their own interests?" (2022, p. 69), Wang would contend.

An even more intense debate would arise around explainability. In light of the difficulty in finding "meaningful" explanations about the logic of Machine Learning, Lilian Edwards &

Michael Veale, for example, would describe the right to an explanation as a "non-fruitful path to take" (2017, p. 22). According to these authors,

> Individual data subjects are not empowered to make use of the kind of algorithmic explanations they are likely to be offered (…). Individuals are mostly too time-poor, resource-poor, and lacking in the necessary expertise to meaningfully make use of these individual rights. In some ways, the transparency fallacy is even worse than its consent cousin, since the explanation itself may not be meaningful enough to confer much autonomy even on the most empowered data subject. (2017, p. 67)

In a similar fashion, Mary Madden, Michele Gilman. Karen Levy, & Alice Marwick would adopt a realistic approach to this right. In their view,

> [w]hen it comes to governmental benefits, a notice and explanation of denial is fairly straightforward because these determinations are usually made in the context of objective eligibility criteria. However, such requirements would engender a radical reshaping of the workplace, higher education, and related settings if every disappointed applicant were entitled to a reason for their rejection along with a dossier of algorithmic formulas that might have contributed to the rejection, especially given that big data often interacts with individual discretion in these situations. (Madden et al., 2017, pp. 119–120)

Relatedly, Joshua A. Kroll would argue against the alleged benefits of the right to explanation. For him, although it isn't true that systems are necessarily inscrutable,

> *[n]or is an individual right to explanation a remedy for opacity*. Such a right sidesteps questions of aggregate effects like *group fairness and nondiscrimination,* while failing to provide individual understanding of particular decisions or to address power dynamics between individuals and computer systems or to facilitate governance of those systems. Understanding how a system fits into its sociotechnical context reveals a stronger set of interventions based around harmonizing the action of systems with the norms demanded by their context. (2018, pp. 2–3)

As a result, as adequate alternatives to offer information about the design efforts behind technical systems, many of these scholars would suggest instead **algorithm auditing**[97] and **algorithmic impact assessments**.[98]

In her 2021 article *An Auditing Imperative for Automated Hiring Systems*, for example, Ifeoma Ajunwa would claim that "when employers choose to use algorithmic systems, fulfilling their duty of care entails *regular audits* of those systems. In turn, audits necessitate the record-keeping and data retention mandates that I also propose in this Article" (2021, p. 6). Relatedly, when addressing Small Change Makes a Big Difference ("SCMBDs") situations in algorithmic decision-making, Jane R. Bambauer, Tal Zarsky, & Jonathan Mayer would explain: "there are two types of algorithm audits: process-focused audits that seek to explain a specific algorithmic decision about an individual, and outcome-focused audits that review algorithms against fairness criteria. Both types of audits could be used to address SCMBD concerns" (2022, p. 2411).

In terms of algorithmic impact assessments (AIA), in 2017 Andrew Selbst (2017) would recommend using them as "a tool to fill in knowledge that is currently lacking—knowledge necessary to even determine how future regulation should proceed" (2017, p. 119). Analogously, in another article written along with Solon Barocas (Selbst & Barocas, 2018), he would reiterate the importance of providing documentation about the decisions behind the models, to ensure that individuals can not only address the problem of inscrutable decisions but also understand the model's normative valence. Finally, in response to criticism based on how the algorithmic impact

[97] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Ajunwa, 2020, 2021; J. R. Bambauer et al., 2022; Desai & Kroll, 2017; Edwards & Veale, 2017; Hull, 2021; Katyal, 2019; Kim, 2020; Kroll, 2018; N. M. Richards & Hartzog, 2016; Selbst & Barocas, 2018; Van Loo, 2019).
[98] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Edwards & Veale, 2017; Hartzog & Richards, 2020; Katyal, 2019; Kim, 2020; Selbst, 2017, 2021; Selbst & Barocas, 2018)

assessments would operate on the ground, in 2021 he would narrow their expected effects by making clear that

> AIA regimes will likely not be effective enough to be the final word on policy. But, given the information disparities between developers on the one hand, and policymakers and the public on the other, *regulation that can slow down the development process, create pathways for public input, and push information out to the public can be an important step toward both mitigating current harms and developing better, more concrete regulation in the future*. (Selbst, 2021, p. 125)

Selbst & Barocas were not the only ones to propose impact assessments. During these years, Michael Froomkin (2015), Edwards & Michael Veale (2017), Sonia K. Katyal, (2019), and Peter Swire (2022) would respectively suggest the use of Privacy Impact Notices ("PINs"), Data Protection Impact Assessments (DPIAs), the crafting of a Human Impact Statement in Algorithmic Decisionmaking according to three key elements, and the implementation of a Portability and Other Required Transfers Impact Assessment (PORT-IA) to evaluate portability initiatives based on fourteen structured questions.

Notably, these two accountability proposals—audits and impact assessments—combine two broader regulatory trends that would become popular among scholars during these years: (i) a risk-based approach and (ii) what Dennis Hirsch (2013) had already described in the past as "collaborative governance."

### 2.4. Risk-based proposals

As described by Meg Leta Jones, "[r]isk-based accountability approaches have been proposed in the wake of FIPPs criticisms. A risk-based approach increasingly allows data controllers and users to assess the risk the use poses to the data subject" (2015, p. 256). Between 2015 and 2020, examples of this approach—which "newly perceived importance" was also reflected in the GDPR

(Bennett & Raab, 2020, p. 456)—could be found in the scholarship of authors such as Paul Ohm (2015), Ira Rubinstein & Woodrow Hartzog (2016), Neil Richards & Woodrow Hartzog (2016), Daniel Solove on his own (2021) and along with Danielle Keats Citron (D. J. Solove & Citron, 2018) and Woodrow Hatzog (D. J. Solove & Hartzog, 2022), as well as Aaron Fluitt and his co-authors (2019). Between 2015 and 2020, these scholars would more and more come to support "the claim that privacy policy can devise strategies not only to mitigate effects but to anticipate and prevent them" (Bennett & Raab, 2020, p. 459).

Paul Ohm, for instance, would suggest adopting a risk-based approach with regards to *sensitive information*. According to him, "we need better, more formal, and more rigorous frameworks for assessing the risk of privacy harm. Rather than focusing on anecdotes and intuition, we should design 'privacy threat models,' learning from computer scientists who study security and risk" (2015, p. 1125). In 2016, in turn, Rubinstein & Hartzog would advise the adoption of a risk management approach to *anonymization/deidentification*. In their view,

> the best way to move data release policy past the alleged failures of anonymization is to focus on the process of minimizing risk, not preventing harm. We argue that *focusing on process and risk* can bridge the concerns of formalists (for whom mathematical proof is the touchstone of any meaningful policy) and pragmatists (for whom workable solutions should prevail over theoretical concerns). This change in focus *reframes the debate away from the endpoint of perfect anonymity and toward the process of risk management.* (2016, p. 706)

### 2.5. Proposals of collaborative governance

Regarding Hirsch's proposed tool of "collaborative governance" (2013), during these years this term would re-appear in this sample of articles thanks to Margot Kaminki's scholarship. In her 2019 article *Binary Governance: Lessons from The GDPR's Approach to Algorithmic Accountability*, Kaminski would draw on regulatory design and private-public partnerships literature to characterize ex ante technical requirements, auditing, oversight boards, whistle-blower

protection, and risk assessments, among other public- and stakeholder-facing accountability mechanisms, as "collaborative governance." "I identify that many recent calls for *systemic approaches to algorithmic accountability* are in fact calls for collaborative governance. I also identify that the EU's GDPR represents an attempt to use collaborative governance towards algorithmic accountability, combined with a system of individual rights" (2019, p. 1533), Kaminski would claim.

In Kaminski's view, collaborative governance mechanisms are useful to address many of the instrumental worries raised by scholars during the last several years—and here documented, namely, error, unfairness, discrimination, and bias. In particular, these mechanisms are especially useful "to affect both the design of algorithms and the organizational design of the human systems around them" (2019, p. 1553). However, Kaminski would also argue that in order to be effective in governing algorithmic decision-making, collaborative governance mechanisms should: (i) be rooted in a "regulatory system that is legitimate, immunized from capture, and strong enough that it is different in kind from self-regulation" (2019, p. 1533); and (ii) be accompanied by individual rights—a combination she refers to as a two-pronged, "binary governance." The latter, in order to also be able to address dignitary (dignity- and autonomy-based) and justificatory (due process-based) concerns surrounding algorithmic decision-making. Notably, although proposing one of the tools here presented as alternatives to the FIPs, for Kaminski, the FIPs' individual privacy rights are still fundamental for this collaborative governance system to work.

Unlike authors proposing isolated audits and impact assessments, by characterizing algorithmic accountability mechanisms as collaborative governance, Kaminski would not only

open the door for a wider array of accountability tools[99]—including the "responsive regulation" approach that William McGeveran (2016) and Moira Paterson (2018) propose based on Ian Ayers & John Braithwaite's theory (1992), but also restore and redefine the role of transparency—criticized by many in this community—in the system. According to her, "[b]ecause regulators will be delegating rulemaking of sorts to private parties, *we need not just transparency and oversight over the algorithm, but second-order transparency and oversight over that rulemaking and compliance process* (2019, p. 1536).

Thus, piggybacking on Kaminski's approach, during these years some of the scholars mentioned above (Ajunwa, 2021; Selbst, 2021), as well as others (Van Loo, 2019), would frame their accountability proposals within this broader concept of collaborative governance. Likewise, Kaminski and her co-authors Anupam Chander and William McGeveran (Chander et al., 2021) would point to collaborative governance as one of the characteristics that differentiate the GDPR (which has taken a vague approach) from the CCPA (which follows a granular style).

[99] Consequently, the toolkit proposed by Kaminski is broader, encompassing "soft and hard law along multiple axes." According to her,

> The goal is to retain both enough give in the legal system that private actors will be incentivized to participate and enough strength in the system that they are motivated to do so towards the public good. Collaborative governance tools range from the more to the less formal and deploy more or less government involvement. *More formal "coregulatory" methods* include negotiated rulemaking, legal safe harbors to encourage the adoption of industry codes of conduct, and the incorporation by reference of technical standards. In these formal methods of collaborative governance, it is clear that the government's goal is structured delegation to or collaboration with the private sector.
> *Less formal methods of collaborative governance* include audited self- regulation, informally "delegating" the interpretation of broader standards to private actors, applying performance standards instead of specific rules, and encouraging private ordering in response to unappealing defaults crafted in the law. These less formal methods may escape identification as collaborative governance tactics or, indeed, may not be deliberately collaborative on the part of the government at all. But they perform collaborative functions by structuring the involvement of the private sector in determining the substance or implementation of regulation and in overseeing compliance with it. (Kaminski, 2019, pp. 1564–1565)

### 2.6. Hands-on set of measures

Evidently, not every scholar reviewed during this period would support the algorithmic accountability proposals, whether presented as isolated tools or as part of a collaborative governance system. In particular, scholars such as Julie Cohen (2019b, 2019a) and Ari Waldman (A. E. Waldman, 2020, 2022) would criticize these proposals as "legal managerialism."[100] Seeding an idea that she would further flesh out in her book *Between Truth and Power: The Legal Constructions of Informational Capitalism* (2019a) —which was not part of this sample, in 2016 Cohen would claim:

> In terms of institutional structure, the data processing industry has generally acquiesced in the FTC's emerging practice of regulation by consent decree, and that stance is a calculated one. It accedes to *cumbersome, but ultimately procedural, audit and disclosure requirements in order to forestall regulatory imposition of more substantive standards of privacy protection*. (2016, pp. 219–220)

Following suit, in 2020 Waldman would denounce the emergence of a "growing privacy compliance market," where not only adherence to privacy law is being conceptualized as a compliance task, but the privacy law itself is being co-opted, suffering a process of legal endogeneity where "mere symbols of compliance are standing in for real privacy protections" (2020, p. 776). Consequently, he would argue, rather than consumer interests, corporate goals and values end up being protected. Moreover, and building on Cohen's work, in 2022 Waldman would add:

> *The managerial information economy reflects the will and the interests of managers and leaders of government,* those with strong interests in the status quo and the revolving door of industry and government. We need the rule of law to shrink the power of *corporate*

[100] Although not part of the sample of papers here reviewed, a better picture of Cohen & Waldman's joint approach on this matter can be seen in their co-authored article *Framing Regulatory Managerialism as An Object Of Study And Strategic Displacement* (2023), presented as an Introduction to the Symposium "Regulatory Managerialism And Public Governance".

> *compliance departments that weaponize processes of legal managerialism, such as privacy impact assessments, record keeping, and audits*. (2022, p. 105)

Therefore, as a substitute, both Cohen and Waldman, as well as many others, would resort to tools that instead of targeting the algorithms or data practices, would intervene both the companies' data-extractive business models and the practices of system design. As a result, the last—and probably most hands-on—batch of alternative solutions includes, among others, the following three tools: (i) design interventions; (ii) fiduciary duties; and (iii) substantive rules and prohibitions.

### 2.6.1. Design-based interventions

Building on scholarship from the previous period, between 2015 and 2020 several scholars would keep proposing **Privacy by Design ("PbD")** as a preferred alternative.[101] Specifically, these scholars would advocate for legislation to mandate companies to take privacy into account throughout the entire engineering lifecycle and encourage the incorporation of privacy protections into products by design.

In 2018, for instance, Woodrow Hartzog would publish his book *Privacy's Blueprint: The Battle to Control the Design of New Technologies*, an extract of which was discussed at PLSC 2016. Arguing for a "design agenda for privacy law," Hartzog would argue:

> [T]he design of popular technologies is critical to privacy, and the law should take it more seriously. Law and policy makers can do so through recognition and guidance. *Lawmakers and courts should better recognize how design shapes our privacy*. Torts, contracts, consumer protection, and surveillance laws can all better reflect how design influences our perceptions and actions with respect to our information. *Privacy law*

[101] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Bhatia & Breaux, 2018; Bronfman, 2015; I. N. Cofone, 2017; Edwards & Veale, 2017; Hartzog, 2018a; Kim, 2020; Mir et al., 2018; Mulligan et al., 2016; Ohm & Frankle, 2018; Sandfuchs & Kapsner, 2016; Shilton & Greene, 2019; Stark, 2016; A. Waldman, 2019; A. E. Waldman, 2018b, 2018a; Wong & Mulligan, 2019a).

> *should guide the design of information technologies to protect our privacy. The law must set boundaries and goals for technological design* (2018a, p. 7)

Also in 2018, Paul Ohm & Jonathan Frankle would equally call for legislators to "consider mandating desirable inefficiency in order to address various concerns about information systems" (2018, p. 784). As a design principle, "desirable inefficiency" has been used by computer scientists for years to make space in technologies for human values (e.g., fairness, trust) other than efficiency. Thus, in their article Ohm & Frankle would suggest it as an additional way to embed values into code.

Similarly, in her article *Turning Privacy Inside Out*, Julie Cohen (2019b) would stress that, instead of designing for seamless data harvesting, companies should be required to operationalize the principles of semantic discontinuity and operational accountability through design. In her view, "[a] semantic discontinuity principle would require the deliberate pursuit of durable strategies for foreclosing and disrupting information flow in ways that frustrate seamless legibility and manipulation" (2019b, p. 24). In turn, "[a]n operational accountability principle would direct regulatory attention to matters such as the nature and quality of explanations about data collection and processing and the possibilities for giving both individual users and society more generally a say in the sorts of legibility we are willing to underwrite" (2019b, pp. 24–25). In other words, for Cohen the goal of both principles would be to destabilize current organizational rhythms.

Finally, in three consecutive articles, Ari Waldman (2019; 2018b, 2018a) would highlight the importance of establishing transparency-enhancing design requirements both on the books (in the law) and on the ground (in practice, by corporations). And, more specifically, in his 2019 article *Privacy's Law of Design* he would draw from the principles of products liability for design defects to propose a model for what a privacy by design statute should look like.

Unlike the previous period, during these years a significant portion of the Privacy by Design ("PbD") literature included in the reviewed sample came from non-legal scholars. To enrich the concept of Privacy by Design, for example, Deirdre Mulligan and her interdisciplinary co-authors (Mulligan et al., 2016; Wong & Mulligan, 2019b) would leverage the approaches to privacy and design proposed in the fields of informatics and human-computer interaction (HCI). Linked to Ryan Calo's (2010) idea of anthropomorphic design and "visceral notices," in 2016 Luke Stark would draw from critical design and reflective design methodologies to propose the practice of "data visceralization." According to him, "developing user interfaces that exploit haptic and aromatic technologies alongside visual and auditory strategies, digital objects can provoke a reflective emotional response tied to the user's visceral sense of privacy" (2016, p. 26).

Computer scientists Jaspreet Bhatia & Travis D. Breaux (2018), in turn, would suggest an empirical framework for determining which personal data are most at risk and which contextual factors increase or decrease that risk, so that designers can more effectively make informed software development design decisions. Darakhshan J. Mir, Yan Shvartzshnaider, & Mark Latonero (2018) would rely on Contextual Integrity and Community Based Participatory Research to propose a participatory framework to ensure that the socio-technical systems are engineered with the privacy concerns and related anxieties of marginalized populations in mind. And in 2019 Katie Shilton & Daniel Greene would investigate the mobile "development practices that encourage developers to define, and then design for, privacy" (2019, p. 132). According to them,

> Discovering these practices points to *actors who can be influential in encouraging ethics-oriented software design*, including mobile platform companies, analytics companies, and users in addition to ethicists and educators. Articulating these practices, and the ecosystem of firms and individuals who encourage those practices, moves us one step further toward encouraging developers to prioritize privacy practices and features in software design. (2019, p. 145)

A related popular solution, derived from PbD and also partly originated in disciplines other than law, could be described as **data-science techniques**. Despite the technical shortcomings of anonymization (Ohm, 2010) already discussed in Chapter IV, some scholars[102] would keep discussing the advantages of this by-now long debated technical solution. Nevertheless, during these years they would adopt a process-based approach, transitioning from a dichotomy (anonymous/identified) to a spectrum of degrees (Birnhack, 2019; Rubinstein & Hartzog, 2016). Some of them would even rebrand it as "the safe release of data" (Rubinstein & Hartzog, 2016, p. 757). Others, in turn, would highlight the importance of: (i) combining it with legal and administrative measures that facilitate or incentivize its use (Froomkin, 2017); and (ii) closing the gaps between legal and mathematical approaches by co-designing legal concepts based on data-science techniques between both legal and technical experts (Altman et al., 2020; Nissim et al., 2018). For Micah Altman, Aloni Cohen, Kobbi Nissim, & Alexandra Wood, for instance, in order to determine whether specific technologies are sufficient to satisfy regulatory anonymization requirements,

> [the] development of new privacy concepts that are both practically justiciable and technically coherent requires not just review by both legal and technical experts, but co-design. When new cross-domain ("hybrid") concepts are needed, it is vital that experts in all implicated fields be enlisted to assist early in the design process.

Likewise, during this period several scholars—including various computer scientists—would also suggest the judicious implementation of novel technical tools, such as differential privacy[103] and—to a lesser extent—synthetic datasets (Bellovin et al., 2019), as promising privacy tools.

[102] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Altman et al., 2020; Birnhack, 2019; Froomkin, 2017; Katyal, 2019; N. M. Richards & Hartzog, 2016; Rubinstein & Hartzog, 2016)

[103] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Bellovin et al., 2019; Dwork et al., 2019; Fluitt et al., 2019; Katyal, 2019; Mir, 2021; Nissim et al., 2018; N. M. Richards & Hartzog, 2016; Wood et al., 2018)

According to Neil Richards & Woodrow Hartzog, for example, "[m]ore robust techniques of deidentification are being developed, such as k-anonymity and differential privacy, and Protection requires that entrustees (especially sophisticated commercial ones) stay abreast of such Protection innovations" (2016, pp. 467–468). Similarly, but from a technical perspective, Alexandra Wood, Micah Altman, Aaron Bembenek, Mark Bun, & Marco Gaboardi would refer to the benefits of differential privacy. According to them, "[d]ifferential privacy is supported by a rich and rapidly advancing theory that enables one to reason with mathematical rigor about privacy risk. Adopting this formal approach to privacy yields a number of practical benefits for users" (2018, p. 213). Finally, alluding to synthetic data, in 2019 Steven M. Bellovin, Preetam K. Dutta, and Nathan Reitinger would argue:

> First, synthetic datasets *are better than traditional anonymization techniques* (i.e., deidentification). Second, current laws are inadequate; while synthetic data may be permissible under some circumstances, the statutes do not appreciate the full benefits or risks of synthetic data. And third, *synthetic data—if constructed properly—may solve Professor Ohm's failure of anonymization*. (2019, p. 49)

### 2.6.2. Fiduciary duties

In terms of fiduciary duties, during the years under study (2015-2020) Neil Richards & Woodrow Hartzog would come to write a saga of co-authored articles on trust and the duty of loyalty. Starting in 2016 with *Taking Trust Seriously in Privacy Law*, Richards & Hartzog would highlight the necessity of having trusted information relationships. For this purpose, in this article they would mainly propose the rejuvenation of the FIPs mentioned above. However, the article would also draw on the law of Fiduciaries—and on previous attempts by Jack Balkin and Daniel Solove to use it as well in the privacy context—to introduce the concept of "loyalty" as one of the foundational values of Privacy Law. According to Richards & Hartzog,

> (…) we argue that there should be limits on the amount of self-dealing one can engage in after being entrusted with personal information. Consent via the fine print of a legal agreement no one reads is disloyal and illegitimate. One of the biggest fears in the modern information economy is that personal information obtained from users will be used against their interests. The obligation of Loyalty aims to prevent that from happening, and should be enshrined in statutes as well as the common law torts and consumer protection law. (2016, p. 436)

However, unlike Balkin and Solove, Richards & Hartzog would make it clear that in their own approach not all relationships of trust would automatically qualify as fiduciary in nature. In their view,

> [i]mposition of the full panoply of fiduciary duties is a serious and burdensome decision. But the law need not face the binary choice of treating information relationships as either "fiduciary" or "unprotected." Surely *some middle ground exists* between these two extremes. Accordingly, we recommend that *duties inspired by fiduciary law can apply in a flexible and variable way* across the full spectrum of information relationships. (2016, p. 458)

In fact, their desired degree of flexibility would be crystalized five years later in the 2021 article *A Duty of Loyalty for Privacy Law*, workshopped at PLSC 2020. In this article, which would be published after various others not discussed at PLSC (and therefore not included in this sample), Richards & Hartzog explain the exact obligations that a duty of loyalty in Privacy Law would require from those entrusted with personal information. For them,

> loyalty would manifest itself primarily as a *prohibition on designing digital tools and processing data in a way that conflicts with a trusting party's best interests*. Data collectors bound by such a duty of loyalty would be *obligated to act in the best interests of the people exposing their data and engaging in online experiences, but only to the extent of their exposure*. (2021, p. 966)

Between the publication of these two articles (N. M. Richards & Hartzog, 2016, 2021), a number of scholars workshopping papers at PLSC would also touch to a greater or lesser extent

on fiduciary duties-related concepts.[104] In the context of the sharing economy, for example, Ryan Calo & Alex Rosenblat would offer the imposition of fiduciary obligations as one of three possible alternatives to answer to the asymmetries of information and power existing between sharing economy firms and consumers. As a hybrid approach, this avenue is praised by the authors for importing a relatively mature area of law premised upon information and power asymmetries, and also avoiding possible First Amendment objections. However, the authors clarify, in order to become a viable alternative, this approach "requires a means by which to ensure fiduciary obligations are being met" (R. Calo & Rosenblat, 2017, p. 67). Relatedly, in 2020 Ifeoma Ajunwa would argue that "hiring platforms are performing a brokerage function [with regard to job applicants' information] and thus should be considered fiduciaries" (2020, p. 276).

Even, concurrent to Richards & Hartzog's 2021 article, Mark MacCarthy would also publish his article *Enhanced Privacy Duties for Dominant Technology Companies*, also workshopped at PLSC 2020. In this article, MacCarthy would call Congress to impose enhanced privacy duties on "technology companies that also are dominant in their line of business" (2021, p. 5), including special duties of care, loyalty and confidentiality. According to him, "[i]f a dominant technology company is not bound by special duties of care, loyalty and confidentiality, it can exploit its customers' vulnerabilities without fear that they will flee to viable alternative providers" (MacCarthy, 2021, p. 6).

Finally, and in the context of the workplace, in a 2022 article discussed at PLSC 2020, Matthew T. Bodie would argue for the imposition of fiduciary responsibilities on employers as to workers' data, given employers' perfect match with the concept of information fiduciaries. "The exact

[104] In order to avoid disrupting the flow of the paragraph, this list of cited sources has been moved to a footnote. (Ajunwa, 2020; Bietti, 2023; R. Calo & Rosenblat, 2017; Chander et al., 2021; McGeveran, 2019; Regan, 2020; A. E. Waldman, 2018b).

nature of the duties imposed upon employers as information fiduciaries would be open to further development," Bodie would argue. "The critical notion would be one of protection: employers would be prohibited from using employee data to harm them opportunistically" (2022, p. 751).

### 2.6.3. Substantive rules and prohibitions

Adding to sparse proposals (D. D. Hirsch, 2014b; MacCarthy, 2011; Ohm, 2010) from the previous period (Chapter IV), between 2015 and 2020 an overwhelming number of scholars would continue the trend of shifting from procedural to substantive standards. In a way, the main rational behind this shift would be to "offer[] social protection where individuals cannot protect themselves" (D. Hirsch, 2020, p. 443). Besides, as Salomé Viljoen would clearly explain,

> the task is to *develop the institutional responses necessary to represent (and adjudicate among) the relevant population-level interests at stake in data production*. In other words, responding adequately to the economic imperatives and social effects of data production will require moving past proposals for individualist data-subject rights and toward *theorizing the collective institutional forms required for responsible data governance*. (2021, p. 579)

In practice, an increasing number of articles published during these years would operationalize this approach by calling for the establishment of outright substantive prohibitions of specific data collection, processing, use, and disclosure activities. Among them, scholars would propose: prohibitions on reidentification and deceptive deidentification (N. M. Richards & Hartzog, 2016; Rubinstein & Hartzog, 2016); prohibitions on processing specific categories of sensitive data (Cohen, 2019b); prohibitions on data practices that go against the best interest of the data subjects (which intersect with the duty of loyalty covered above) (N. M. Richards & Hartzog, 2021); bans to certain types of personal data transfers (D. J. Solove, 2021); prevention of certain data collection and data use activities "when they go beyond people's likely expectations or when they are unfair

or potentially harmful" (D. J. Solove, 2021, p. 50); prohibitions of technology designs that are insecure, or unreasonably deceptive, abusive, or dangerous/risky (Hartzog, 2018a; MacCarthy, 2021; D. J. Solove, 2021); bans on behavioral targeting location tracking (A. E. Waldman, 2022a); and democratically-established distinctions between legitimate and illegitimate data use as well as just and unjust data relations (Viljoen, 2021).

According to Gordon Hull, for instance, "[t]he problems need to be addressed at the *structural level*. For example, if inaccurate credit reporting causes harm, then *the use of credit reporting could be restricted* and *other 'do not use' rules could be put on private information*" (2021, p. 20). Likewise, in Dennis Hirsch's view, a new legal and regulatory paradigm "must shift from a liberalist regulatory approach that seeks to facilitate individual choice, to one that *empowers public officials to make choices about which predictive analytics practices are safe for individuals and consistent with social values and which are not*" (2020, p. 462).

Importantly, many of these and other scholars would nevertheless be cautious about the reach and scope of the proposed prohibitions. For Ira Rubinstein & Woodrow Hartzog, "blanket and robust prohibitions on information collection and disclosure would be incredibly costly to organizations and society as a whole. Shutting down research and the information economy would be devastating. Even if such restrictions were wise and politically palatable, they would likely be ineffective given the existing data ecosystem" (2016, p. 731). Similarly, Pauline Kim would highlight a key distinction when it comes to prohibiting access to sensitive information:

> Restricting access to information *can be effective* in preventing intentional discrimination when the employer would not otherwise know about the protected characteristic and therefore would be unable to act on that basis. However, restricting access to sensitive information *is not likely to be effective* in preventing classification bias that results from data analytic models. (…) On the other hand, the problem of omitted variable bias means that *prohibiting the collection or use of sensitive data may sometimes increase the biased effects of a data model*. Thus, *a simple prohibition on access to sensitive information will not prevent classification bias, and in some cases could make it worse*. (2017, p. 898)

Likewise, given that machine learning-based predictive tools are constantly looking for workarounds to experienced constraints, Julie Cohen would recommend legislators to design no-flow and low-flow of personal information mandates differently. In particular, they "would need to be specified in terms designed to secure compliance by automated machine-learning systems (…) [as well as] complementary strategies for incentivizing compliance with low-flow and no-flow directives" (2019b, p. 29).

One last noteworthy example comes from Mark MacCarthy, who would ask himself whether there are "uses of data by dominant technology companies that should be banned, rather than be subjected to the procedural limits described so far (…)". For him, the answer to this question is case-dependent: "the question cannot be answered in the abstract. It might be possible to formulate a good reason to ban the use of information for a specific purpose in the context of a specific business" (2021, p. 88).

Notably, in a few cases, a combination of design interventions, fiduciary duties, and outright prohibitions would be presented by scholars as part of **wider, holistic interventions**, composed of a rich variety of additional tools also proposed by American privacy law scholars over the years. In *Privacy's Constitutional Moment and the Limits of Data Protection*, for example, Hartzog & Richards (2020) propose a "third way," which not only tackles power disparities within relationships through duties of loyalty, but also includes a wide variety of measures intended to address the corporate structure and business incentives, data collection and processing risks, and data externalities. In a similar fashion, in 2021 Waldman would claim:

> We need to move away from process-oriented, check-box visions of privacy law that are susceptible to symbolic structures. Fortunately, *we have other options*. Woodrow Hartzog has called for *leveraging contract, tort, and consumer protection law to regulate the design of new technologies*. Elsewhere, I argued for *leveraging lessons from the law of*

> *products liability for design defects to create an accountability regime for companies that design technologies with insufficient designed-in privacy protections*. (…) In addition, Jonathan Zittrain, Jack Balkin, Daniel Solove, Danielle Citron, and I have argued that *data collectors should be treated as fiduciaries of our information* and, therefore, subject to similar duties of care, loyalty, and confidentiality that characterize our relationships to doctors, lawyers, and trustees. (…).

A year later, in *The New Privacy Law* (2021)—an article that was not part of this project's sample of articles, Waldman would include these and other measures (e.g., civil rights approaches, direct regulation of the Internet business model) as part of a holistic intervention labeled by him as "a 'third wave' for Privacy Law" (2021, p. 40).

### 2.7. Tools drawn from other areas of law

To be sure, even during this period scholars would keep recurring to other areas of law—in addition to Fiduciary law— to look for alternatives to the FIPs. In particular, sporadic references to solutions coming from **Tort law** (Ajunwa, 2020; Hartzog & Richards, 2020; Skinner-Thompson, 2020; A. E. Waldman, 2018b) and, to a lesser extent, **Patent law** (Wilka, 2018) could be highlighted. Nevertheless, their weight during these years can be considered minimal in comparison to the overwhelming number of scholars discussing the rest of the tools reviewed in this Chapter.

***

From this Chapter, several reflections can be drawn. Besides algorithmic discrimination and procedural injustice (which had been already discussed by scholars in the previous period), the other harms that became dominant during this period—online manipulation, diminished exposure to differing perspectives, and subordination/oppression—can also be characterized as *objective*, and as stemming from the *actual processing phase* of the data cycle. Online manipulation, for

example, materializes outside of the individual's psyche, as a decision they make in detriment of their own interests. Likewise, the reason why it can happen is because the personal data of that individual (or of the individuals in their social groups, as will be seen below) is processed to infer their cognitive vulnerabilities.

In addition, the way in which scholars writing during this time describe these five dominant harms also makes them worthy of a new characteristic, namely, *architectural* or *modern*. According to Daniel Solove, one of the instances in which "architectural privacy problems" manifest is when "a particular activity can *upset the balance of social or institutional power in undesirable ways*" (Solove, 2006, p. 487).

In order to see how algorithmic discrimination, procedural injustice, online manipulation, diminished exposure to differing perspectives, and subordination/oppression are architectural, it is worth to go back to the "the relational character of data" highlighted by various scholars during this period. As explained in Sub-section B.1.2.6, many of the scholars here reviewed consider that the aforementioned harms have effects not only on specific individuals, but also on the larger groups these individuals are part of. In particular, they can have effects on other individuals who, by sharing characteristics or any other sort of connection with the profiled individual, are part of the social groups in which the initial data subject is being categorized. In that sense, the dominant harms here reviewed can be pervasive, affecting entire social groups and therefore, upsetting the balance of social or institutional power these groups enjoy. In fact, it may be due to these identified dynamics that, compared to previous periods, it was during this period that scholars called out almost unanimously the existence of power imbalances in society.

In terms of the regulatory tools proposed by scholars during this period, it is interesting to highlight how the state of flux that re-emerged between 2008 and 2014 would continue for some

time during the period here under study. Nevertheless, and possibly animated by this period's "techlash," by the end of the 2010s a large number of scholars would slowly start to coalesce. This time, however, around a set of alternatives that might be considered more hands-on in comparison to the FIPs. Thus, instead of aiming to give power *to* individuals, a significant number of scholars would propose tools (i.e. design-based interventions, fiduciary duties, and substantive rules and prohibitions) intended to take power *away* from corporations, by intervening their data-extractive business models and system design practices.

Finally, at least two things should be noted regarding the interaction between the scholars' work and the legal systems in place during this period. In the first place, it is fascinating to note that, although many of the legislative initiatives introduced during these years failed, they attempted to address precisely the types of harms that dominated the sample of American privacy law scholarship for this period (i.e., the 'disparate impact' resulting from data analysis and targeted use, the use of dark patterns for manipulation). As a second point, it is noteworthy that, although some of the initial alternatives considered by scholars during this period (e.g., algorithmic accountability tools, risk-based approaches, collaborative governance mechanisms) may have been influenced to a greater or lesser extent by legal developments in the European Union, the batch of hands-on tools emerging by the end of the period exhibit a distinctive American character.

### C. How privacy's algorithmic turn came to happen

So, how did privacy's algorithmic turn actually happen? As I hope to have demonstrated in this and the last three Chapters, between 1990 and 2020 the community of scholars that has developed *around* PLSC wrote extensively about emerging technologies. In the framework of numerous technological developments, a frenzied legal system, and an American society that almost until the

end of the studied period appeared—*in the eyes of scholars*—ambivalent about the value of information privacy, the scholars here reviewed took on the task of examining the sociotechnical legal problems posed by these technologies, as well as different ways in which the American legal system should respond to them.

Through almost indiscernible reformulations of traditional harms, proposals of new harms, and re-bounce of sparsely mentioned harms, between 1990 and 2020 scholars transitioned from focusing primarily on autonomy-based harms to raising a vast array of harms that share the following three characteristics: being *objective*, originating from the *actual processing phase* of the data cycle, and having *architectural* effects. In the process, scholars shifted twice from states of regulatory innovation and flux (uncertainty about what the best regulatory approach would be) to those of relative convergence regarding the preferred techniques to protect information privacy.

This intellectual history begins during a time of flux (1990-1999), when scholars seemed to agree about the harms posed by the technologies and practices of the epoch but were uncertain about what the best tool would be to address them. In the first phase of cohesion and agreement (2000-2007), scholars almost unanimously supported the binding implementation of the FIPs, trusting in the power of procedural standards to *empower individuals*. Yet, the community's disillusionment with these principles' ability to address the newly identified harms shattered this stability within the intellectual community. After a second period of flux (2008-2018(?))—which could be said to have been partly impacted by the European Union's regulatory developments during this period, by the end of the third studied decade scholars seemed to be entering a new phase of cohesion, but this time around a hands-on set of substantive requirements, duties, and prohibitions intended to *take power away from corporations*.

As advanced in the Introduction, these two transformations with regard to the scholars' (i) identified harms and (ii) proposed privacy tools constitute the main two features of the "privacy's algorithmic turn" experienced by the concept of information privacy in a considerable portion of American privacy law scholarship.

## VI. The Transformation of Techno-legal Imaginaries

Having traced, in detail, the development of privacy's algorithmic turn in the framework of a broader socio-technical and techno-legal context, several hypotheses arise about the possible sociotechnical and techno-legal causes of the turn. As mentioned in the Theoretical Framework section, it may seem at first reasonable to assume, for example, that the transition from personal computers and networks to the Internet of Things ("IoT"), algorithmic decision-making systems, and artificial intelligence ("AI") influenced the two transformations that compose privacy's algorithmic turn.[105]

Another possible explanation could be attributed to changes in the legal system. In this regard, one could propose that the transition from a relatively inactive Executive branch between 1990 and 1999 (Chapter II) to a panorama in which the FTC emerged as an important player in the American privacy landscape between 2015 and 2020 (Chapter IV) could explain, in turn, the dominance that certain harms (e.g., online manipulation, procedural injustice) acquired in American privacy law scholarship during the latter period. Or in a more granular way, that it was the inclusion of Privacy by Design ("PbD") in the FTC's report *Protecting Consumer Privacy in an Era of Rapid Change*—preliminarily released in 2010 and finally published in 2012—that sparked the scholars' interest in it as a possible legal tool in the 2008-2015 period and on.

[105] Yet, that hypothesis would not allow us to explain why, despite no revolutionary technological changes occurring between 2000 and 2007 (aside from the improvement of many already existing techniques for data collection, analysis, and use) (Chapter III), the set of legal tools offered by the American privacy law scholars reviewed here did change dramatically during that period. In particular, between 2000 and 2007 the community shifted from the state of flux and regulatory innovation experienced between 1990 and 1999 (Chapter II) to a state of relative convergence regarding (i) the inconvenience of market-based solutions, and (ii) the merits of adopting legally enacted FIPs.

Rather than testing or disproving any of these possible hypotheses, the purpose of this Chapter is to use the concept of "techno-legal imaginaries" to add a new element—a cognitive one—to the complex relationships that may exist between these different factors. As pointed out earlier, the concept of "techno-legal imaginaries" is defined here as the *visions of a given legal community about the desirable futures that could be achieved through the regulation of technology.* Applied to this particular case study, it would refer to the visions of the community of American privacy law scholars here studied, about the desirable futures that could be achieved through Information Privacy law (broadly understood).[106]

As announced in the Theoretical Framework section, by placing privacy's algorithmic turn within a broader context where technological, social, legal, and cognitive elements interact and become entangled, the concept of "techno-legal imaginaries" serves—at a *theoretical level*—to detach privacy's algorithmic turn from the algorithmic technologies reviewed in Chapters II to V and to consider it instead as an intricate sociotechnical phenomenon. Yet, how can it help us in practice?

This *practice level* was exactly what I was seeking to uncover with the second research question posed in this dissertation. What can American privacy law scholars' aspirations, expectations, and visions about the future further tell us about privacy's algorithmic turn? My goal in this Chapter is to demonstrate that the transformation of scholars' aspirations, expectations, and visions about the future over the period of time covered by this study (1990-2020) can provide us with some insight into the second feature of the turn, namely, the transformation of the tools proposed by scholars to protect information privacy. In particular, by understanding the scholars' techno-legal imaginaries and their transformation over time, we will be better able to comprehend

[106] Here, I am assuming that Information Privacy law can be broadly considered as regulation of technology.

why some privacy scholars would end up abandoning the legal implementation of the Fair Information Practices (FIPs) principles in favor of a batch of hands-on tools aimed at taking power *away* from corporations.

As will be seen, when thinking about what Information Privacy law should look like back in the late 1990s and early 2000s, many of the American privacy law scholars here studied aimed for a pluralist, free, democratic society that promoted liberty, autonomy, and self-determination. Within that normative framework, a FIPs-based legislative approach stood out as a balanced intervention, directed at empowering individuals so they could take control over their personal information. Against the backdrop of the sociotechnical developments reviewed in Chapters II to V, however, the scholars' visions of desirable future radically changed. By the end of the 2010s, a significant portion of American privacy law scholars envisioned—and keep envisioning, according to several of the oral history interviews conducted for this study—a society that besides caring about individuals' autonomy, also cares about social equality, justice, and fairness. In that sense, they expect Information Privacy law to defend the vulnerable and marginalized, protect individuals against data extraction and its consequent power asymmetries, and hold corporate power accountable. And it is within the framework of these normative commitments that the batch of hands-on tools reviewed in Chapter V makes sense.

The review of the theoretical precursors of the STS concept of "imaginaries" conducted described above highlighted the nature of "imaginaries" as the constructs of mind, which come together through *shared narratives*. Similarly, when recently studying the technological imaginaries articulated in national AI strategy papers, Jascha Bareis and Christian Katzenbach aptly pointed out how "looking at technology *narratives* serves as a means to look into desired futures, informing us about *societal strivings and aspirations*" (2021, p. 860). In consonance with

this view, in other to identify the American privacy law scholars' techno-legal imaginaries and how they have transformed over time, in this Chapter I look at the *shared narratives* found in both my sample of articles and the oral history interviews conducted. Nevertheless, I see the law review articles reviewed here, in particular, as the primary anticipatory practices that have enabled the scholars' techno-legal imaginaries to be produced and spread within the community of scholars developed *around* PLSC.

This Chapter proceeds in two parts. In Section A, I describe the techno-legal imaginary that might have shaped the scholar's preference for a FIPs-based legislative approach between 1990 and 2007. Subsequently, in Section B I describe the one that might be underlying the batch of hands-on tools proposed by a considerable group of scholars by the end of the 2015-2020 period. In each case, I explain both (1) the narratives that bring the imaginary together, as well as (2) the resulting desirable future that American privacy law scholars here reviewed expect Information Privacy law to achieve in each period.

## A. A FIPs-based legislative approach: In pursuit of a pluralistic, free, and democratic society in which autonomous individuals thrive

Having started in the early 1990s and consolidated between 2000 and 2007, by the end of the second studied period (2000-2007) (see Chapter III) there seems to be a relative convergence among a large portion of the American privacy law scholars here reviewed about the necessity of implementing legally enacted Fair Information Practices ("FIPs") principles. In particular, the push was for a comprehensive federal privacy law that could empower individuals with information and rights to take control over their personal information.

As this Section aims to demonstrate, the described approach to Information Privacy Law as mandatory FIPs was nested within a broader vision of a desirable future in which individuals could live in a pluralist, free, and democratic society that supported liberty, autonomy, and self-determination for each of them.

## 1. Narratives

The narrative construction of the techno-legal imaginary that shaped the scholars' preference for a FIPs-based legislative approach followed mainly two steps. First, scholars writing between 1990 and 2007 would often present privacy as necessary for individual autonomy. Under this framing, privacy would be depicted as a liberal, individualistic value, which allows moral persons to control how much others know about them, develop critical perspectives, make un-coerced choices, and self-determine. Second, the first narrative would be accompanied by a complementary one, according to which, privacy is a social value. As such, a loss of information privacy would not only affect the individual, but also collective values such as democracy and freedom.

### 1.1. Privacy as necessary for individual autonomy

In the scholarship published between 1990 and 2007 around personal computers, networks, and the techniques for data collection, analysis, and use developed during those years, multiple manifestations present privacy as an indispensable condition for individual autonomy.

To set the stage, during the covered years several American privacy law scholars would situate privacy in the context of liberal individualism. According to M.J. van den Hoven, for example, "[p]rivacy, conceived along these lines, *would only provide protection to the individual in his quality of a moral person* engaged in self-definition and self-improvement against the

normative pressures which public opinions and moral judgements exert on the person to conform to a socially desired identity" (1997, p. 36). As such, privacy would be therefore justified during these years by the idea that individuals are moral persons with inherent dignity and worth.

Against this normative framework, in 1999 Anita Allen would alert of the "numerous little consensual and nonconsensual privacy loses, too trivial to protest individually, [which] aggregate into a large privacy loss that is a detriment to *the liberal way of life*" (1999a, p. 540). What would—in the view of these scholars—this liberal way of life entail? When writing about the Intelligent Vehicle Highway Systems ("IVHS"), in 1995 Jeffrey H. Reiman would contend:

> The liberal vision is *guided by the ideal of the autonomous individual*, the one who acts on principles which she has accepted after *critical review* rather than simply absorbing them unquestioned from outside. Moreover, the liberal stresses the importance of *people making sense of their own lives, and of having authority over the sense of those lives*. All this requires *a kind of space in which to reflect on and entertain beliefs*, and to experiment with them-a private space (…). (1995, p. 42).

Therefore, the liberal individualism at the base of these scholars' claims about privacy would also underscore the need to protect the individuals' capacity to make choices in ways that are un-coerced by institutions or organizations. Besides, it would concretize as well in the idea of individual control. In fact, Scott Shorr would refer to these two elements—capacity to make choices and individual control—as "the decisional and control dimensions of personal autonomy" (1995, p. 1768). According to Shorr,

> Consumer monitoring impinges upon *decisional autonomy* when it *alters consumers' buying decisions*. For instance, one may decline to purchase a magazine or birth control device in a grocery store for fear that the check-out machine will record and maintain records of these transactions that unknown others can peruse, sell, and use as the basis for personal judgments. . . . Credit bureaus' effect on *the control dimension of autonomy* is even clearer. When credit bureaus divulge personal information about consumers to third parties without consumer consent, *consumers lose their ability to control how much others know about them* (…). (1995, pp. 1768–1769)

In a similar tone, but referring solely to the former dimension, in 1992 Paul Schwartz would define autonomy as "the ability to *make decisions and to act on these decisions* through participation in social and political life" (1999, p. 1362). In 1995, he would divide this decision-making capacity in two: (1) deliberative autonomy, and (2) deliberative democracy. For now, we will only concentrate here on the first one. According to Schwartz, "[d]eliberative autonomy refers to the underlying *capacity of individuals to form and act on their notions of the good when deciding how to live their lives*" (1999, p. 560).

Finally, the narrative that portraits privacy as necessary for individual autonomy was also built on the idea that information privacy protects individuals' capacity for critical reflection and thought, allowing them to self-determine. For example, in 2000 Julie Cohen would argue how "privacy *fosters (partial) self-determination*. It enables individuals both to maintain relational ties and to *develop critical perspectives* on the world around them" (2000, p. 1906). In the same way, the flip side of the coin would be the idea that monitoring and surveillance erode individual self-determination. How so? In Robert G. Boehmer's view, "artificial monitoring and surveillance has the capacity to eliminate worker autonomy. In other words, *the ability of the worker to decide how his job will be done is severely impaired*" (1992, p. 769). Similarly, writing about the government's use of computers to process personal data, in 1992 Schwartz would argue:

> Americans no longer know how their personal information will be applied, who will gain access to it, and what decisions will be made with it. The resulting uncertainty *increases pressure for conformity.* Individuals whose personal data are shared, processed and stored by a mysterious, incalculable bureaucracy will be more likely to act as the government wishes them to behave. (1992, p. 1374).

Thus, at first sight, between 1990 and the early 2000's scholars *seemed* to depict privacy as a liberal, individualistic value, which would allow moral persons to control how much others

know about them, develop critical perspectives, make un-coerced choices, and self-determine. However, a second narrative would accompany and complement this approach.

### 1.2. Privacy as a social value

In the rhetorical construction of privacy as a necessary condition for individual autonomy, American privacy law scholars writing between 1990 and 2007 would go even further, by establishing an interdependent connection between individual autonomy and certain collective benefits. "[A]utonomy matters for both the individual and society" (1992, p. 1350), Schwartz would argue in 1992.

As such, this framing would create a powerful rhetorical triangle that would shed pivotal attention to privacy as not only an individual but a social value. As Jean-François Blanchette & Deborah G. Johnson would highlight in 2002, "[p]rivacy as an individual good and privacy as a social good are inextricably tied together" (2002, p. 36). Under this narrative, privacy would be framed as a precondition for collective benefits such as democracy and freedom.

With regards, to the relationship between privacy and democracy, Paul Schwartz's scholarship could be said to be an enormous repository of this narrative. As mentioned earlier, in 1995 Schwartz would argue that the idea of deliberative autonomy should go hand in hand with the collective benefit of deliberative democracy. For him,

> Deliberative democracy requires that citizens be permitted to apply their deliberative capacities to the consideration of the justice of basic institutions and social processes. As in the area of deliberative autonomy, data protection law plays a critical role in deliberative democracy; the law must structure the use of personal information *so that individuals will be free from state or community intimidation that would destroy their involvement in the democratic life of the community*. (1995, p. 561)

Likewise, inspired by Robert Post and anchored on civic republican theory, in 1999 Schwartz would similarly proclaim: "information privacy is best conceived of as *a constitutive element of civil society*" (1999, p. 1613). In his view, "[r]ather than upholding 'the interests of individuals against the demands of community,' information privacy creates rules that in some significant measure 'constitute both individuals and community'" (1999, p. 1663). Similarly, in 2004 he would state: "At its core, information privacy has both an individual and a social value. Hence, I end on a note of caution: ongoing scrutiny of regulation of personal data is needed because failure in the privacy market *can harm both individual self-determination and democratic deliberation*" (2004, p. 2128). In fact, even during his oral history interview held in 2023, Schwartz would reiterate:

> "Privacy doesn't just exist for the individual. It ultimately matters because of *a certain kind of vision of society as being a democratic order.* That theme [has] been, you know, in my work from the very beginning, from the article in the American General Comparative Law, from my Hastings article." (oral history interview, March 29, 2023)

In a similar fashion, in her early days as a privacy law scholar, Julie Cohen would also link privacy with democracy. In her 2000 article *Examined Lives: Informational Privacy and the Subject as Object*, Cohen would generally but forcefully contend: "the values of informational privacy are far more fundamental. A degree of freedom from scrutiny and categorization by others promotes important noninstrumental values, and *serves vital individual and collective ends*" (2000, p. 1423). Regarding the types of collective ends privacy fosters, Cohen would add: "Development of the capacity for autonomous choice is an indispensable condition for *reasoned participation in the governance of the community* and its constituent institutions—political, economic, and social. The cornerstone of *a democratic society* is informed and deliberate self- governance." (2000, p.

1426). For her, thus, autonomy would generate concrete collective benefits such as democratic participation.

When it comes to the relationship that scholars would claim exists between privacy and freedom, several examples from the scholarship here reviewed are on point. For Jeffrey H. Reiman, "privacy is essential to *a free society*" (1995, p. 30). According to him,

> in a free society, there are actions thought immoral by many or even a majority of citizens that a significant minority thinks are morally acceptable. The preservation of *freedom* requires that, wherever possible, *the moral status of these actions be left to individuals to decide for themselves*, and thus that not everything that a majority of citizens thinks is immoral be made illegal. (1995, p. 35).

In a similar fashion, in 1998 Helen Nissenbaum would stress that "[t]hese two forms of privacy, namely, control over information and control over access, *are among the conditions for a free society* and, among other things, *enhance people's capacity to function as autonomous, creative, free agents*" (1998, p. 592). And in 1999, Anita Allen would add: "To speak of 'coercing' privacy is to call attention to privacy *as a foundation, a precondition of a liberal egalitarian society*" (1999b, p. 19).

As seen, between 1990 and 2007, privacy was being portrayed by these scholars as of pivotal importance for democracy and freedom. Through these collective benefits, information privacy would receive the status of a social value that needed to be fostered and protected for the sake of society.

## 2. Resulting vision of desirable future

When put together, the narratives mentioned above undergird the vision of a pluralistic, free, and democratic society where autonomous individuals could thrive.

First, this techno-legal imaginary would include a society in which individuals would be protected from coercive choices about how to live their lives. Based on a "fear of control of thought and social interaction" (J. R. Reidenberg, 1995, p. 537), this desired order was one where "protecting citizens against thought manipulation and abuses of power" (J. R. Reidenberg, 1995, p. 541) would be a priority. In fact, in line with this vision in 2000 Julie Cohen would emphasize: "there are compelling theoretical and practical justifications for legislating strong data privacy protection that creates and preserves *a zone of informational autonomy* for individuals" (2000, p. 1428).

Furthermore, the desirable future sustained by these narratives would also include a society that "values and thrives on the diversity of its citizenry" (Boehmer, 1992, p. 771). According to many of the scholars writing about information privacy in those days, thanks to the protection of their individual autonomy "individuals will develop their individual and unique characteristics" (Boehmer, 1992, p. 771). As a result, scholars would envision the emergence of a pluralistic community of individuals who would be free to grow and develop in different ways, and who would be therefore able to self-determine as they wished, without any external influence.

Finally, this desired order would be a democratic one. In the view of the scholars whose work was published during those years, individual autonomy also allows for participation in the spheres of social and political life. In that sense, in this desired order individuals would be "free from state or community intimidation that would destroy their involvement in the democratic life of the community" (Schwartz, 1995, p. 561). Having noticed this inclination of scholars writing about privacy around the turn of the twenty first century, when describing the "new privacy" in 2003 Paul Schwartz & William Michael Treanor would state: "The new-privacy scholarship calls for

majoritarian construction of privacy standards that will, in turn, help foster *the individual autonomy necessary for majoritarian governance*" (2003, p. 2184).

It was, thus, within this specific normative framework that the FIPs-based legislative approach got tracking, standing out as a balanced intervention, directed at empowering individuals to take control over their personal information. As the new century progressed, however, the vision of desirable future of the community of scholars reviewed here would begin to transform.

### B. The batch of hands-on tools: Aiming for a socially-just society in which tech corporate power is held accountable and vulnerable populations are protected

After the backlash against the FIPs occurred between 2008 and 2015, and several American privacy law scholars started to refer to the limitations of many of the FIPs principles in the framework of the Information Age, a second period of flux and regulatory innovation began in the sample of American privacy law scholarship here reviewed (see Chapter IV). Yet, by the end of the last reviewed period (2015-2020) a large number of scholars began to coalesce again around a group of tools—here referred to as the "batch of hands-on tools"—which would include, among others, the following three types of measures: (i) design interventions; (ii) fiduciary duties; and (iii) substantive rules and prohibitions.

Instead of targeting the algorithms or data practices, this set of measures is mostly aimed at intervening both the companies' data-extractive business models and the practices of system design. Likewise, instead of aiming to give power *to* individuals, these tools would look to take power *away* from corporations. Notably, as it was outlined in Chapter V, in a few cases scholars would present this batch of measures as part of wider, holistic interventions (e.g., Hartzog & Richards's "third way" (2020), Waldman's "'third wave' for Privacy Law" (2021)) composed of

a rich variety of additional tools intended to address, among other things, the corporate structure and business incentives, as well as data externalities.

As I hope to demonstrate in this Section, the described approach to Information Privacy Law as a set of hands-on measures directed to intervene the companies' data-extractive business models, the practices of system design, the corporate structure and business incentives, and even data externalities, is nested within a broader vision of a desirable future in which individuals can live in a society that protects social equality, justice, and fairness, and in which tech corporate power is held accountable and vulnerable populations are protected.

## 1. Narratives

Unlike the narratives developed in Section A, during the last years covered in this study information privacy is *not only* framed by American privacy law scholars as a necessary precondition for individual autonomy. Besides ensuring individuals' autonomy and self-determination, privacy also contributes to human flourishing, as well as to ensuring equality and justice. Yet, in order to achieve the protection of these values, the third narrative goes, privacy should be seen as a means to intervene (or tear down) the informational capitalism model.

### 1.1. Privacy as a necessary element of human flourishing

For scholars writing between the third (2008-2014) and last periods (2015-2020) reviewed, privacy would be indispensable for the realization of the person *as a whole*.

A perfect example of how this first narrative would work can be seen in Julie Cohen's renown article *What Privacy is For*. Drawing from the theory of capabilities for human flourishing developed by Martha Nussbaum and Amartya Sen, in 2013 Cohen would add to what she had

already claimed in the past in terms of self-determination and democracy, by stressing: "privacy does not only protect individuals. Privacy furthers fundamental public policy goals relating to liberal democratic citizenship, innovation, *and human flourishing*" (2013, p. 1928). In her view,

> Privacy will not always produce expressions of subjectivity that have social value, and here I mean expressly to leave open the question whether there might be particular types of privacy claims that do not merit protection or even respect. *Even so, privacy is one of the resources that situated subjects require to flourish*. (2013, p. 1911)

In a similar fashion, in 2014 Dennis Hirsch would also add the human development element to the list of social values promoted by privacy. In his own words, "[i]f this trend continues, we will pass on to our children a depleted ecosystem for the cultivation of the human personality. It is vital to *human development*, creativity and innovation that we prevent this" (2014a, p. 381). But what does human flourishing and development actually entail?

Between 2008 and 2020, a number of scholars would indeed fill these lofty goals with more specific content. In 2020, for instance, Woodrow Hartzog & Neil Richards pointed out:

> If privacy is important because it is necessary for human flourishing, our privacy-relevant rules should include *a conceptualization for human flourishing that goes beyond autonomy and dignity derived from control over data and includes mental and social well-being as we interact and expose ourselves and our information to the world*. (2020, p. 1760).

Similarly, in 2022 Ari E. Waldman would claim: "[w]e could also *think about privacy as a necessary element of human flourishing*, or the realization of the whole person, including our *physical well-being, happiness*, self-determination, *and more*" (2022, p. 53).

Consequently, as time passed, for an increasing number of the scholars here reviewed privacy would become an integral part of well-being. When viewed in this manner, as an umbrella that can accommodate and protect a broad range of values, privacy would be considered necessary not only to protect individuals' autonomy, but also to protect the values, freedoms, and rights that contribute

directly to individuals' happiness. "Properly understood," Richards & Hartzog would point out, "data privacy is about civil rights, free expression, freedom from harassment, collective autonomy interests, and how personal information is leveraged to erode our attention spans, our mental well-being, and our public institutions" (2020, p. 4).

### 1.2. Privacy as an anti-oppression and emancipation legal tool

In addition, during the last years of the 2010s a growing portion of the American privacy law scholars included in this study would also portrait Information Privacy as a legal tool to protect the marginalized and vulnerable.

For example, in his book *Privacy at the Margins*, which Chapter 6 was discussed at PLSC 2017, Scott Skinner-Thompson would argue that "privacy (both informational and while in public) *can serve important anti-subordination goals* and, indeed, that where privacy does advance anti-subordination ends for marginalized groups, legal protections for privacy rights should be at their apex" (2020, p. 6). In a similar tone, Ari E. Waldman (2021a) has recently argued:

> Privacy is *a state of freedom from overlapping forms of subordination*: corporate, institutional, and social. *Privacy's emancipatory capacities* underly Professor Citron's call for sexual privacy, which, if fully protected, would *liberate women, LGBTQ+ people, and sexual minorities* from oppressive social and institutional structures. Emancipation sits at the center of Salomé Viljoen's call for democratizing data governance to *liberate people from a system of datafication that enacts, reifies, and amplifies unjust and unequal social relations*. *Scholars and advocates should adopt this language when speaking and thinking about privacy*. Doing so will contribute to new ways of thinking about the role of privacy law, privacy litigation, and privacy wrongs. (2022, p. 1273).

Hence, according to this narrative, privacy should be thought about as a tool to promote equality and justice. In fact, when describing his desirable future in relation to privacy, during his oral history interview Woodrow Hartzog would portray "[o]ne *where our privacy rules*

meaningfully foster and protect democracy, *ensure equity*, and *an equitable distribution of power along, certainly, along all groups with, you know, hopefully groups with a particular focus on traditionally marginalized groups, like people of color, members of the LGBTIQ community*" (personal communication, February 27, 2023).

Interestingly, almost 10 years ago Antonio A. Casilli (2015) would have already proposed an illuminating explanation of this evolution in the views of what privacy can do for society. For him, this change is a reflection of a broader trend in society in which modern democracies are advocating for a more inclusive political space. According to him,

> The *care of privacy* (…) is closely linked to the democratic functioning and *has proved indissociable (sic) from the gradual extension of civil liberties and their application to increasingly large swathes of the population*. If in the past the requirement to protect privacy was not been (sic) perceived equally within populations, that was precisely because, as a concern, it is not immune to the influence of differential hierarchies and forms of subjection. *The care of privacy is becoming more widespread insofar as modern democracies advocate – at least theoretically – a political space that is accessible to all.* As Hannah Arendt would have it, it is the very possibility of accessing an active, professional and public, life that makes it necessary to draw a line between what pertains to collective achievements and what is confined to the individual's private sphere. Although this possibility was previously restricted to a specific category of individuals (free able-bodied adult men with steady incomes), *it now extends to all those (women, children, underprivileged citizens, etc.) who previously had no need to protect their privacy precisely because they were excluded from public life*. (2015, p. 8)

Under this view, the narrative here described implies, in a way, the simple extension of rights to the members of social groups who have historically been deprived of them. In fact, related to this assertion is also the idea that privacy, as a rhetorical tool, can give voice to marginalized populations, helping them to break free from historical oppressive practices. Drawing on a "critical definitional facilitation" approach that she develops in an article (Allen, 2022) which was not part of this study's sample, during her oral history interview Anita Allen would contend:

> *what this is all about is listening to what people, especially people of color and others who are marginalized, what they are saying*, what they say, understanding the problem they're trying to get at, or point to, by talking about privacy, and then evaluating the soundness of their claims, and then doing something about that. (oral history interview, March 30, 2023)

Thus, in Allen's—as well as many other scholars writing during the last years of the 2010s'—view, privacy discourse can play a political role in contemporary society.

### 1.3. Information Privacy law as a means to intervene the informational capitalism model

As seen in Chapters II to V, for years American privacy law scholars have claimed that the aggregation and uncontrolled uses of personal information critically disrupt the distribution of power between individuals and large corporations. There has, however, been a recent addition to this narrative. According to several scholars writing in the last few years, in order to rebalance these disparities of power, Information Privacy Law should intervene (or tear down) the informational capitalism model.

In her 2019 book *Between Truth and Power: The Legal Constructions of Informational Capitalism*—which was not part of this sample, Julie Cohen would define "informational capitalism" as "the alignment of capitalism as a mode of production with informationalism as a mode of development. (…) In a regime of informational capitalism, market actors use knowledge, culture, and networked information technologies *as a means of extracting and appropriating surplus value, including consumer surplus"* (Cohen, 2019a, p. 5-6).

So understood, during the last years of the 2010s, several scholars would directly or indirectly refer to this sociotechnical phenomenon as the most important target of intervention.

During her oral history interview, for example, Anita Allen would contend: "[t]he kind of legislation that it would take to give Americans control over their privacy would basically require *that we completely altered the business models of not only Big Tech, but most other companies as well*" (oral history interview, March 30, 2023).

According to the scholars reviewed for this study, the means to intervene the informational capitalism model could take many different forms. For example, they could include "(…) *imposing discipline on the claims that underpin data collection's value and working to internalise the risk such activities generate*, [so that] the cost of extractive data practices can be increased and excessive demand for such data reduced" (Benthall & Viljoen, 2021, p. 486); or "*increase[ing] obligations and restrictions on dominant parties as they amassed power*. The more power a company has in a relationship, the more protective and loyal it must be" (Hartzog & Richards, 2022, p. 10). For Julie Cohen, in turn, it would mean getting

> (…) serious about privacy governance in a register that does not really rely on "notice and choice" at all, and that *takes aim at the infrastructures that have been constructed to target communications, map behaviors, circulate communications, amplify and polarize.* And that *requires understanding how to intervene in information infrastructures*, right? Which is something that you can never do by centering individuals. And something that, I think is quite challenging, and that we haven't really fully understood yet at all. (oral history interview, February 27, 2023)

A slightly more radical approach, however, would be to tear the model down. In his oral history interview, for example, Ari Waldman would contend:

> The future that I want is an economy that's not based on, uh, profiting from data extraction. And *whether that means completely upending the entire business model of an advertising-based online system, or it means, you know, legal constraints on that system, um, my and, I don't know the answer to that. My inclination is to burn it all down, or regulate it out of, out of existence*. (oral history interview, November 30, 2022)

In a strikingly similar fashion, during his oral history interview Paul Ohm would also contend:

> I mean, I am like, a little unsparing in my belief that a lot of the big problems of the world are attributable to tech companies, and their choices, and their design decisions. And so, I think more than most scholars are willing to say, *I just want to take them down. I just want to strip them of their power and their influence. I just want to make them much less important in society. I want to take away a lot of their wealth*, right? (oral history interview, September 22, 2023)

And even for Andrew Selbst, the approach would be very similar. As we would explain during his oral history interview:

> We had a joke in Data & Society that inevitably, every conversation leads to the statement that *capitalism is really the problem*. And I think there's a degree to which I don't think it's really a joke, right? So, it's really hard for me to take my imagined futures of Information law outside of my imagined futures in general, *which is the end of sort of neoliberal visions of capitalism.* Even in a power structure in society, right? Which includes like, more power for like labor and other folks like that. Not all dying in 30 years to the environment, right? All these things, it's really hard, when I try to imagine the future, it's really hard for me to separate the issues of privacy or algorithms from those MUCH BROADER issues, partially because the reason we can't solve these issues in privacy and AI are because of the broader issues, right? Because of power imbalances, because of broken politics, because of disinformation or whatever. And so, they are all tied in together. (oral history interview, October 26, 2023)

Thus, as in previous decades, in the view of many American privacy law scholars writing during the last few years of the 2010s, Information Privacy law should re-balance the power asymmetries that exist between corporations and individuals (and groups). But for doing so, the contemporary narrative goes, the time has come for Privacy Law to intervene the model at the base of the companies' power.

## 2. Resulting vision of desirable future

In contrast to the narratives put forward between 1990's and 2007, the three narratives described in this Section underpin a vision of a socially-just society where corporate power is held accountable and social groups—especially vulnerable ones—are protected by the government.

To begin with, the desirable future envisioned by the end of the 2010s—and even today—by a big portion of American privacy law scholars is a society that cares about social equality, justice, and fairness. As suggested by Danielle Citron when stressing the importance of her Cyber Civil Rights approach, "a civil rights approach would play a valuable normative and expressive role in society. Civil rights prosecutions *would communicate society's commitment to 'values of equality of treatment and opportunity'* and make clear that conduct transgressing those values will not be tolerated" (2009, p. 90). Similarly, when developing his idea about a law of design for privacy, Ari Waldman would clearly recognize that "there are a number of values that could be at the center of privacy by design, ranging from enhancing user control to protecting *justice, fairness, and equality*" (A. Waldman, 2019, p. 1242), and suggest legislators to follow a products liability paradigm in order to prioritize the latter. And for Ifeoma Ajunwa, one of the main reasons to hold liable employers and makers of algorithmic hiring systems for employment discrimination should be to honor the "*societal goal of equality* and the spirit of antidiscrimination laws meant to accomplish that goal" (2020, p. 1681).

Therefore, the envisioned society is one that makes a special effort to protect marginalized groups, including minorities (e.g., racial, religious, sexual, etc.) and socioeconomically vulnerable individuals. As Dennis Hirsch would categorically express in 2020, "[i]f society is to protect people in the era of predictive analytics, it needs a new strategy grounded in *social protection* rather than individual control" (2020, p. 443). But protect them from what? Mainly, from public

and private surveillance regimes, discriminatory decision-making systems, and "situations where they are unable to keep information private ex ante" (Skinner-Thompson, 2020, p. 128).

How so? By avoiding hidden normative ends and masked power embedded in data-driven systems. Likewise, by ensuring that all individuals, regardless of gender, race, nationality, sexual orientation, age, membership in a particular group or affiliation, "have an equal chance to obtain and keep jobs, to secure affordable insurance, to find housing, and to pursue other crucial life opportunities" (D. Solove & Citron, 2022, p. 855) without being affected by unfair automated decisions.

Finally, this envisioned society holds corporate power accountable. Within it, "*the law needs to assert authority over powerful information economy actors and* relieve individuals of an impossible task—securing illusory control over their privacy one website at a time" (A. E. Waldman, 2022a, p. 105). In practice, this future entails either radical measures to tear down the informational capitalism model, or more moderate interventions such as "set[ting] boundaries and goals for technological design" (Hartzog, 2018b, p. 7); "giv[ing] advocacy organizations representing marginalized populations, and not corporations, a seat at the table" (Waldman, 2022b, p. 1277); making sure that "workers and worker interests are more a part of the conversation from the very beginning, (…) [s]o that when a technology is being implemented, it's not just being implemented from the perspective of, "what can this do for the employer? How can this help us reduce our costs?" (P. T. Kim, oral history interview, November 30, 2023); and "advancing the political status of marginalized populations and others, by critically assessing, from a power and political perspective, the rationale behind disqualifying certain definitions of privacy and validating others" (A. L. Allen, oral history interview, March 30, 2023).

***

As this Chapter has aimed to demonstrate, cognitive factors—American privacy law scholars' techno-legal imaginaries—may have played a role in the development of the algorithmic turn experienced by the concept of privacy used in the sample of American privacy law scholarship examined here. Specifically, a transformation in scholars' techno-legal imaginations may have paved the way for the transformation of legal tools proposed by scholars over the years to protect privacy. Or, more concretely, for the transition from supporting FIPs-based legislative interventions to pushing for a batch of hands-on tools directed at taking power away from corporations.

Thus, while the FIPs-based legislative approach promoted during the 1990s and early 2000s was underpinned by the vision of a pluralistic, free, democratic society in which autonomous individuals thrive, the package of hands-on tools was nested in a vision of a socially-just society in which tech corporate power is held accountable and vulnerable populations are protected.

To be sure, as it was pointed out since the Introduction, by offering this additional factor I am not assuming that the transformation in American privacy law scholars' techno-legal imaginaries was the *principal* or *only possible driver* of privacy's algorithmic turn. Rather, following prior legal scholarship on the Legal Construction of Technology, I contend that privacy's algorithmic turn is a sociotechnical phenomenon, resulting from a complex and multi-way relationship between social, technical, legal, and—as I hope to have shown here—cognitive factors.

# CONCLUSION

## A. Summing up

In this dissertation I aimed to answer the following two research questions: (1) How did privacy's algorithmic turn actually happen? and (2) What can American privacy law scholars' aspirations, expectations, and visions about the future further tell us about this turn? For doing so, I have drawn upon Intellectual History's discursive context of thought approach (Hollinger, 1985) to trace, in detail, the evolution of the concept of information privacy in the portion of American privacy law scholarship examined here. Likewise, I have built on Science & Technology Studies ("STS") literature on "imaginaries" as well as on interdisciplinary scholarship where this concept has been applied to legal endeavors, to propose the theoretical concept of 'techno-legal imaginaries" and apply it to the case of the American privacy law scholars here examined.

By conducting document analysis of 574 law review articles written between 1990 and 2020, as well as fifteen oral history interviews with a purposely drawn representative sample of privacy law scholars, and analyzing the collected information through a Ground Theory approach, in this dissertation I sought to accomplish two goals.

First, and in response to my first research question, in this dissertation I tell the intellectual history (Chapters II to V) of how, over the past thirty years, the community of privacy scholars that has developed *around* PLSC transitioned from focusing primarily on autonomy-based harms to raising a vast array of harms that share the following three characteristics: being *objective*, originating from the *actual processing phase* of the data cycle, and having *architectural* effects. In the process, scholars shifted twice from states of regulatory innovation and flux (uncertainty about what the best regulatory approach would be) to those of relative convergence regarding the

preferred techniques to protect information privacy. Thus, while between 2000 and 2007 scholars almost unanimously supported the binding implementation of the Fair Information Practices ("FIPs") principles in order to *empower individuals*, by the end of the third studied decade scholars seemed to be coalescing around a hands-on set of substantive requirements, duties, and prohibitions intended to *take power away from corporations*.

Second, and in response to my second research question, here I demonstrate that the transformation of the scholars' techno-legal imaginaries over the period of time covered by this study (1990-2020) can provide us with some insight into the second feature of privacy's algorithmic turn, namely, the transformation of the tools proposed by scholars to protect information privacy. In particular, I have looked to show how, by understanding the scholars' techno-legal imaginaries and their transformation over time, we are better able to comprehend why some privacy scholars would end up abandoning the legal implementation of the FIPs principles in favor of a batch of hands-on tools directed to intervene the companies' data-extractive business models, the practices of system design, the corporate structure and business incentives, and even data externalities.

With this last task, this research builds upon Margot Kaminski & Meg Leta Jones's new conceptualization of the Legal Construction of Technology method (now nested in co-production) (2024), presenting privacy's algorithmic turn as a complex sociotechnical phenomenon, and placing it within a broader context where technological, social, legal, and—as I hope to have demonstrated here—cognitive elements interact and become entangled.

## B. Future research

To conclude this dissertation, I would like to suggest some possible directions for future research that build on the work that has already been completed here. At least four possible research avenues loom on the horizon.

First, the theoretical concept of "techno-legal imaginaries" here proposed can be used in the future to study the imaginaries of other legal actors (e.g., Congress; Public servants at the Executive Branch involved in AI governance). Second, another possible future research project can look to investigate whether the newly generated theory of privacy's algorithmic turn can be also traced in the intellectual history of other legal communities (e.g., FTC). In third place, the research methodology already designed for this dissertation could be used by myself or others in the future to trace the evolution of the concept of information privacy in other type of privacy-related scholarship (e.g., on the Fourth Amendment and government surveillance).

Finally, using the oral histories collected for this research project, as well as the information provided in Chapter I as a starting point, other researchers could conduct an ethnographic study of the Privacy Law Scholars Conference ("PLSC"). As a way of inspiring the development of this future project, there would be no better way to conclude this dissertation than by sharing the following quote from Paul Schwartz's oral history interview:

> Joel [Reidenberg] and I were once at the Privacy Law Scholars Conference. This was before the pandemic hit, maybe like 2018, 2017. The event was at Berkeley that year. We were in the main room for breakfast, it was packed, there were hundreds of people in there. And Joel looked at me and said, "Paul, do you remember when there were four privacy scholars in the United States, and we were two of them?" It was a wonderful feeling to look out and to see this field thriving, with so much interesting work being done, and so much energy, and people who were helping each other and promoting each other's work, and were interested in open discussion. (oral history interview, March 29, 2023)

Having avoided the attempt to conduct an ethnography of the conference here, I hope the present dissertation will make some contribution to understanding the intellectual development of this thriving community.

## References


*2018 Privacy Law Scholars Conference (PLSC2018)*. (N.D.). Berkeley Law. Retrieved April 2, 2024, From Https://Www.Law.Berkeley.Edu/Research/Bclt/Bcltevents/2018annual-Privacy-Law-Scholars-Conference/

*2020 Privacy Law Scholars Conference (PLSC 2020)*. (N.D.). Berkeley Law. Retrieved April 3, 2024, From Https://Www.Law.Berkeley.Edu/Research/Bclt/Bcltevents/2020-Privacy-Law-Scholars-Conference/

Abrams, L. (2016). *Oral History Theory*. Routledge Book.

Ajunwa, I. (2020). The Paradox of Automation as Anti-Bias Intervention. *Cardozo Law Review, 41*, 1671–1742.

Ajunwa, I. (2021). An Auditing Imperative for Automated Hiring Systems. *Harvard Journal of Law & Technology, 34*(2), 1–80.

Ajunwa, I., Crawford, K., & Schultz, J. (2017). Limitless Worker Surveillance. *California Law Review, 105*, 735–776.

Allen, A. L. (2000). Privacy-as-data control: Conceptual, practical, and moral limits of the paradigm. *Connecticut Law Review, 32*(3), 861.

Allen, A. L. (2001). Minor Distractions: Children, Privacy and E-Commerce. *Houston Law Review, 38*, 751–776.

Allen, A. L. (2003). Privacy Isn't Everything: Accountability as a Personal and Social Good. *Alabama Law Review, 54*(4), 1375–1391.

Allen, A.L. (2005). Privacy. In Hugh LaFollette (ed). *The Oxford handbook of practical ethics* (Oxford handbooks). Oxford; New York: Oxford University Press.

Allen, A. L. (2021). Dismantling The "Black Opticon": Privacy, Race, Equity, And Online Data-Protection Reform. *The Yale Law Journal, 131*. Https://Www.Yalelawjournal.Org/Forum/Dismantling-The-Black-Opticon

Allen, A. L. (2022). Privacy in Critical Definition and Racial Justice. In *Oxford Handbook of Applied Philosophy of Language*.

Allen, A. L. (2023, March 30). *Oral History Interview for The Intellectual History of American Privacy Law Scholarship Project* [Oral history interview].

Allen, A. L. (1999a). Coercing Privacy. *WILLIAM AND MARY LAW REVIEW, 40*(3), 723–757.

Allen, A. L. (2000b). Gender And Privacy in Cyberspace. *STANFORD LAW REVIEW, 52*(5), 1175–1200.

Allen, A. L. (1999b). Lying To Protect Privacy. *Villanova Law Review, 44*(2), 161–187.

Altman, M., Cohen, A., Nissim, K., & Wood, A. (2020). What A Hybrid Legal-Technical Analysis Teaches Us About Privacy Regulation: The Case of Singling Out. *Boston University Journal of Science & Technology Law*, 27(1), 1-63.

Alvial-Palavicino, C. & Konrad, K. (2018). The Rise of Graphene Expectations: Anticipatory Practices in Emergent Nanotechnologies. *Futures* 109: 192-202.

Anderson, B. (1983). *Imagined Communities: Reflections on the Origin and Spread of Nationalism.* London: Verso.

Angel, M. P. (2024). Privacy's Algorithmic Turn. *Boston University Journal of Science & Technology Law, 30(1).*

Angel, M. P., & Calo, R. (2024). Distinguishing Privacy Law: A Critique of Privacy as Social Taxonomy. *Columbia Law Review, 124*, 507–562.

Ayres, I., & Braithwaite, J. (1992). *Responsive Regulation: Transcending The Deregulation Debate*. Oxford University Press.

Baker, C. E. (2004). Autonomy And Informational Privacy, Or Gossip: The Central Meaning of The First Amendment. *Social Philosophy and Policy*, *21*(2), 215–268.

Balkin, J. (2015). The Path of Robotics Law. *California Law Review 6*, 45-60.

Balkin, J., & Siegel, R. B. (2006). Principles, Practices, And Social Movements. *University Of Pennsylvania Law Review 154*, 927-950.

Bambauer, D. E. (2014). Exposed. *Minnesota Law Review*, *98*(6), 2025–2102.

Bambauer, J. R., Zarsky, T., & Mayer, J. (2022). When A Small Change Makes A Big Difference: Algorithmic Fairness Among Similar Individuals. *University Of California, Davis*, *55*, 2337–2419.

Bambauer, J., & Zarsky, T. (2018). The Algorithm Game. *Notre Dame Law Review*, *94*(1), 1–47.

Bamberger, K. A., & Mulligan, D. K. (2011). Privacy on the Books and on the Ground. *Stanford Law Review*, *63*(2), 247–316.

Bamberger, K. A., & Mulligan, D. K. (2013). Privacy In Europe: Initial Data on Governance Choices and Corporate Practices. *The George Washington Law Review*, *81*, 1529–1664.

Barbas, S. (2015). *Laws of Image: Privacy and Publicity in America*. Palo Alto: Stanford University Press.

Bareis, J., & Katzenbach, C. (2021). Talking AI Into Being: The Narratives and Imaginaries of National AI Strategies and Their Performative Politics. *Science, Technology, & Human Values*, *46*(5), 855–881.

Barnes, W. R. (2006). Rethinking Spyware: Questioning The Propriety of Contractual Consent to Online Surveillance. *U.C. Davis Law Review*, *39*(4), 1545–1620.

Barocas, S., & Levy, K. (2020). Privacy Dependencies. *Washington Law Review*, *95*, 555–616.

Barocas, S., & Selbst, A. D. (2016). Big Data's Disparate Impact. *California Law Review*, *104*, 671–732.

Barrett, L. (2018). Model(Ing) Privacy: Empirical Approaches To Privacy Law & Governance. *Santa Clara High Technology Law Journal*, *35*, 1–64.

Bartow, A. (2000). Our Date, Ourselves: Privacy, Propertization, and Gender. *University Of San Francisco Law Review*, *34*(4), 633–704.

Baxi, S. N., & Nickel, A. A. (1994). Big Brother or Better Business: Striking a Balance in the Workplace. *Kansas Journal of Law & Public Policy*, *4*(1), 137–150.

Beckmann, R. A. (2001). Privacy Policies and Empty Promises: Closing The "Toysmart Loophole." *University Of Pittsburgh Law Review*, *62*(4), 765–792.

Bellovin, S. M., Dutta, P. K., & Reitinger, N. (2019). Privacy and Synthetic Datasets. *Stanford Technology Law Review*, *22*, 1–51.

Bennett, C. J., & Raab, C. D. (2006). The Governance of Privacy Policy Instruments in Global Perspective. The MIT Press.

Bennett, C. J., & Raab, C. D. (2020). Revisiting The Governance of Privacy: Contemporary Policy Instruments in Global Perspective. *Regulation & Governance*, *14*(3), 447–464.

Benthall, S., & Viljoen, S. (2021). Data Market Discipline: From Financial Regulation to Data Governance. *Journal of International and Comparative Law*, *8(2)*, 459–486.

Berman, J., & Mulligan, D. (1999). Privacy In the Digital Age: Work in Progress. *Nova Law Review*, *23*(2), 551–584.

Bernstein, G. (2006b). The Paradoxes of Technological Diffusion: Genetic Discrimination and Internet Privacy. *Connecticut Law Review*, *39*(1), 243–297.

Bernstein, G. (2006a). When New Technologies Are Still New: Windows of Opportunity for Privacy Protection. *Villanova Law Review*, *51*(4), 921–950.

Bezanson, R. P. (1992). The Right to Privacy Revisited: Privacy, News, And Social Change. *California Law Review*, *80*(5), 1133–1176.

Bhatia, J., & Breaux, T. D. (2018). Empirical Measurement of Perceived Privacy Risk. *ACM Transactions on Computer-Human Interaction*, *25*(6), 1–47.

Bibas, S. (1994). A Contractual Approach to Data Privacy. *Harvard Journal of Law & Public Policy*, *17*(2), 591–611.

Bietti, E. (2023). A Genealogy of Digital Platform Regulation. *Georgetown Law Technology Review*, *7*, 1–68.

Bijker, W. E. (1994). Sociohistorical technology studies. In *Handbook of Science and Technology Studies* (pp. 229-256). SAGE.

Bijker, W. (1997). *Of bicycles, bakelites, and bulbs: Toward a theory of sociotechnical change*. Cambridge: MIT Press.

Bignami, F. (2005). Transgovernmental Networks Vs. Democracy: The Case of The European Information Privacy Network. *Michigan Journal of International Law*, *26*(3), 807–868.

Bindler, S. E. (1992). Peek And Spy: A Proposal for Federal Regulation of Electronic Monitoring in the Work Place. *Washington University Law Quarterly*, *70*, 853–885.

Birnhack, M. (2019). A Process-Based Approach to Informational Privacy and the Case of Big Medical Data. *Theoretical Inquiries in Law*, *20*(1), 257–290.

Birnhack, M., Toch, E., & Hadar, I. (2014). Privacy Mindset, Technological Mindset. *Jurimetrics*, *55*, 55–114.

Blanchette, J.-F., & Johnson, D. G. (2002). Data Retention and The Panoptic Society: The Social Benefits of Forgetfulness. *The Information Society*, *18*(1), 33–45.

Blanke, J. M. (2000). "Safe Harbor" and the European Union's Directive on Data Protection. *Albany Law Journal of Science & Technology*, *11*(1), 57–88.

Bodie, M. T. (2022). The Law of Employee Data: Privacy, Property, Governance. *Indiana Law Journal*, *97*(2), 707–754.

Boehmer, R. G. (1992). Artificial Monitoring and Surveillance of Employees: The Fine Line Dividing the Prudently Managed Enterprise Form the Modern Sweatshop. *DePaul Law Review*, *41*(3), 739–820.

Borup, M., Brown, N., Konrad, K. & Van Lente, H. (2006). The Sociology of Expectations in Science and Technology. *Technology Analysis and Strategic Management* 18: 285–298.

Bowers, S. L. (2006). Privacy and Library Records. *The Journal of Academic Librarianship*, *32*(4), 377–383.

Boyd, d., Levy, K., & Marwick, A. (2014). *The Networked Nature of Algorithmic Discrimination*. New America - Open Technology Institute.

Boyd, d., & Marwick, A. (2011). Social Privacy in Networked Publics: Teens' Attitudes, Practices, And Strategies. *Paper To Be Presented at Oxford Internet Institute's "A Decade in Internet Time: Symposium On The Dynamics Of The Internet And Society."*

Brandimarte, L., College, H., Acquisti, A., College, H., & Gino, F. (2013). Of Revelations and Iron Hands: Unexpected Effects of Sensitive Disclosures. In *Advances in Consumer Research* (Vol. 41). Association For Consumer Research.

Branscomb, A. W. (1995). Anonymity, Autonomy, And Accountability: Challenges to The First Amendment in Cyberspaces. *The Yale Law Journal*, *104*(7), 1639–1679.

Brayne, S., Lageson, S., & Levy, K. (2023). Surveillance Deputies: When Ordinary People Surveil for The State. *Law & Society Review*, *57*(4), 462–488.

Brennan-Marquez, K., & Henderson, S. E. (2019). Artificial Intelligence and Role-Reversible Judgment. *Journal Of Criminal Law and Criminology*, *109*(2), 137–164.

Brensinger, J. (2023). Identity Theft, Trust Breaches, And the Production of Economic Insecurity. *American Sociological Review*, *88*(5), 844–871.

Bresnahan, J. (2000). Personalization, Privacy, And the First Amendment: A Look at The Law and Policy Behind Electronic Databases. *Virginia Journal of Law & Technology*, *5*(3), 1–30.

Brito, J. (2004). Relax, Don't Do It: Why RFID Privacy Concerns Are Exaggerated and Legislation Is Premature. *UCLA Journal of Law and Technology*, *8*(2), 1–42.

Bronfman, J. (2015). Weathering The Nest: Privacy Implications of Home Monitoring for The Aging American Population. *Duke Law & Technology Review*, *14*, 192-226.

Brooks, K. (2020). An Intellectual History of Comparative Tax Law. *Alberta Law Review*, *57*(3).

Brown, N., & Michael, M. (2003). A Sociology of Expectations: Retrospecting Prospects and Prospecting Retrospects. *Technology Analysis & Strategic Management* 15(1): 3–18.

Bruening, P. J., & Culnan, M. J. (2016). Through A Glass Darkly: From Privacy Notices to Effective Transparency. *North Carolina Journal of Law and Technology*, *17*(4), 515–579.

BW/Harris Poll: Online Insecurity. (1998, March 16). *Business Week*.

Byers, S. J. (2007). Untangling The World Wide Weblog: A Proposal For Blogging, Employment-At-Will, And Lifestyle Discrimination Statutes. *Valparaiso University Law Review*, *42*(1), 245–290.

*Call For Abstracts: Privacy Law Scholars Conference 2024*. (N.D.). Retrieved April 3, 2024, From Https://Privacyscholars.Org/Plsc-2024/

Callon, M. (1980). Struggles and Negotiations to Define What is Problematic and What is Not. In *The Social Process of Scientific Investigation* (Sociology of the Sciences A Yearbook, pp. 197-219). Dordrecht: Springer Netherlands.

Callon, M. (1986). Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of Saint-Brieuc Bay. In Jhon Law (Ed.), *Power, Action and Belief: a new Sociology of Knowledge? Sociological Review Monograph* (pp. 196-233). London: Routledge and Kegan Paul.

Callon, M. (1990). Techno-economic Networks and Irreversibility. *The Sociological Review (Keele)*, *38*(1_suppl), 132-161.

Calo, R. (2010). People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship. *A New Frontier*, 1–48.

Calo, R. (2011a). The Boundaries of Privacy Harm. *Indiana Law Journal*, *86*(3), 1141–1162.

Calo, R. (2011b). The Drone as Privacy Catalyst, *Stanford Law Review Online*, *64*, 29–33.

Calo, R. (2014). Digital Market Manipulation. *The George Washington Law Review*, *82*, 995–1051.

Calo, R. (2015). Privacy And Markets: A Love Story. *Notre Dame Law Review*, *91*(2), 649–690.

Calo, R. (2016). Robots in American Law. *University Of Washington School of Law Research Paper* No. 2016-04.

Calo, R., & Citron, D. K. (2021). The Automated Administrative State: A Crisis of Legitimacy. *Emory Law Journal*, *70*, 797–845.
Calo, R., & Rosenblat, A. (2017). The Taking Economy: Uber, Information, And Power. *Columbia Law Review*, *117*, 1623–1690.
Cappello, L. (2019). *None of Your Damn Business. Privacy in the United States from the Gilded Age to the Digital Age.* The University of Chicago Press.
Casilli, A. A. (2015). *Four Theses on Digital Mass Surveillance and The Negotiation of Privacy* [Draft Available Online].
Cate, F. H. (1999). The Changing Face of Privacy Protection in The European Union and The United States. *Indiana Law Review*, *33*(1), 173–232.
Cavico, F. J. (1993). Invasion Of Privacy in The Private Employment Sector: Tortious and Ethical Aspects. *Houston Law Review*, *30*(3), 1263–1346.
Chander, A. (2011). Youthful Indiscretion in An Internet Age. In S. Levmore & M. C. Nussbaum (Eds.), *The Offensive Internet: Speech, Privacy, And Reputation*. Harvard University Press.
Chander, A., Kaminski, M. E., & Mcgeveran, W. (2021). Catalyzing Privacy Law. *Minnesota Law Review*, 1733–1802.
Chang, A.-M., Kannan, P. K., & Whinston, A. B. (1999). The Economics of Freebies in Exchange for Consumer Information on The Internet: An Exploratory Study. *International Journal of Electronic Commerce*, *4*(1), 85–102.
Citron, D. K. (2007). Reservoirs Of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age. *Southern California La W Review*, *80*(2), 241–298.
Citron, D. K. (2008). Technological Due Process. *Washington University Law Review*, *85*(6), 1249–1314.
Citron, D. K. (2009). Cyber Civil Rights. *Boston University Law Review*, *89*(1), 61–126.
Citron, D. K. (2014). Digital Hate. In *Hate Crimes in Cyberspace*. Harvard University Press.
Citron, D. K., & Pasquale, F. (2014). The Scored Society: Due Process for Automated Predictions. *Washington Law Review*, *89*, 1–33.
Clearwater, A. & Hughes, J. T. (2013). The Second Wave of Global Privacy Protection: In the Beginning ... An Early History of the Privacy Profession. *Ohio State Law Journal*, *74*(6), 897–921.
Cockburn, J., & Green, T.A. (1988). *Twelve good men and true: The criminal trial jury in England, 1200-1800*. Princeton, NJ: Princeton University Press.
Coen, R., Paul, E., Vanegas, P., Lange, A., & Hans, G. S. (2016). *A User--Centered Perspective on Algorithmic Personalization* [Master of Information Management and Systems: Final Project].
Cofone, I. N. (2017). The Way the Cookie Crumbles: Online Tracking Meets Behavioural Economics. *International Journal of Law and Information Technology*, *25*, 38–62.
Cofone, I. N. (2019). Antidiscriminatory Privacy. *SMU Law Review*, *72*, 139–176.

Cofone, I. N. (2022). Privacy Standing. *University of Illinois Law Review*, *2022*(4), 1367-1416 (2022).
Cofone, I.N. & Robertson, A. Z. (2018). Privacy Harms. *The Hastings Law Journal, 69*(4), 1039-1098.
Cofone, I. N., & Strandburg, K. J. (2019). Strategic Games and Algorithmic Secrecy. *Mcgill Law Journal*, *64*(4), 623–663.

Cohen, J. E. (1996). A Right to Read Anonymously: A Closer Look At "Copyright Management" In Cyberspace. *Connecticut Law Review*, *28*(4), 981–1040.
Cohen, J. E. (2000). Examined Lives: Informational Privacy and The Subject as Object. *Stanford Law Review*, *52*(5), 1373–1438.
Cohen, J. E. (2001). Privacy, Ideology, And Technology: A Response to Jeffrey Rosen. *The Georgetown Law Journal*, *89*, 2029–2045.
Cohen, J. E. (2002). Overcoming Property: Does Copyright Trump Privacy? *University Of Illinois Journal of Law, Technology & Policy*, *2002*(2), 375–384.
Cohen, J. E. (2003). DRM And Privacy. *Berkeley Technology Law Journal*, *18*(2), 575–618.
Cohen, J. E. (2013). What Privacy Is For. *Harvard Law Review*, *126*(7), 1904–1933.
Cohen, J. E. (2016). The Surveillance–Innovation Complex. The Irony of The Participatory Turn. In D. Barney, G. Coleman, C. Ross, J. Sterne, & T. Tembeck (Eds.), *The Participatory Condition in The Digital Age*. University Of Minnesota Press.
Cohen, D. (2017). *Family Secrets: Shame and Privacy in Modern Britain*. Oxford University Press.
Cohen, J. E. (2019a). *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford University Press.
Cohen, J. E. (2019b). Turning Privacy Inside Out. *Theoretical Inquiries in Law*, *20*(1), 1–32.
Cohen, J. E. (2023, February 27). *Oral History Interview for The Intellectual History of American Privacy Law Scholarship Project* [Oral history interview].
Cohen, J. E., & Waldman, A. E. (2023). Introduction: Framing Regulatory Managerialism as an Object of Study and Strategic Displacement. *Law And Contemporary Problems*, *86*(3), I–Xx.
Conlon, K. J. (1996). Privacy in the Workplace. *Chicago-Kent Law Review*, *72*, 285–296.
Court, L., & Warmington, C. (2004). Employment and Labor Law. *Oklahoma City University Law Review*, *29*(1), 15–40.
Cranor, L. F., Leon, P. G., & Ur, B. (2016). A Large-Scale Evaluation of U.S. Financial Institutions' Standardized Privacy Notices. *ACM Transactions on The Web*, *10*(3), 1–33.
Crawford, K., & Schultz, J. (2014). Big Data and Due Process: Toward A Framework to Redress Predictive Privacy Harms. *Boston College Law Review*, *55*, 93–128.
Crisci, C. L. (2002). All The World Is Not a Stage: Finding A Right to Privacy in Existing and Proposed Legislation. *New York University Journal of Legislation and Public Policy*, *6*(1), 207–244.
Crootof, R., & Ard, B. (2021). Structuring Techlaw. *Harvard Journal of Law & Technology*, *34*(2).
Cuaresma, J. C. (2002). The Gramm-Leach-Bliley Act. *Berkeley Technology Law Journal*, *17*(1), 497-[Ii].
Cuijpers, D. C. (2007). ICT And Employer-Employee Power Dynamics: A Comparative Perspective of United States' and Netherlands' Workplace Privacy in Light of Information And Computer Technology Monitoring And Positioning Of Employees. *John Marshall Journal of Computer and Information Law*, *25*(1), 37–78.
Culnan, M. J. (2011). *Accountability As the Basis for Regulating Privacy: Can Information Security Regulations Inform Privacy Policy?* An earlier version of this paper was presented at the 2011 Privacy Law Scholars Conference, Berkeley, CA., June 2-3, 2011.
Culnan, M. J., & Bies, R. J. (2003). Consumer Privacy: Balancing Economic and Justice Considerations. *Journal Of Social Issues*, *59*(2), 323–342.

Daggett, L. M., & Huefner, D. S. (2001). Recognizing Schools' Legitimate Educational Interests: Rethinking FERPA's Approach to The Confidentiality of Student Discipline and Classroom Records. *American University Law Review*, *51*(1), 1–48.

Davies, S.G. (1998). Re-Engineering the Right to Privacy: How Privacy has Been Transformed from a Right to a Commodity, in Philip E. Agre & Marc Rotenberg, M. (eds.), *Technology and Privacy: The New Landscape*. The MIT Press.

Davis, K. E., & Marotta-Wurgler, F. (2019). Contracting For Personal Data. *New York University Law Review*, *94*, 662–705.

Debusseré, F. (2005). The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster? *International Journal of Law and Information Technology*, *13*(1), 70–97.

DeCew, J. W. (1997). Origins and History of Privacy, in *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Cornell University Press.

Desai, D. R., & Kroll, J. A. (2017). Trust But Verify: A Guide to Algorithms and The Law. *Harvard Journal of Law & Technology*, *31*(1), 1–64.

Despoja, N. S. (2007). A Brief Look at the History of Privacy. *AQ: Australian Quarterly*, *79*(3), 60-66.

Devries, W. T. (2003). Protecting Privacy in the Digital Age. *Berkeley Technology Law Journal*, *18*(1), 283–312.

Diggelmann, O., & Cleis, M. (2014). How the Right to Privacy Became a Human Right. *Human Rights Law Review*, *14*, 441–458.

Doshi-Velez, F., Kortz, M., Budish, R., Bavitz, C., Gershman, S. J., O'Brien, D., Shieber, S., Waldo, J., Weinberger, D., & Wood, A. (2017). *Accountability Of AI Under the Law: The Role of Explanation* [Working Paper]. Berkman Klein Center for Internet & Society.

Draper, N. (2014). *Reputation, Inc.: Assessing the industrialization of self-presentation and privacy in the digital era* (Doctoral dissertation). Retrieved from ProQuest.

Dreyfuss, R. C. (1999). Warren And Brandeis Redux: Finding (More) Privacy Protection in Intellectual Property Lore. *Stanford Technology Law Review*, *1999*.

Dwork, C., Kohli, N., & Mulligan, D. (2019). Differential Privacy in Practice: Expose Your Epsilons! *Journal Of Privacy and Confidentiality*, *9*(2).

Dwork, C., & Mulligan, D. K. (2013). It's Not Privacy, And It's Not Fair. *Stanford Technology Law Review Online*, *66*, 35–40.

Easterbrook, F. H. (1996). Cyberspace And the Law of the Horse. *The University of Chicago Legal Forum*, *1996*, 207–216.

Edwards, L., & Harbinja, E. (2013). Protecting Post-Mortem Privacy: Reconsidering The Privacy Interests of The Deceased in a Digital World. *Cardozo Arts & Entertainment*, *32*, 83-129.

Edwards, L., & Veale, M. (2017). Slave to the Algorithm? Why A "Right to an Explanation" is Probably not the Remedy You Are Looking For. *Duke Law & Technology Review*, *16*(1), 18–84.

Epstein, R. A. (1994). The Legal Regulation of Genetic Discrimination: Old Responses to New Technology. *Boston University Law Review*, *74*(1), 1023.

Errera, R. (2011). *On the Origins and Content of Article 9 of the Civil Code on the Right to Privacy.* Available at: http://www.rogererrera.fr/liberte_expression/docs/Article_9.pdf

Evans, L. (2007). Monitoring Technology in the American Workplace: Would Adopting English Privacy Standards Better Balance Employee Privacy and Productivity? *California Law Review*, *95*(4), 1115–1150.

Ezrahi, Y. (2012). *Imagined Democracies*. New York: Cambridge University Press.

Fan, M. D. (2011). Sex, Privacy and Public Health in a Casual Encounters Culture. *Davis Law Review*, *45*, 531–596.
Farmer, J. A. (2003). The Spector of Crypto-Anarchy: Regulating Anonymity-Protecting Peer-To-Peer Networks. *Fordham Law Review*, *72*, 725–784.
Fathaigh, R. Ã., Van Hoboken, J., & Van Eijk, N. (2019). Mobile Privacy and Business-To-Platform Dependencies: An Analysis of SEC Disclosures. *Journal Of Business & Technology Law*, *14*(1), 49–105.
Feld, B. C. (2016). My Life in Crime: An Intellectual History of the Juvenile Court. *Nevada Law Journal*, *17*(2), 299–330.
Fernandez, M. (2016). Aproximación Sinóptica a la Historia de la Intimidad en Occidente y su Protección Jurídica. *Revista de Filosofía Jurídica y Social*.
Fissell, B. (2016). Modern Critiques of Judicial Empathy: A Revised Intellectual History. *Michigan State Law Review*, *2016*(3), 817–852.
Flaherty, D. H. (1972). *Privacy in Colonial New England 1630-1776*. Charlottesville: University Press of Virginia.
Flanagan, J. A. (1994). Restricting Electronic Monitoring in The Private Workplace. *Duke Law Journal*, *43*(6), 1256–1281.
Fluitt, A., Cohen, A., Altman, M., Nissim, K., Viljoen, S., & Wood, A. (2019). Opinions · Data Protection's Composition Problem. *European Data Protection Law Review*, *5*(3), 285–292.
Ford, R. A. (2016). Unilateral Invasions of Privacy. *Notre Dame Law Review*, *91*(3), 1076–1115.
Ford, R. A. (2019). Data Scams. *Houston Law Review*, *57*(1), 111–183.
Ford, R. A., & Price II, W. N. (2016). Privacy And Accountability in Black-Box Medicine. *Michigan Telecommunications and Technology Law Review*, *23*(1), 1–43.
Franks, M. A. (2017). Democratic Surveillance. *Harvard Journal of Law & Technology*, *30*(2), 425–489.
Friedman, L. M. (2007). *Guarding Life's Dark Secrets: Legal and Social Controls over Reputation, Propriety, and Privacy*. Stanford University Press.
Friedman, A., & Hoffman, L. J. (2014). *The Internet Of (Whose) Things: Business Models, Computer Architectures, And Privacy* [Report GW-CSPRI 2014-3].
Frischmann, B., & Selinger, E. (2018). On Extending Minds and Mind Control. In *Re-Engineering Humanity* (Pp. 81–101).
Fromholz, J. M. (2000). The European Union Data Privacy. *Berkeley Technology Law Journal*, *15*(1), 461–484.
Froomkin, A. M. (1996a). Flood Control on The Information Ocean: Living with Anonymity, Digital Cash, And Distributed Databases. *Journal of Law and Commerce*, *15*(2), 395–507.
Froomkin, A. M. (1996b). The Essential Role of Trusted Third Parties in Electronic Commerce. *Oregon Law Review*, *75*, 49–115.
Froomkin, A. M. (2000a). The Constitution and Encryption Regulation: Do We Need A "New Privacy"? *Legislation And Public Policy*, *3*, 25–37.
Froomkin, A. M. (2000b). The Death of Privacy? *Stanford Law Review*, *52*(5), 1461–1544.
Froomkin, A. M. (2015). Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements. *University of Illinois Law Review*, *2015*, 1713–1790.
Froomkin, A. M. (2017). Lessons Learned Too Well: Anonymity in a Time of Surveillance. *Arizona Law Review*, *59*(1), 95–160.

Froomkin, A. M. (2023, September 21). *Oral History Interview for The Intellectual History of American Privacy Law Scholarship Project* [Oral history interview].
Gandy Jr, O. H. (2021). *The Panoptic Sort: A Political Economy of Personal Information* (Second Edition). Oxford University Press.
Gantt, L. O. N. (1995). An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace. *Harvard Journal of Law & Technology*, *8*(2), 345–425.
Garrie, D. B., & Wong, R. (2006). Demystifying Clickstream Data: A European and U.S. Perspective. *Emory International Law Review*, *20*(2), 563–590.
Garrow, D. J. (1994). *Liberty and sexuality: The right to privacy and the making of Roe v. Wade*. New York: Macmillan Publishing Company.
Gellman, R. (2003). A Better Way to Approach Privacy Policy in The United States: Establish A Non-Regulatory Privacy Protection Board. *Hastings Law Journal*, *54*(4), 1183–1226.
Gerards, J., & Zuiderveen Borgesius, F. (2022). Protected Grounds and The System of Non-Discrimination Law in the Context of Algorithmic Decision-Making And Artificial Intelligence. *Colorado Technology Law Journal*, *20*, 1–55.
Gibson, W. (1984). *Neuromancer*. Ace Books. Https://Www.Abebooks.Com/Book-Search/Title/Neuromancer/Author/Gibson-William/
Gilles, S. M. (1995). Promises Betrayed: Breach Of Confidence as a Remedy for Invasions of Privacy. *Buffalo Law Review*, *43*(1), 1–84.
Gillespie, T., Boczkowski, P.J., & Foot, K.A. (2013). Introduction. In *Media Technologies. Essays on Communication, Materiality, and Society* (pp. 1-19). MIT Press.
Gilman, M., & Green, R. (2018). The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization. *NYU Review of Law & Social Change*, *42*, 253–307.
Givens, B. (2000). Privacy Expectations in a High Tech World. *Santa Clara High Technology Law Journal*, *16*, 347–356.
Glasser, B. G., & Strauss, A. L. (1967). *The Discovery of Grounded Theory. Strategies for Qualitative Research*. Aldine Transaction.
Glancy, D. J. (1995). Privacy And Intelligent Transportation Technology. *Computer & High Technology Law Journal*, *11*(1), 151–203.
Glancy, D. J. (1979). The Invention of the Right to Privacy. *Arizona Law Review*, *21*(1), 1—39.
González Fuster, G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Springer.
Gordon, P.E. (2014). Contextualism and Criticism in the History of ideas. In Darrin M. McMahon & Samuel Moyn (Eds.), *Rethinking Modern European Intellectual History*. Oxford University Press.
Gormley, K. (1992). One Hundred Years of Privacy. *Wisconsin Law Review*, *1992*(5), 1335–1442.
Gostin, L. O. (1995). Health Information Privacy. *CORNELL LAW REVIEW*, *80*, 451–528.
Gostin, L. O., & Hodge Jr., J. G. (1999). Genetic Privacy and The Law: An End to Genetics Exceptionalism. *Jurimetrics*, *40*(1), 21–58.
Gostin, L. O., & Hodge, Jr., J. G. (2002). Personal Privacy and Common Goods: A Framework for Balancing Under The National Health Information Privacy Rule. *Minnesota Law Review*, *86*(6), 1439–1480.
Gostin, L. O., Jr, J. G. H., & Marks, L. (2002). The Nationalization of Health Information Privacy Protections. *Tort Trial & Insurance Practice Law Journal*, *37*, 1113–1138.

Gratton, E. (2014). If Personal Information Is Privacy's Gatekeeper, Then Risk of Harm Is the Key: A Proposed Method for Determining What Counts as Personal Information. *Journal Of Science and Technology*, *24*.

Green, C. (2008). An Intellectual History of Judicial Activism. *Emory Law Journal*, *58*(5), 1195–1264.

Green, R. (2020). Candidate Privacy. *Washington Law Review*, *95*, 205–257.

Greenberg, T. R. (1994). E-Mail and Voice Mail: Employee Privacy and The Federal Wiretap Statute. *American University Law Review*, *44*(1), 219–254.

Gürses, S., & Van Hoboken, J. (2017). Privacy After the Agile Turn. In J. Polonetsky, O. Tene, and E. Selinger (Eds.), *Cambridge Handbook of Consumer Privacy*.

Gupta, D. (2021, December 8). In-Store Tracking: Is It A Threat To Consumer Privacy? *Forbes*. https://www.forbes.com/sites/forbestechcouncil/2021/12/08/in-store-tracking-is-it-a-threat-to-consumer-privacy/?sh=26b165ea67b7

Habib, H., Zou, Y., Jannu, A., Sridhar, N., Swoopes, C., Acquisti, A., Cranor, L. F., Sadeh, N., & Schaub, F. (2019, August 12). An Empirical Analysis of Data Deletion and Opt-Out Choices On 150 Websites. *Proceedings of the Fifteenth Symposium on Usable Privacy and Security*. Fifteenth Symposium on Usable Privacy and Security, Santa Clara, CA, USA.

Hackney, J. R. Jr. (2014). Judge Jack Weinstein and the Construction of Tort Law in America: An Intellectual History. *DePaul Law Review*, *64*(2), 495–512.

Hafner, K., & Lyon, M. (1998). *Where Wizards Stay Up Late. The Origins of the Internet*.Touchstone.

Hahn, C. (2008). *Doing Qualitative Research Using Your Computer: A Practical Guide*. Sage Publications.

Han, C., Reyes, I., Bamberger, K. A., Egelman, S., & Vallina-Rodriguez, N. (2019). *Do You Get What You Pay For? Comparing The Privacy Behaviors of Free Vs. Paid Apps*. The Workshop on Technology and Consumer Protection (Conpro '19).

Hardy, T. (1994). The Proper Legal Regime for "Cyberspace." *University Of Pittsburgh Law Review*, *55*(4), 993–1056.

Harris, S. (2014). @War: The rise of the military-internet complex. Eamon Dolan.

Hartzog, W. (2009). Promises And Privacy: Promissory Estoppel and Confidential Disclosure in Online Communities. *Temple Law Review*, *82*(4), 891–928.

Hartzog, W. (2011). Website Design as Contract. *American University Law Review*, *60*, 1635–1671.

Hartzog, W. (2014). Reviving Implied Confidentiality. *Indiana Law Journal*, *89*, 763–806.

Hartzog, W. (2018a). Introduction: Designing Our Privacy Away. In *Privacy's Blueprint: The Battle to Control the Design of New Technologies*. Harvard University Press.

Hartzog, W. (2018b). The Case Against Idealising Control. *European Data Protection Law Review*, *4*, 423–432.

Hartzog, W. (2023, February 27). *Oral History Interview for The Intellectual History of American Privacy Law Scholarship Project* [Oral history interview].

Hartzog, W., & Richards, N. (2020). Privacy's Constitutional Moment and The Limits of Data Protection. *Boston College Law Review*, *61*(5), 1687–1761.

Hartzog, W., & Richards, N. M. (2022). The Surprising Virtues of Data Loyalty. *Emory Law Journal*, *71*, 985–1033.

Hartzog, W., & Solove, D. J. (2015). The Scope and Potential of FTC Data Protection. *George Washington Law Review*, *83*, 2030–2300.
Hartzog, W., & Stutzman, F. (2013b). Obscurity By Design. *Washington Law Review*, *88*, 385–418.
Hartzog, W., & Stutzman, F. D. (2013a). The Case for Online Obscurity. *California Law Review*, *101*(1), 1–49.
Harvard Law Review. (2020). The Intellectual History of Unjust Enrichment. *Harvard Law Review*, *133*(6).
Harvey, G. M. (1992). Confidentiality: A Measured Response to The Failure of Privacy. *University Of Pennsylvania Law Review*, *140*(6), 2385.
Haynes, A. W. (2007). Online Privacy Policies: Contracting Away Control Over Personal Information? *Penn State Law Review*, *111*(3), 587–624.
Hazel, S. H. (2021). Privacy Self-Help. *Berkeley Technology Law Journal*, *36*, 305–352.
Helberger, N., Borgesius, F. Z., & Reyna, A. (2017). The Perfect Match? A Closer Look at The Relationship Between Eu Consumer Law and Data Protection Law. *Common Market Law Review*, *54*(5), 1427–1465.
Herbert, W. A. (2006). No Direction Home: Will The Law Keep Pace with Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery. *I/S: Journal of Law and Policy for The Information Society*, *2*(2), 409–474.
Hetcher, S. (2001). Changing The Social Meaning of Privacy in Cyberspace. *Harvard Journal of Law & Technology*, *15*(1), 149–206.
Hetcher, S. (2000b). The De Facto Federal Privacy Commission. *John Marshall Journal of Computer and Information Law*, *19*(1), 109–132.
Hetcher, S. (2000a). The FTC As Internet Privacy Norm Entrepreneur. *Vanderbilt Law Review*, *53*(6), 2041–2062.
Hildebrandt, M. & De Vries, K. (2013). Privacy, Due Process and the Computational Turn at a Glance. In M. Hildebrandt & K. De Vries (Eds.), *Privacy, Due Process and The Computational Turn*. Routledge Taylor & Francis Group.
Hildner, L. (2006). Defusing The Threat Of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at The State Level. *Harvard Civil Rights-Civil Liberties Law Review*, *41*(1), 133–176.
Hiller, J. S., & Blanke, J. M. (2017). Smart Cities, Big Data, And the Resilience of Privacy. *Hastings Law Journal*, *68*(2), 309–356.
Hirsch, D., Bartley, T., Chandrasekaran, A., Parthasarathy, S., Turner, P., Norris, D., Lamont, K., & Drummond, C. (2019). *Corporate Data Ethics: Data Governance Transformations for The Age of Advanced Analytics And AI*. The Ohio State University Moritz College of Law. Program On Data and Governance.
Hirsch, D. D. (2006). Protecting The Inner Environment: What Privacy Regulation Can Learn from Environmental Law. *Georgia Law Review*, *41*(1), 1–64.
Hirsch, D. D. (2013). Going Dutch? Collaborative Dutch Privacy Regulation and the Lessons it Holds for U.S. Privacy Law. *Michigan State Law Review*, *2013*(1), 83–166.
Hirsch, D. D. (2014a). The Glass House Effect: Big Data, The New Oil, and the Power of Analogy. *Maine Law Review*, *66*(2), 373–395.
Hirsch, D. D. (2014b). That's Unfair! Or Is It? Big Data, Discrimination and The FTC's Unfairness Authority. *Kentucky Law Journal*, *103*, 345–362.

Hirsch, D. D. (2020). From Individual Control to Social Protection: New Paradigms for Privacy Law in The Age of Predictive Analytics. *Maryland Law Review*, *79*(2), 439–505.

Hodge Jr., J. G. (1999). The Intersection of Federal Health Information Privacy and State Administrative Law: The Protection of Individual Health Data and Workers' Compensation. *Administrative Law Review*, *51*(1), 117–144.

Hoepman, J.-H. (2014). Privacy Design Strategies. In N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam, & T. Sans (Eds.), *ICT Systems Security and Privacy Protection* (Vol. 428, Pp. 446–459). Springer Berlin Heidelberg.

Hoffman, S., & Podgurski, A. (2007). In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information. *Boston College Law Review*, *48*(2), 331–386.

Hollinger, D. A. (1985). *In The American Province: Studies in The History and Historiography of Ideas*. The Johns Hopkins University Press.

Hondius, E. (2010). Towards an Intellectual History of European Private Law. *European Review of Private Law*, *18*(6), 1051–1054.

Hong, S. (2007). Can Blogging and Employment Co-Exist? *University Of San Francisco Law Review*, *41*(3), 445–476.

Hoofnagle, C. J. (2004). Digital Rights Management: Many Technical Controls on Digital Content Distribution Can Create a Surveillance Society. *The Columbia Science and Technology Law Review*.

Hoofnagle, C. J. (2016). Strengthening The FTC And Protecting Privacy. In *Federal Trade Commission Privacy Law and Policy* (1st Ed.). Cambridge University Press.

Hoofnagle, C. J. (2023, September 8). *Oral History Interview for The Intellectual History of American Privacy Law Scholarship Project* [Oral history interview].

Hu, M. (2015). Big Data Blacklisting. *Florida Law Review*, *67*, 1735–1811.

Hu, M. (2017). Algorithmic Jim Crow. *Fordham Law Review*, *86*, 633–696.

Hughes, T. P. (1994). Technological momentum. In Merritt R. Smith and Leo Marx (Eds.*), Does Technology Drive History? The Dilemma of Technological Determinism* (pp. 101–114). MIT Press.

Hull, G. (2021). The Death of The Data Subject. *Law, Culture and The Humanities*, 1–21.

Hyman, D. A., & Kovacic, W. E. (2019). Implementing Privacy Policy: Who Should Do What? *Intellectual Property Media & Entertainment Law Journal*, *29*, 1117–1149.

Igo, S. E. (2015). The beginnings of the end of privacy. *The Hedgehog Review*, *17*(1), 18–29.

Igo, S. E. (2016). Toward a Free-Range Intellectual History. In James T. Kloppenberg, Joel Isaac, Michael O'Brien & Jennifer Ratner-Rosenhagen, *The Worlds of American Intellectual History*. Oxford: Oxford University Press, Incorporated.

Igo, S. E. (2018). *The Known Citizen: A History of Privacy in Modern America*. Harvard University Press.

Isajiw, P. J. (2001). Workplace E-Mail Privacy Concerns: Balancing the Personal Dignity of Employees with The Proprietary Interests of Employers. *Temple Environmental Law & Technology Journal*, *20*(1), 73–104.

IVHS America Legal Issues Committee. (N.D.). *"Strawman" Privacy Principles – Comment Form*.

Jamtgaard, L. (2000). Big Bird Meets Big Brother: A Look at The Children's Online Privacy Protection Act. *Santa Clara Computer and High-Technology Law Journal*, *16*(2), 385–400.

Janger, E. J., & Schwartz, P. M. (2002). The Gramm-Leach-Bliley Act, Information Privacy, And the Limits of Default Rules. *Minnesota Law Review.*, 1219–1262.

Jasanoff, S. (Ed.) (2004). *States of Knowledge: The Co-Production of Science and Social Order.* Routledge.

Jasanoff, S. (2004a). The idiom of co-production. In Sheila Jasanoff (Ed), *States of Knowledge*: *The Co-Production of Science and the Social Order* (pp.1-12). Taylor & Francis Group.

Jasanoff, S. (2004b). Ordering knowledge, ordering society. In Sheila Jasanoff (Ed), *States of Knowledge: The Co-Production of Science and the Social Order* (pp. 13-45). Taylor & Francis Group.

Jasanoff, S. (2015a). Future Imperfect: Science, Technology, And the Imaginations of Modernity. In Sheila Jasanoff & Sang-Hyun Kim (Eds.). *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power* (pp. 1-33). Chicago: University Of Chicago Press.

Jasanoff, S. (2015b). Imagined and Invented Worlds. In Sheila Jasanoff & Sang-Hyun Kim (Eds.). *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power* (pp. 321-341). Chicago: University of Chicago Press.

Jasanoff, S & Kim, S. (2009). Containing the Atom: Sociotechnical Imaginaries and Nuclear Power in The United States and South Korea. *Minerva* 47: 119–146.

Jasanoff, S & Kim, S. (Eds.). (2015). *Dreamscapes of Modernity: Sociotechnical Imaginaries and The Fabrication of Power.* Chicago: University Of Chicago Press.

Jenkins, R. V. (1975). Technology and the Market: George Eastman and the Origins of Mass Amateur Photography, *Technology & Culture, 16*(1), 1–19.

Jia, H., & Xu, H. (2016). Measuring Individuals' Concerns Over Collective Privacy on Social Networking Sites. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10*(1).

Johnson, D. R., & Post, D. (1996). Law And Borders: The Rise of Law in Cyberspace. *STANFORD LAW REVIEW*, *48*(5), 1367–1402.

Jones, M. L. (2015). Lessons From the Avalanche of Numbers: Big Data in Historical Perspective. *I/S: Journal of Law and Policy for The Information Society*, *11*(2), 201–278.

Jones, M. L. (2018). Does Technology Drive Law? The Dilemma of Technological Exceptionalism in Cyberlaw. *Journal Of Law, Technology & Policy* 2018(2): 249-284.

Jones, M. L. (2020). Cookies: A Legacy of Controversy, Internet Histories, Special Issue on Legacy Systems, 4(1), 87-104.

Jones, M. L. (2024-Forthcoming). *The Character of Consent: The History of Cookies and the Future of Technology Policy*. MIT Press.

Jones, M. L., Levy, K., & Kaufman, E. (2018). *Methods to Our Madness: An Interdisciplinary Reflection on 10 Years of Privacy Scholarship* (Draft). Not available online.

Jr, R. G. S. (1992). Privacy In German Employment Law. *Hastings International and Comparative Law Review*, *15*(2), 135–167.

Jurata Jr., J. A. (1999). The Tort That Refuses to Go Away: The Subtle Reemergence of Public Disclosure of Private Facts. *San Diego Law Review*, *36*(2), 489–546.

Kaminski, M. E. (2017). Authorship, Disrupted: AI Authors In Copyright and First Amendment Law. *U.C. Davis Law Review* 51(2): 589-616.

Kaminski, M. E. (2019). Binary Governance: Lessons From the GDPR's Approach to Algorithmic Accountability. *Southern California Law Review, 92*, 1529–1616.

Kaminski, M. E., & Witnov, S. (2015). The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech. *University Of Richmond Law Review*, *49*(2), 465–518.
Kaminski, M.E. (2021). Technological "Disruption" of the Law's Imagined Scene: Some Lessons from Lex Informatica. *Berkeley Technology Law Journal, 36*, 883-914.
Kaminski, M. E., & Jones, M. L. (2024). Constructing AI Speech. *The Yale Law Journal Forum*, *133*, 1212-1266.
Kang, J. (1998). Information Privacy in Cyberspace Transactions. *Stanford Law Review*, *50*(4), 1193–1294.
Kang, J., & Buchner, B. (2004). Privacy in Atlantis. *Harvard Journal of Law & Technology*, *18*(1), 229-[Ii].
Kang, J., Shilton, K., Estrin, D., & Burke, J. (2012). Self-Surveillance Privacy. *Iowa Law Review*, *97*(3), 809–848.
Kato Ku, A. (2005). Talk Is Cheap, But A Picture Is Worth a Thousand Words: Privacy Rights in the Era of Camera Phone Technology. *Santa Clara Law Review*, *45*, 679–706.
Katyal, S. K. (2004). Privacy Vs. Piracy. *Yale Journal of Law and Technology, 7*(1), 222–345.
Katyal, S. K. (2019). Private Accountability in the Age of Artificial Intelligence. *UCLA Law Review*, *66*, 54–141.
Kennedy, C., & Alderman, E. (1997). *The Right to Privacy*. New York: Alfred A. Knopf.
Keulen, S., & Kroeze, R. (2018). Privacy from a Historical Perspective. In Van der Sloot B. & De Groot A. (Eds.), *The Handbook of Privacy Studies: An Interdisciplinary Introduction* (pp. 21-56). Amsterdam: Amsterdam University Press.
Kloppenberg, J. T., Isaac, J. O'Brien, M., & Ratner-Rosenhagen, J. (2016). *The Worlds of American Intellectual History*. Oxford: Oxford University Press, Incorporated.
Kerr, I. (2013). Prediction, Pre-Emption, Presumption. In *Privacy, Due Process and The Computational Turn: The Philosophy of Law Meets the Philosophy of Technology*. Taylor & Francis Group.
Kerr, I. R. (2001). The Legal Relationship Between Online Service Providers and Users. *Canadian Business Law Journal*, *35*(3), 419–458.
Kerr, O. S., & Schneier, B. (2018). Encryption Workarounds. *The Georgetown Law Journal*, *106*, 989–1019.
Kesan, J. P. (2002). Cyber-Working Or Cyber-Shirking?: A First Principles Examination Of Electronic Privacy In The Workplace. *Florida Law Review*, *54*(2), 289–332.
Killingsworth, S. (1999). Minding Your Own Business: Privacy Policies in Principle and in Practice. *Journal Of Intellectual Property Law*, *7*(1), 57–98.
Kim, P. T. (1996). Privacy Rights, Public Policy, and the Employment Relationship. *Ohio State Law Journal*, *57*(3), 661–730.
Kim, P. T. (2002). Genetic Discrimination, Genetic Privacy. *Northwestern University Law Review*, *96*(4), 1497–1552.
Kim, P. T. (2017). Data-Driven Discrimination at Work. *William & Mary Law Review*, *58*, 857–936.
Kim, P. T. (2020). Manipulating Opportunity. *Virginia Law Review*, *106*, 867–935.
Kim, P. T. (2023, November 30). *Oral History Interview for The Intellectual History of American Privacy Law Scholarship Project* [Oral history interview].

King, D. N. (1994). Privacy Issues in The Private-Sector Workplace: Protection from Electronic Surveillance And The Emerging Privacy Gap. *Southern California Law Review*, *67*(2), 441–474.

King, J. (2012, July 11). *How Come I'm Allowing Strangers to Go Through My Phone? Smartphones And Privacy Expectations.* Symposium On Usable Privacy and Security (SOUPS) 2012, Washington, DC, USA.

King, J. (2015). *Understanding Privacy Decision- Making Using Social Exchange Theory*. CSCW, Vancouver, British Columbia, Canada.

Kirkland, A. (2006). "You Got Fired? On Your Day Off?!": Challenging Termination of Employees for Personal Blogging Practices. *Umkc Law Review*, *75*(2), 545–568.

Konrad, K., Van Lente, H., Groves, C., & Selin, C. (2016). Performing and Governing the Future in Science and Technology. In Ulrike Felt (Ed.), *The Handbook of Science and Technology Studies*. The MIT Press.

Konrad, K. & Böhle, K. (2019). Socio-Technical Futures and The Governance of Innovation Processes—An Introduction to the Special Issue. *Futures* 109: 101–107.

Koops, B.-J., & Leenes, R. (2005). "Code" and the Slow Erosion of Privacy. *Michigan Telecommunications & Technology Law Review*, *12*, 115–188.

Koops, B.-J., Newell, B. C., Roberts, A., Škorvánek, I., & Galič, M. (2018). The Reasonableness of Remaining Unobserved: A Comparative Analysis of Visual Surveillance and Voyeurism In Criminal Law. *Law & Social Inquiry*, *43*(04), 1210–1235.

Kreimer, S. F. (1991). Sunlight, Secrets, And Scarlet Letters: The Tension Between Privacy And Disclosure In Constitutional Law. *University Of Pennsylvania Law Review*, *140*(1), 1.

Kroll, J. A. (2018). The Fallacy of Inscrutability. *Philosophical Transactions Of The Royal Society A: Mathematical, Physical And Engineering Sciences*, *376*(2133), 20180084.

Lane, F. S. (2009). *American Privacy: The 400-year History of Our Most Contested Right*. Beacon Press.

Lange, F. (2012). Conference Report—The Intellectual History of International Law as a Research Field—Lauterpacht and beyond: Jewish/German Authorship and the History of International Law. *German Law Journal*, *13*(6), 793–808.

Latour, B. (1984). The Powers of Association. *The Sociological Review*, *32*(1_suppl), 264–280.

Latour, B. (1987). *Science in Action. How to Follow Scientists and Engineers through Society.* Cambridge: Harvard University Press.

Latour, B. (1992). Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts. In Wiebe E. Bijker and John Law (Eds.), *Shaping Technology/Building Society: Studies in Sociotechnical Change*. Cambridge: MIT Press.

Latour, B. (1996). On actor-network theory: A few clarifications. *Soziale Welt*, *47*(4), 369–381.

Latour, B. (1999). On Recalling Ant. *The Sociological Review*, *47*(1_suppl), 15–25.

Latour, B. (1999b). Factures/Fractures: From the Concept of Network to the Concept of Attachment. *Res: Anthropology and Aesthetics*, *36*, 20–31.

Latour, B. (2004). How to Talk About the Body? the Normative Dimension of Science Studies. *Body & Society*, *10*(2–3), 205–229.

Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory.* Oxford & New York: Oxford University Press.

Latour, B. (2009). A collective of humans and nonhumans: Following Daedalus's labyrinth. In D. M. Kaplan (Ed.), *Readings in the philosophy of technology*. Lanham: Rowman & Littlefield Publishers.

Latour, B. (2010). *The Making of Law. An ethnography of the Conseil D'Etat.* Cambridge: Polity Press.
Lauer, J. (2010). The good consumer: Credit Reporting and the invention of financial identity in the United States, 1840-1940. *Enterprise & Society, 11*, 686-694.
Lauer, J. (2012). Making the ledgers talk: Customer control and the origins of retail data mining, 1920-1940. In H. Berghoff, P. Scranton & U. Spiekermann (Eds.), *The rise of marketing and market research*. Palgrave Macmillan.
Law, J. (1992). Notes on the Theory of the Actor Network - Ordering, Strategy, and Heterogeneity. *Systems Practice, 5*(4), 379-393.
Law, J. (1994). *Organizing modernity*. Oxford, UK; Cambridge, Mass., USA: Blackwell.
Law, J. (2006). Traduction / Trahison: Notes on ANT. *Convergencia, 13*(42), 47-72.
Law, J. (2009). Actor network theory and material semiotics. In B. Turner (Ed.), *The New blackwell companion to social theory*. Chichester: John Wiley & Sons.
Leahy, C. P. (2021). The afterlife of interviews: explicit ethics and subtle ethics in sensitive or distressing qualitative research. *Qualitative Research, 00*(0), 1–18.
Lee, A. (2001). Editorial. *MIS Quarterly, 25*(1), iii-vii.
Lee, L. T. (1994). Watch Your E-Mail! Employee E-Mail Monitoring and Privacy Law in The Age of the "Electronic Sweatshop." *The John Marshalllaw Review*, *28*(1), 139–178.
Leebron, D. W. (1991). The Right to Privacy's Place in the Intellectual History of Tort. *Case Western Reserve Law Review, 41*, 769-809.
Lengwiler, M. (2004). *Privacy, justice and equality: The history of privacy legislation and its significance for civil society.* WZB Discussion Paper, No. SP IV 2004-503.
*Lepore*, J. (2013). *Privacy in an Age of Publicity.* The New Yorker. Retrieved January 30, 2021, from https://www.newyorker.com/magazine/2013/06/24/the-prism
Lessig, L. (1999). *Code And Other Laws of Cyberspace*. Basic Books.
Lessig, L. (1999a). The Architecture of Privacy: Remaking Privacy in Cyberspace. *Vanderbilt Journal of Entertainment and Technology Law, 1*, 56–65.
Lessig, L. (1999b). The Law of The Horse: What Cyberlaw Might Teach. *Harvard Law Review*, *113*(2), 501.
Lev-Aretz, Y. (2019). Data Philanthropy. *Hastings Law Journal*, *70*, 1491–1545.
Lev-Aretz, Y., & Strandburg, K. J. (2020). Privacy Regulation and Innovation Policy. *Yale Journal of Law and Technology*, *22*, 256–317.
Levin, A., & Nicholson, M. J. (2005). Privacy Law in the United States, The EU And Canada: The Allure of the Middle Ground. *University Of Ottawa Law & Technology Journal*, *2*(2), 357–395.
Levy, K. (2023, November 17). *Oral History Interview for the Intellectual History of American Privacy Law Scholarship Project* [Oral history interview].
Lewis, R. (2007). Employee E-Mail Privacy Still Unemployed: What the United States Can Learn from The United Kingdom. *Louisiana Law Review*, *67*(3), 959–990.
Lichtenstein, S. D., & Darrow, J. J. (2006). Employment Termination for Employee Blogging: Number One Tech Trend For 2005 And Beyond, Or A Recipe For Getting Dooced? *UCLA Journal of Law And Technology*, *10*(2), 1–49.
Lin, E. (2002). Prioritizing Privacy: Constitutional Response to The Internet. *Berkeley Technology Law Journal*, *17*(3), 1085–1154.
Lipton, J. D. (2012). Combating Cyber-Victimization. *Berkeley Technology Law Journal*, *26*(2), 1103–1155.

Litan, R. E. (2001). Law And Policy in The Age of The Internet. *Duke Law Journal*, *50*(4), 1045–1085.

Litman, J. (2000). Information Privacy/Information Property. *Stanford Law Review*, *52*(5), 1283–1314.

Long II, G. P. (1994). Who Are You: Identity And Anonymity in Cyberspace. *University Of Pittsburgh Law Review*, *55*(4), 1177–1214.

Louis Harris Assocs., & Westin, A. F. (1990). *The Equifax Report on Consumers in the Information Age*. Equifax, Inc.

Louis Harris Assocs., & Westin, A. F. (1995). *The Equifax-Harris Mid-Decade Survey on Consumer Privacy*. EQUIFAX, INC.

Luguri, J., & Strahilevitz, L. J. (2021). Shining A Light on Dark Patterns. *Journal of Legal Analysis*, *13*(1), 43–109.

Lyon, D. (1994). *The Electronic Eye: The Rise of Surveillance Society* (NED-New Edition). University Of Minnesota Press. Https://Www.Jstor.Org/Stable/10.5749/J.Ctttsqw8

Maccarthy, M. (2011). New Directions in Privacy: Disclosure, Unfairness and Externalities. *I/S: Journal of Law and Policy for the Information Society*, *6*(3), 426–512.

Maccarthy, M. (2017). Privacy Policy and Contextual Harm. *I/S: Journal of Law and Policy for The Information Society*, *13*(2), 309–463.

Maccarthy, M. (2021). Enhanced Privacy Duties for Dominant Technology Companies. *Rutgers Computer and Technology Law Journal*, *47*(1), 1–102.

MacKenzie, D. A., & Wajcman, J. (Eds.). (1985). *The Social Shaping of Technology* (1st. ed.). Open University Press.

Madden, M., Gilman, M., Levy, K., & Marwick, A. (2017). Privacy, Poverty, And Big Data: A Matrix of Vulnerabilities for Poor Americans. *Washington University Law Review*, *95*, 53–125.

Madejski, M., Johnson, M., & Bellovin, S. M. (2012). A Study of Privacy Settings Errors in an Online Social Network. *2012 IEEE International Conference on Pervasive Computing and Communications Workshops*, 340–345.

Marcus, George E. (Ed). 1995. *Technoscientific Imaginaries: Conversations, Profiles, And Memoirs*. Chicago: University Of Chicago Press.

Marotta, V., Zhang, K., & Acquisti, A. (2016). *The Welfare Impact of Targeted Advertising* [Working Paper].

Marshall, D. & Thomas, T. (2017). A Brief History of Privacy. In *Privacy and Criminal Justice* (pp. 13–38). Springer Nature eBooks.

Martin, J.P. (2014). Brief History of Privacy and Selected Electronic Surveillance Laws. In *Cloud Computing & Electronic Discovery* (pp. 37–53). Complementary Index.

Martin, K. (2015). Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice is Related to Meeting Privacy Expectations Online. *Journal Of Public Policy & Marketing*, *34*(2), 210–227.

Martin, K., & Nissenbaum, H. (2017). Privacy Interests in Public Records: An Empirical Investigation. *Harvard Journal of Law & Technology*, *31*(1), 111–143.

Martin, K., & Shilton, K. (2016). Why Experience Matters to Privacy: How Context-Based Experience Moderates Consumer Privacy Expectations for Mobile Applications. *Journal Of the Association for Information Science and Technology*, *67*(8), 1871–1882.

Marwick, A., Fontaine, C., & Boyd, d. (2017). "Nobody Sees It, Nobody Gets Mad": Social Media, Privacy, And Personal Responsibility Among Low-SES Youth. *Social Media + Society*, *3*(2).

Marx, G. T. (2015). Surveillance Studies. In *International Encyclopedia of the Social & Behavioral Sciences* (pp. 733–741). Elsevier.

Mathur, A., Mayer, J., & Kshirsagar, M. (2021). What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, And Measurement Methods. *Proceedings Of The 2021 CHI Conference on Human Factors in Computing Systems*, 1–18.

Matwyshyn, A. M. (2012). Generation C: Childhood, Code, And Creativity. *Notre Dame Law Review*, *87*(5), 1979–2030.

Matwyshyn, A. M. (2019). The Internet of Bodies. *William & Mary Law Review*, *61*, 77–167.

McAdam, J. (2011). An Intellectual History of Freedom of Movement in International Law: The Right to Leave as a Personal Liberty. *Melbourne Journal of International Law*, *12*(1), 27–56.

Mccartney, D. R. (1994). Electronic Surveillance and The Resulting Loss of Privacy in the Workplace. *UMKC Law Review*, *62*(4), 859–892.

Mcclurg, A. J. (1995). Bringing Privacy Law Out of the Closet: A Tort Theory Of Liability For Intrusions In Public Places. *North Carolina Law Review*, *73*(3), 989–1088.

Mcclurg, A. J. (2003). *A Thousand Words Are Worth a Picture: A Privacy Tort Response To Consumer Data Profiling*. *98*(1), 63–144.

Mcclurg, A. J. (2006). Kiss And Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality. *University Of Cincinnati Law Review*, *74*(3), 887–940.

McCullough, B. (2018). *How The Internet Happened. From Netscape to the Iphone*. Liveright Publishing Corporation.

Mcdonald, A. M., & Cranor, L. F. (2006). How Technology Drives Vehicular Privacy. *I/S: Journal of Law and Policy for the Information Society*, *2*(3), 981–1016.

Mcgeveran, W. (2001). Programmed Privacy Promises: P3P And Web Privacy Law. *New York University Law Review*, *76*, 1812–1854.

Mcgeveran, W. (2003). Mrs. Mcintyre's Checkbook: Privacy Costs of Political Contribution Disclosure. *University Of Pennsylvania Journal of Constitutional Law*, *6*(1), 1–55.

Mcgeveran, W. (2016). Friending The Privacy Regulators. *Arizona Law Review*, *58*, 959–1051.

Mcgeveran, W. (2019). The Duty of Data Security. *Minnesota Law Review*, *103*, 1135–1208.

Mckelvey, B. (2001). Financial Institutions' Duty of Confidentiality to Keep Cutomers' Personal Information Secure from the Threat of Identity Theft. *UC Davis Law Review*, *34*, 1077–1128.

Mckenna, A. T., Gaudion, A. C., & Evans, J. L. (2019). The Role of Satellites and Smart Devices: Data Surprises and Security, Privacy, And Regulatory Challenges. *Penn State Law Review*, *123*, 591–665.

McMahon, D. M., & Moyn, S. (2014). *Rethinking Modern European Intellectual History*. Oxford University Press.

Mcneil, M., Arribas-Ayllon, M., Haran, J., Mackenzie, A., & Tutton, R. (2016). Conceptualizing Imaginaries of Science, Technology, and Society. In Felt, U., Fouche, R., Miller, C. A., & Smith-Doerr, L. (Eds.), *The Handbook of Science and Technology Studies*. The MIT Press.

Meinel, F. (2007). Ernst Forsthaff and the Intellectual History of German Administrative Law Developments—Review Essay. *German Law Journal*, *8*(8), 785–800.

Micklitz, H.W. (2015). On the Intellectual History of Freedom of Contract and Regulation. *Penn State Journal of Law and International Affairs*, *4*(1), 1–32.
Miller, C. S., & Poe, B. D. (1996). Employment Law Implications in the Control and Monitoring of E-Mail Systems. *Business Law Journal*, *6*, 95–118.
Milligan, C. S. (1999). Facial Recognition Technology, Video Surveillance, And Privacy. *Southern California Interdisciplinary Law Journal*, *9*(1), 295–334.
Mir, D. J. (2021). Designing For the Privacy Commons. In M. R. Sanfilippo, B. M. Frischmann, & K. J. Strandburg (Eds.), *Governing Privacy in Knowledge Commons* (1st Ed., Pp. 245–267). Cambridge University Press.
Mir, D. J., Shvartzshnaider, Y., & Latonero, M. (2018). It Takes a Village: A Community Based Participatory Framework for Privacy Design. *2018 IEEE European Symposium on Security and Privacy Workshops (Euros&PW)*, 112–115.
Moore, B. (1984). *Privacy: Studies in social and cultural history*. M.E. Sharpe: Pantheon/Random House.
Moshell, R. (2005). And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection. *Texas Tech Law Review*, *37*(2), 357–432.
Mourey, J. A., & Waldman, A. E. (2018). Priming & Privacy: How Subtle Trust Cues Online. *NA - Advances in Consumer Research*, *46*.
Mulligan, D. K., Koopman, C., & Doty, N. (2016). Privacy is an Essentially Contested Concept: A Multi-Dimensional Analytic for Mapping Privacy. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *374*(2083), 20160118.
Murray, C. M. (2010). Hard Cases Make Good Law: The Intellectual History of Prior Acquittal Sentencing. *St. John's Law Review*, *84*(4), 1415–1476.
Murphy, R. S. (1996). Property Rights in Personal Information: An Economic Defense of Privacy. *Georgetown Law Journal*, *84*(7), 2381–2418.
Naeem M., & Ozuem W. (2022). Understanding Misinformation and Rumors that Generated Panic Buying as a Social Practice During COVID-19 Pandemic: Evidence from Twitter, Youtube And Focus Group Interviews. *Information Technology & People*, 35(7), 2140–2166.
Nehf, J. P. (2003). Recognizing The Societal Value in Information Privacy. *Washington Law Review*, *78*.
Nehf, J. P. (2005). Incomparability and the Passive Virtues of Ad Hoc Privacy Policy. *University Of Colorado Law Review*, *76*(1), 1–56.
Nelson, D. (2002). *Pursuing Privacy in Cold War America*. New York: Columbia University Press.
Newman, N. (2017). Reengineering Workplace Bargaining: How Big Data Drives Lower Wages and How Reframing Labor Law Can Restore Information Equality in The Workplace. *University Of Cincinnati Law Review*, *85*, 693–760.
Newhall, B. (1949). *The History of Photography: From 1839 to the Present Day*. Taschen.
Nguyen, X.-T. N. (2004). Collateralizing Privacy. *Tulane Law Review*, *78*(3), 553–604.
Nissenbaum, H. (1997). Toward An Approach to Privacy in Public: Challenges of Information Technology. *Ethics & Behavior*, *7*(3), 207–219.
Nissenbaum, H. (1998). Protecting Privacy in An Information Age: The Problem of Privacy in Public. *Law And Philosophy*, *17*(5–6), 559–596.
Nissenbaum, H. (2004). Privacy As Contextual Integrity. *Washington Law Review*, *79*.

Nissenbaum, H. (2009). *Privacy In Context: Technology, Policy, And the Integrity of Social Life*. Stanford University Press.
Nissenbaum, H. (2015). Respecting Context to Protect Privacy: Why Meaning Matters. *Science And Engineering Ethics*, *24*(3), 831–852.
Nissim, K., Bembenek, A., Wood, A., Bun, M., & Gasser, U. (2018). Bridging The Gap Between Computer Science and Legal Approaches to Privacy. *Harvard Journal of Law & Technology*, *31*(2), 687–780.
Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors. *Journal Of Consumer Affairs*, *41*(1), 100–126.
Ohm, P. (2010). Broken Promises of Privacy: Responding To The Surprising Failure Of Anonymization. *UCLA Law Review*, *57*, 1701–1777.
Ohm, P. (2013). Branding Privacy. *Minnesota Law Review*, *97*, 907–989.
Ohm, P. (2015). Sensitive Information. *Southern California Law Review*, *88*, 1125–1196.
Ohm, P. (2023, September 22). *Oral History Interview for The Intellectual History of American Privacy Law Scholarship Project* [Oral history interview].
Ohm, P., & Frankle, J. (2018). Desirable Inefficiency. *Florida Law Review*, *70*(4), 777–838.
Olivier, M. (2007). George Eastman's Modern Stone-Age Family: Snapshot Photography and the Brownie. Technology & Culture, 48(1), 1-19.
O'Mara, M. (2019). *The Code: Silicon Valley and the Remaking of America.* Penguin Random House.
Packin, N. G. (2020). Show Me The (Dataaboutthe) Money! *Utah Law Review*, *5*, 1277–1348.
Palmer, V. V. (2011). Three Milestones in the History of Privacy in the United States. *Tulane European and Civil Law Forum*, *26*, 67–98.
Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press. Https://Www.Jstor.Org/Stable/J.Ctt13x0hch
Paterson, M. (2018). Regulating Surveillance: Suggestions For a Possible Way Forward. *Canadian Journal of Comparative And Contemporary Law*, *4*(1), 1–37.
Patterson, H., & Nissenbaum, H. (2013). *Context-Dependent Expectations of Privacy In Self-Generated Mobile Health Data*. Privacy Law Scholars Conference (Plsc) 2013 Working Paper.
Peek, M. (2003). Passing Beyond Identity on the Internet: Espionage & Counterespionage In The Internet Age. *Vermont Law Review*, *28*(1), 91–120.
Peek, M. (2009). The Observer and The Observed: Re-Imagining Privacy Dichotomies In Information Privacy Law. *Northwestern Journal of Technology And Intellectual Property*, *8*(1), 51–66.
Penney, J. (2022). Understanding Chilling Effects. *Minnesota Law Review*, *106*(1451–1530).
Penney, J. W. (2017). Internet Surveillance, Regulation, And Chilling Effects Online: A Comparative Case Study. *Internet Policy Review*, *6*(2).
Peppet, S. R. (2012). Privacy & The Personal Prospectus: Should We Introduce Privacy Agents or Regulate Privacy Intermediaries. *Iowa Law Review Bulletin*, *97*, 77–93.
Perri, P., & Thaw, D. (2017). Ancient Worries and Modern Fears: Different Roots and Common Effects of U.S. And EU Privacy Regulation. *Connecticut Law Review*, *49*(5), 713–747.
Petkova, B. (2016). The Safeguards of Privacy Federalism. *Lewis & Clarck Law Review*, *20*(20), 595–645.
Phillips, D. J. (2003). Beyond Privacy: Confronting Locational Surveillance in Wireless Communication. *Communication Law and Policy*, *8*(1), 1–24.

Pinch, T. J. & Bijker, W. E. (1984). The social construction of facts and artefacts: or how the sociology of science and the sociology of technology might benefit each other. *Social Studies of Science, 14,* 399–441.

Pincus, L. B., & Trotter, C. (1995). The Disparity Between Public and Private Sector Employee Privacy Protections: A Call For Legitimate Privacy Rights For Private Sector Workers. *American Business Law Journal*, *33*(1), 51–90.

*Privacy Law Scholars Conference.* (n.d.). Retrieved April 2, 2024, from https://privacyscholars.org/

*PLSC 2023 – Privacy Law Scholars Conference*. (n.d.). Retrieved April 2, 2024, from https://Privacyscholars.Org/Plsc-History/Plsc-2023/

*PLSC Charter – Privacy Law Scholars Conference*. (n.d.). Retrieved April 2, 2024, from https://Privacyscholars.Org/About-Us/Plsc-Charter/

*PLSC History – Privacy Law Scholars Conference*. (n.d.). Retrieved April 2, 2024, From https://Privacyscholars.Org/Plsc-History/

*PLSC Sponsorship Statement – Privacy Law Scholars Conference*. (n.d.). Retrieved April 2, 2024, from https://Privacyscholars.Org/About-Us/Plsc-Sponsorship-Statement/

Polonetsky, J., & Tene, O. (2015). Who Is Reading Whom Now: Privacy in Education from Books To Moocs. *Vanderbilt Journal of Entertainment and Technology Law*, *17*(4), 927–990.

Ponemon, L. (2010). *How Global Organizations Approach the Challenge of Protecting Personal Data*. Accenture.

Poort, J., & Zuiderveen Borgesius, F. J. (2019). Does Everyone Have a Price? Understanding People's Attitude Towards Online and Offline Price Discrimination. *Internet Policy Review*, *8*(1).

Portelli, A. (2015). What Makes Oral History Different. In R. Perks & A. Thompson (Eds.), *The Oral History Reader* (3rd ed.). Routledge.

Porat, A., & Strahilevitz, L. J. (2014). Personalizing Default Rules and Disclosure with Big Data. *Michigan Law Review, 112*, 1417–1478.

Priest, G. (2020). *The rise of law and economics: An intellectual history*. Abingdon: Routledge.

Pritts, J. L. (2002). Altered States: State Health Privacy Laws and The Impact of The Federal Health Privacy Rule. *Yale Journal of Health Policy, Law, And Ethics*, *2*(2), 327–364.

*Privacy Law Scholars Conference 2008*. (N.D.). Retrieved July 22, 2021, from Http://Docs.Law.Gwu.Edu/Facweb/Dsolove/PLSC/PLSC-2008.Htm

Prosser, W. (1960). Privacy. *California Law Review, 48*(3), 383-423.

Rao, R. (2006). A Veil of Genetic Ignorance—Protecting Genetic Privacy to Ensure Equality. *Villanova Law Review*, *51*(4), 827–840.

Regan, P. M. (2015). Privacy and the Common Good: Revisited. In B. Roessler & D. Mokrosinska (Eds.), *Social Dimensions of Privacy* (1st Ed., Pp. 50–70). Cambridge University Press.

Regan, P. M. (2020). A Design for Public Trustee and Privacy Protection Regulation. *Seton Hall Legislative Journal*, *44*(3), 487–513.

Regan, P. M. (2023, September 18). *Oral History Interview for The Intellectual History Of American Privacy Law Scholarship Project* [Oral history interview].

Reidenberg, J. (2015). The Transparent Citizen. *Loyola University Chicago Law Journal*, *47*, 437–463.

Reidenberg, J. R. (1992). Privacy in the Information Economy: A Fortress Or Frontier For Individual Rights? *Federal Communications Law Journal*, *44*, 195–243.

Reidenberg, J. R. (1995). Setting Standards for Fair Information Practice In The U.S. Private Sector. *Iowa Law Review*, *80*(3), 497–552.
Reidenberg, J. R. (1996). Governing Networks and Rule-Making In Cyberspace. *Emory Law Journal*, *45*, 911–930.
Reidenberg, J. R. (1998). Lex Informatica: The Formulation of Information Policy Rules Through Technology. *Texas Law Review*, *76*, 553–593.
Reidenberg, J. R. (1999). Restoring Americans' Privacy in Electronic Commerce. *Berkeley Technology Law Journal*, *14*(2), 771–792.
Reidenberg, J. R. (2000). Resolving Conflicting International Data Privacy Rules in Cyberspace. *Stanford Law Review*, *52*(5).
Reidenberg, J. R. (2002). Privacy Wrongs in Search of Remedies. *Hastings Law Journal*, *54*(4), 877–898.
Reidenberg, J. R., & Gamet-Pol, F. (1995). The Fundamental Role of Privacy and Confidence in The Network. *Wake Forest Law Review*, *30*, 105–125.
Reiman, J. H. (1995). Driving to the Panopticon: A Philosophical Exploration of The Risks to Privacy Posed by The Highway Technology of The Future. *Computer & High Technology Law Journal*, *11*, 27–44.
Richards, N. (2005). Reconciling Data Privacy and The First Amendment. *UCLA Law Review*, *52*(4), 1149–1222.
Richards, N. (2006). The Information Privacy Law Project. *The Georgetown Law Journal*, *94*(4), 1087–1140.
Richards, N. (2008). Intellectual Privacy. *Texas Law Review*, *87*(2), 387–446.
Richards, N. (2013). The Perils of Social Reading. *The Georgetown Law Journal*, *101*, 689–724.
Richards, N. (2014). Four Privacy Myths. In A. Sarat (Ed.), *A World Without Privacy* (1st Ed., Pp. 33–82). Cambridge University Press.
Richards, N. M. (2023, April 14). *Oral History Interview for The Intellectual History of American Privacy Law Scholarship Project* [Oral history interview].
Richards, N. M., & Hartzog, W. (2016). Taking Trust Seriously in Privacy Law. *Stanford Technology Law Review*, *19*, 431–472.
Richards, N. M., & Hartzog, W. (2020). A Relational Turn for Data Protection? *European Data Protection Law Review*, *6*(4), 492–497.
Richards, N. M., & Hartzog, W. (2021). A Duty of Loyalty for Privacy Law. *Washington University Law Review*, *99*, 961–1021.
Richards, N. M., & Solove, D. J. (2007). Privacy's Other Path: Recovering The Law of Confidentiality. *The Georgetown Law Journal*, *96*(1), 123–182.
Richards, N. M., & Solove, D.J. (2010). Prosser's Privacy Law: A Mixed Legacy. *California Law Review*, *98*(6), 1887–1924.
Richardson, M. (2017). *The Right to Privacy: Origins and Influence of a Nineteenth-Century Idea*. Cambridge University Press.
Rita, E. R., & Gunning, E. D. (2006). Navigating The Blogosphere in The Workplace; The Blogosphere Or: How I Learned to Stop Worrying and Love The Blog. *Colorado Lawyer*, *35*(5), 55–62.
Rodriguez, A. I. (1998). All Bark, No Byte: Employee E-Mail Privacy Rights in the Private Sector Workplace. *Emory Law Journal*, *47*(4), 1439–1474.
Romano, R. C. (2012). Not Dead Yet: My Identity Crisis as a Historian of the Recent Past. In C. Bond Potter & R. C. Romano (Eds.), *Doing Recent History: On Privacy, Copyright, Video*

*Games, Institutional Review Boards, Activist Scholarship, and History That Talks Back* (Pp. 23-54). University of Georgia Press.
Romanosky, S., Hoffman, D., & Acquisti, A. (2014). Empirical Analysis of Data Breach Litigation. *Journal Of Empirical Legal Studies*, *11*(1), 74–104.
Rommetveit, K. & Van Dijk, N. (2022). Privacy Engineering and The Techno-Regulatory Imaginary. *Social Studies of Science* 52(6): 853–877.
Rosen, J. (2001). *The Unwanted Gaze: The Destruction of Privacy in America*. Random House.
Rosenberg, J. M. (1969). *The Death of Privacy*. New York: Random House.
Rotenberg, M. (2001). Fair Information Practices and The Architecture of Privacy (What Larry Doesn't Get). *Stanford Technology Law Review*, *1*(2001), 1–34.
Rothstein, L. E. (2000). Privacy or Dignity?: Electronic Monitoring In The Workplace. *New York Law School Journal of International and Comparative Law*, *19*(3), 379–412.
Rubel, A., & Biava, R. (2013). A Framework for Comparing Privacy States. *Iconference 2013 Proceedings*, 85–90.
Rubel, A., & Jones, K. (2017). Data Analytics in Higher Education: Key Concerns and Open Questions. *University Of Saint Thomas Journal Of Law & Public Policy*, *XI*(1), 25–44.
Rubinstein, I. (2011). Regulating Privacy By Design. *Berkeley Technology Law Journal*, *26*, 1409–1456.
Rubinstein, I. (2014). Voter Privacy in the Age of Big Data. *Wisconsin Law Review*, *5*, 861–936.
Rubinstein, I. (2018). Privacy Localism. *Washington Law Review*, *93*, 1961–2049.
Rubinstein, I., & Good, N. (2013). Privacy By Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents. *Berkeley Technology Law Journal*, *28*, 1333–1413.
Rubinstein, I., & Hartzog, W. (2016). Anonymization and Risk. *Washington Law Review*, *91*, 203–260.
Rubinstein, I., & Petkova, B. (2020). Governing Privacy in the Datafied City. *Fordham Urban Law Journal*, *XLVII*, 755–826.
Rule, J. B. (2004). Toward Strong Privacy: Values, Markets, Mechanisms, And Institutions. *University Of Toronto Law Journal*, *54*(2), 183–226.
Rule, J., McAdam, D., Stearns, L. & Uglow, D. (1980). *The Politics of privacy: planning for personal data systems as powerful technologies*. New York: Elsevier North Holland, Inc.
Russell, M. M. (1995). Privacy And IVHS: A Diversity of Viewpoints. *Computer & High Technology Law Journal*, *11*(1), 145–147.
Salzwedel, M. R., & Ericson, J. (2003). Cleaning Up Buckley: How The Family Educational Rights and Privacy Act Shields Academic Corruption in College Athletics. *Wisconsin Law Review*, *2003*(6), 1053–1114.
Samaha, A. M., & Strahilevitz, L. J. (2015). Don't Ask, Must Tell—And Other Combinations. *California Law Review*, *103*, 919–987.
Samuelson, P. (2000). Privacy As Intellectual Property? *Stanford Law Review*, *52*(5), 1125–1174.
Sanchez Abril, P. (2007a). A (My)Space of One's Own: On Privacy and Online Social Networks. *Northwestern Journal of Technology and Intellectual Property*, *6*(1).
Sanchez Abril, P. (2007b). Recasting Privacy Torts in A Spaceless World. *Harvard Journal of Law & Technology*, *21*(1), 1–48.
Sandfuchs, B., & Kapsner, A. (2016). Coercing Online Privacy. *I/S: Journal of Law and Policy for The Information Society*, *12*(2), 185–230.
Sanfilippo, M. R., & Shvartzshnaider, Y. (2023). Technofuturism In Play: Privacy, Surveillance, And Innovation at Walt Disney World. In B. M. Frischmann, M. J. Madison, & M. R.

Sanfilippo (Eds.), *Governing Smart Cities as Knowledge Commons* (1st Ed., Pp. 223–247). Cambridge University Press.
Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2018). Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality & Quantity*, *52*(4), 1893–1907.
Steve Sawyer, S. & Jarrahi, M. H. (2014). Sociotechnical Approaches to the Study of Information Systems. In H. Topi & A. Tucker (Eds.), *Computing Handbook: Information Systems and Information Technology*. CRC Press LLC.
Sax, M., Helberger, N., & Bol, N. (2018). Health As a Means Towards Profitable Ends: Mhealth Apps, User Autonomy, And Unfair Commercial Practices. *Journal Of Consumer Policy*, *41*(2), 103–134.
Schlogl, L., Elias W., & Barbara P. (2021). Constructing The 'Future of Work': An Analysis of The Policy Discourse. *New Technology, Work and Employment* 36: 307-326.
Schnaitman, P. (1999). Building A Community Through Workplace E-Mail: The New Privacy Frontier. *Michigan Telecommunicationsand Technology Law Review*, *5*(1), 177–216.
*Scholars Tell UC Berkeley: Cut Ties with Palantir*. (2019, May 29). Https://Www.Mijentesupportcommittee.Com/Post/Scholars-Tell-Uc-Berkeley-Cut-Ties-With-Palantir
Schriver, R. R. (2002). You Cheated, You Lied: The Safe Harbor Agreement and Its Enforcement by The Federal Trade Commission. *Fordham Law Review*, *70*(6), 2777–2818.
Schwartz, P. M. (1992). Data Processing and Government Administration: The Failure Of The American Legal Response To The Computer. *Hastings Law Journal*, *43*, 1321–1389.
Schwartz, P. M. (1995). Privacy And Participation: Personal Information and Public Sector Regulation in The United States. *Iowa Law Review*, *80*(3), 553–618.
Schwartz, P. M. (1997). Privacy And the Economics of Personal Health Care Information. *Texas Law Review*, *76*(1), 1–76.
Schwartz, P. M. (1999). Privacy And Democracy in Cyberspace. *Vanderbilt Law Review*, *52*, 1609–1701.
Schwartz, P. M. (2000a). Internet Privacy and The State. *Connecticut Law Review*, *32*, 815–859.
Schwartz, P. M. (2000b). Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control and Fair Information Practices. *Wisconsin Law Review*, 743–788.
Schwartz, P. M. (2004). Property, Privacy, And Personal Data. *Harvard Law Review*, *117*(7), 2056–2128.
Schwartz, P. M. (2023, March 29). *Oral History Interview for The Intellectual History of American Privacy Law Scholarship Project* [Oral history interview].
Schwartz, P. M., & Peifer, K.-N. (2017). Transatlantic Data Privacy Law. *The Georgetown Law Journal*, *106*, 115–179.
Schwartz, P. M., & Solove, D. J. (2011). The PII Problem: Privacy and A New Concept of Personally Identifiable Information. *New York University Law Review*, *86*(6), 1814–1894.
Schwartz, P. M., & Treanor, W. M. (2003). New Privacy. *Michigan Law Review*, *101*(6), 2163–2184.
Seipp, D.J. (1978). *The Right to Privacy in American History.* Boston: Program on information Resources Policy, Harvard University.
Selbst, A. D. (2017). Disparate Impact in Big Data Policing. *Georgia Law Review*, *52*, 109–195.
Selbst, A. D. (2021). An Institutional View of Algorithmic Impact Assessments. *Harvard Journal of Law & Technology*, *35*(1), 118–191.

Selbst, A. D. (2023, October 26). *Oral History Interview for the Intellectual History of American Privacy Law Scholarship Project* [Oral history interview].
Selbst, A. D., & Barocas, S. (2018). The Intuitive Appeal of Explainable Machines. *Fordham Law Review, 87*, 1885–1139.
Sepehr, P. & Felt, U. (2023). Urban Imaginaries as Tacit Governing Devices: The Case of Smart City Vienna. *Science, Technology, & Human Values*: 1-23.
Sheftel, A., & Zembrzycki, S. (2010). Only Human: A Reflection on the Ethical and Methodological Challenges of Working with "Difficult" Stories. *The Oral History Review*, *37*(2), 191-214.
Shilton, K., & Greene, D. (2019). Linking Platforms, Practices, And Developer Ethics: Levers for Privacy Discourse in Mobile Application Development. *Journal Of Business Ethics*, *155*(1), 131–146.
Shorr, S. (1995). Personal Information Contracts: How to Protect Privacy Without Violating the First Amendment. *Cornell Law Review*, *80*(6), 1756–1850.
Siebecker, M. R. (2003). Cookies and the Common Law: Are Internet Advertisers Trespassing on our Computers? *Southern California Law Review*, *76*, 893–952.
Silverman, R. M., & Patterson, K. L. (2014). *Qualitative Research Methods for Community Development.* Routledge.
Singh, R. (2006). Two-Factor Authentication: A Solution to Times Past or Present—The Debate Surrounding the Gramm-Leach-Bliley Security Safeguards Rule and the Methods of Risk Assessment and Compliance. *I/S: Journal of Law and Policy for The Information Society*, *2*(3), 761–780.
Skinner-Thompson, S. (2017). Performative Privacy. *University Of California, Davis*, *50*, 1673–1739.
Skinner-Thompson, S. (2020). *Privacy at the Margins* (1st Ed.). Cambridge University Press.
Sloan, R. H., & Warner, R. (2014). Beyond Notice and Choice: Privacy, Norms, and Consent. *Journal Of High Technology Law*, *14*(2), 370–414.
Sloan, R. H., & Warner, R. (2016). "I'll See": How Surveillance Undermines Privacy by Eroding Trust. *Santa Clara High Technology Law Journal*, *32*, 221–267.
Sloan, R. H., & Warner, R. (2019). Algorithms And Human Freedom. *Santa Clara High Technology Law Journal*, *35*, 1–35.
Slomovic, A. (2017). Ehealth And Privacy in U.S. Employer Wellness Programs. In S. Adams, N. Purtova, & R. Leenes (Eds.), *Under Observation: The Interplay Between Ehealth and Surveillance* (Vol. 35). Springer International Publishing.
Smith, E. (2009). Imaginaries of Development: The Rockefeller Foundation and Rice Research. *Science As Culture* 18(4): 461-482.
Smith, J. E. (2007). You Can Run, But You Can't Hide: Protecting Privacy from Radio Frequency Identification Technology. *North Carolina Journal of Law and Technology*, *8*(2), 249–272.
Smith, L. S. (2006). RFID And Other Embedded Technologies: Who Owns the Data? *Santa Clara Computer & High Technology Law Journal*, *22*(4), 695–756.
Smolla, R. A. (2002). Accounting for the Slow Growth of American Privacy Law. *Nova Law Review*, *27*(2), 289–324.
Sobel, R. (2002). The Demeaning of Identity and Personhood in National Identification Systems. *Harvard Journal of Law & Technology*, *15*(2), 319–388.
Solove, D. J. (2001). Privacy And Power: Computer Databases and Metaphors For Information Privacy. *Stanford Law Review*, *53*, 1393–1462.

Solove, D. J. (2002a). Digital Dossiers and the Dissipation of Fourth Amendment Privacy. *Southern California Law Review*, *75*(5), 1083–1168.
Solove, D. J. (2002b). Access And Aggregation: Public Records, Privacy and the Constitution. *Minnesota Law Review*, *86*(6), 1137–1218.
Solove, D.J. (2002c). Conceptualizing Privacy. *California Law Review, 90*, 1087-1156.
Solove, D. J. (2003a). The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure. *Duke Law Journal*, *53*(3), 967–1066.
Solove, D. J. (2003b). Identity Theft, Privacy, And the Architecture of Vulnerability. *Hastings Law Journal*, *54*(4), 1227–1276.
Solove, D. J. (2006a). A Taxonomy of Privacy. *University Of Pennsylvania Law Review*, *154*(3), 477–564.
Solove, D. J. (2006b). A Tale of Two Bloggers: Free Speech and Privacy in The Blogosphere. *Washington University Law Review*, *84*(5), 1195–1200.
Solove, D. J. (2006c). *A Brief History of Information Privacy Law*. Proskauer on Privacy.
Solove, D. J. (2007). "I've Got Nothing to Hide" And Other Misunderstandings of Privacy. *San Diego Law Review*, *44*(4), 745–772.
Solove, D. J. (2021). The Myth of The Privacy Paradox. *The George Washington Law Review, 89*(1), 1–51.
Solove, D. J. (2023, February 26). *Oral History Interview for the Intellectual History of American Privacy Law Scholarship Project* [Oral history interview].
Solove, D. J., & Citron, D. K. (2018). Risk And Anxiety: A Theory of Data Breach Harms. *Texas Law Review, 96*, 737-86.
Solove, D. J, & Citron, D. K. (2022). Privacy Harms. *Boston University Law Review*, *102*, 793–863.
Solove, D. J., & Hartzog, W. (2013). The FTC and the New Common Law of Privacy. *Columbia Law Review*, *114*, 583–676.
Solove, D. J., & Hartzog, W. (2022). Introduction: Chronicle of a Breach Foretold. In *Breached! Why Data Security Law Fails and How to Improve It*. Oxford University Press.
Solove, D. J., & Hoofnagle, C. J. (2006). A Model Regime of Privacy Protection. *University Of Illinois Law Review*, *2006*(2), 357–404.
Sovern, J. (1999). Opting In, Opting Out, Or No Options at All: The Fight for Control of Personal Information. *Washington Law Review*, *74*(4), 1033–1118.
Sovern, J. (2001). Protecting Privacy with Deceptive Trade Practices Legislation. *Fordham Law Review*, *69*, 1305–1358.
Spencer, S. B. (2002). Reasonable Expectations and the Erosion of Privacy. *San Diego Law Review, 39*(3), 843–916.
Sprague, R., Grauberger, K., & Barberis, N. (2015). *One Hundred Twenty Years of U.S. Privacy Law Scholarship: A Latent Semantic Analysis* (Draft). Available online.
Stark, L. (2016). The Emotional Context of Information Privacy. *The Information Society*, *32*(1), 14–27.
Stark, L., & Levy, K. (2018). The Surveillant Consumer. *Media, Culture & Society*, *40*(8), 1202–1220.
Stark, L., Stanhaus, A., & Anthony, D. L. (2020). "I Don't Want Someone to Watch Me While I'm Working": Gendered Views of Facial Recognition Technology in Workplace Surveillance. *Journal of the Association for Information Science and Technology*, *71*(9), 1074–1088.

Staten, M. E., & Cate, F. H. (2003). The Impact of Opt-In Privacy Rules on Retail Credit Markets: A Case Study Of MBNA. *Duke Law Journal*, *52*(4), 745–786.
Steinbock, D. (2006). Designating The Dangerous: From Blacklists to Watch Lists. *Seattle University Law Review*, *30*(1), 65–118.
Steinbock, D. J. (2005). Data Matching, Data Mining, And Due Process. *Georgia Law Review*, *40*(1), 1–84.
Strahilevitz, L. J. (2010). Reunifying Privacy Law. *California Law Review*, *98*(6), 2007–2048.
Strahilevitzt, L. (2005). A Social Networks Theory of Privacy. *The University of Chicago Law Review*, *72*(3), 919–988.
Strandburg, K. J. (2005). Privacy, Rationality, And Temptation: A Theory of Willpower Norms. *Rutgers Law Review*, *57*(4), 1235–1306.
Stuart, S. P. (2005). Lex-Praxis of Education Informational Privacy for Public Schoolchildren. *Nebraska Law Review*, *84*(4), 1158–1225.
Suitner, J. (2015). *Imagineering Cultural Vienna: Urban Studies*. Germany: Verlag Transcript.
Sullivan, C. (2013). Digital Identity, Privacy and the Right to Identity in the United States of America. *Computer Law & Security Review*, *29*(4), 348–358.
Surden, H. (2007). Structural Rights in Privacy. *SMU Law Review*, *60*(4), 1605–1632.
Susser, D. (2022). Data And the Good? *Surveillance & Society* 20(3): 297-301
Susser, D., Roessler, B., & Nissenbaum, H. F. (2019). Online Manipulation: Hidden Influences in a Digital World. *Georgetown Law Technology Review*, *4*, 1–45.
Swaya, M. E., & Eisenstein, S. R. (2005). Emerging Technology in the Workplace. *Labor Lawyer*, *21*(1), 1–18.
Sweeney, L. (2013). Discrimination In Online Ad Delivery. *Search Engines*, *9*, 1–19.
Swire, P. P. (1997). Markets, Self-Regulation, And Government Enforcement in the Protection of Personal Information, In *Privacy and Self-Regulation in the Information Age by the U.S. Department of Commerce*.
Swire, P. P. (1998). Of Elephants, Mice, and Privacy: International Choice of Law and the Internet. *The International Lawyer*, *32*(4), 991–1025.
Swire, P. P. (2002). The Surprising Virtues of The New Financial Privacy Law. *Minnesota Law Review*, *86*(6), 1263–1324.
Swire, P. P. (2003). Trustwrap: The Importance of Legal Rules to Electronic Commerce And Internet Privacy. *Hastings Law Journal*, *54*, 847–875.
Swire, P. P. (2005). Elephants And Mice Revisited: Law and Choice of Law on the Internet. *University Of Pennsylvania Law Review*, *153*(6), 1975–2002.
Swire, P. P. (2012). Social Networks, Privacy, And Freedom of Association: Data Protection Vs. Data Empowerment. *North Carolina Law Review*, *90*(5), 1371–1416.
Swire, P. P. (2022). The Portability and Other Required Transfers Impact Assessment (Port-Ia): Assessing Competition, Privacy, Cybersecurity, And Other Considerations. *Georgetown Law Technology Review*, *6*, 57–122.
Sylvester, D. J., & Lohr, S. (2005). The Security of Our Secrets: A History of Privacy and Confidentiality in Law and Statistical Practice. *Denver University Law Review*, *83*(1), 147–208.
Taylor, C. (2002). Modern Social Imaginaries. *Public Culture, 14*(1), pp. 91-124.
Taylor, C. (2004). *Modern Social Imaginaries. Durham*. NC: Duke University Press.

Tene, O., & Polonetsky, J. (2012a). To Track Or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising. *Minnesota Journal of Law, Science & Technology*, *13*, 281–357.

Tene, O., & Polonetsky, J. (2012b). Privacy in the Age of Big Data: A Time for Big Decisions. *Stanford Technology Law Review Online*, *64*, 63–69.

Tene, O., & Polonetsky, J. (2013). A Theory of Creepy: Technology, Privacy and Shifting Social Norms. *Yale Journal of Law and Technology*, *16*, 59–102.

Tene, O., & Polonetsky, J. (2017). Taming The Golem: Challenges Of Ethical Algorithmic Decision-Making. *North Carolina Journal of Law and Technology*, *19*(1), 125–173.

*The Human Genome Project*. (N.D.). National Human Genoma Research Institute. Retrieved January 15, 2024, From Https://Www.Genome.Gov/Human-Genome-Project

Tranter, Kieran. 2011. The Speculative Jurisdiction. The Science Fictionality of Law and Technology. *Griffith Law Review* 20(4): 817-850.

Tschider, C. (2018). The Consent Myth: Improving Choice for Patients of the Future. *Washington University Law Review*, *96*, 1505–1536.

Tushnet, M. (2011). From Judicial Restraint to Judicial Engagement: A Short Intellectual History. *George Mason Law Review*, *19*(4), 1043–1052.

Twomey, W. (2018). A History of Privacy Rights in America: From the Fourth Amendment to the Patriot Act. *Colloquium: The Political Science Journal of Boston College*, *2*(2), 18-28.

Vagle, J. L. (2016). *The History, Means, And Effects of Structural Surveillance* [Faculty Scholarship at Penn Carey Law].

Vaidyanathan, S. (2011). *The Googlization of everything: (And why we should worry)*. University of California Press.

Van Den Hoven, M. J. (1997). Privacy and the Varieties of Moral Wrong-Doing in an Information Age. *ACM SIGCAS Computers and Society*, *27*(3), 33–37.

Van Der Sloot, B. (2017). Where is the Harm in a Privacy Violation? Calculating The Damages Afforded in Privacy Cases by the European Court of Human Rights. *Journal Of Intellectual Property, Information Technology and E-Commerce Law*, *8*, 322–351.

Van Hoboken, J. (2016). From Collection to Use in Privacy Regulation? A Forward-Looking Comparison of European and US Frameworks for Personal Data Processing. In B. Van Der Sloot, D. Broeders, & E. Schrijvers (Eds.), *Exploring The Boundaries Of Big Data*. The Netherlands Scientific Council for Government Policy.

Van Lente, H. & Rip, A. (1998). Expectations In Technological Developments: An Example of Prospective Structures to Be Filled in by Agency. In *Getting New Technologies Together: Studies in Making Sociotechnical Order*, Edited by Cornelis Disco, and Barend Van Der Meulen. De Gruyter, Inc.

Van Loo, R. (2019). The Missing Regulatory State: Monitoring Businesses in an Age of Surveillance. *Vanderbilt Law Review*, *72*, 1563–1631.

Veale, M., & Zuiderveen Borgesius, F. (2022). Adtech And Real-Time Bidding Under European Data Protection Law. *German Law Journal*, *23*, 226–256.

Viljoen, S. (2021). A Relational Theory of Data Governance. *The Yale Law Journal*.

Vincent, D. (2016). *Privacy: A Short History*. Polity Press.

Wachter, S., & Mittelstadt, B. (2019). A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data And AI. *Columbia Business Law Review*, *2019*(2), 1–130.

Wachter, S., Mittelstadt, B., & Russell, C. (2018). Counterfactual Explanations Without Opening the Black Box: Automated Decisions and The GDPR. *Harvard Journal of Law & Technology*, *31*(2), 841–887.

Wachter, S., Mittelstadt, B., & Russell, C. (2021). Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law And AI. *Computer Law & Security Review*, *41*, 1–31.

Wakana, J. M. (2003). The Future of Online Privacy: A Proposal for International Legislation. *Loyola Of Los Angeles International and Comparative Law Review*, *26*(1), 151–180.

Waldman, A. E. (2018a). Privacy, Notice, And Design. *Stanford Technology Law Review*, *21*, 129–184.

Waldman, A. E. (2018b). Designing Without Privacy. *Houston Law Review*, *55*(3), 659–727.

Waldman, A. E. (2019). Privacy's Law of Design. *U.C. Irvine Law Review*, *9*, 1239–1288.

Waldman, A. E. (2020). Privacy Law's False Promise. *Washington University Law Review*, *97*, 773–834.

Waldman, A. E. (2021). The New Privacy Law. *UC Davis Law Review*, *55*, 19–42.

Waldman, A. E. (2022a). Privacy's Rights Trap. *Northwestern University Law Review*, *117*, 88–106.

Waldman, A. E. (2022b). Privacy, Practice, and Performance. *California Law Review*, *110*, 1221–1280.

Waldman, A. E. (2022, November 30). *Oral History Interview for the Intellectual History of American Privacy Law Scholarship Project* [Oral history interview].

Waldman, A. E., & Martin, K. (2022). Governing Algorithmic Decisions: The Role of Decision Importance and Governance on Perceived Legitimacy of Algorithmic Decisions. *Big Data & Society*, *9*(1), 1–16.

Wang, H. (2022). Transparency As Manipulation? Uncovering The Disciplinary Power of Algorithmic Transparency. *Philosophy & Technology*, *35*(69), 1–25.

Warner, R., & Sloan, R. H. (2012). Behavioral Advertising: From One-Sided Chicken to Informational Norms. *Vanderbilt Journal of Entertainment and Technology Law*, *15*, 49–83.

Warner, R., & Sloan, R. H. (2014). Self, Privacy, And Power: Is It All Over? *Tulane Journal of Technology and Intellectual Property*, *17*, 61–108.

Watson, N. (2001). *The Private Workplace and the Proposed "Notice of Electronic Monitoring Act": Is "Notice" Enough? 54*(1), 79–102.

Webb, D. (2007). *Privacy and Solitude: The Medieval Discovery of Personal Space*.

Wesche, T. M. (2002). Reading Your Every Keystroke: Protecting Employee E-Mail Privacy. *Journal Of High Technology Law*, *1*(1), 101–118.

West, S. M. (2017). Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business & Society*, *58*(1), 20-41.

Westin, A. F. (1967). *Privacy and Freedom.* Atheneum.

Westin, A. F. (1996). Privacy in the Workplace: How Well Does American Law Reflect American Values? *Chicago-Kent Law Review*, *72*, 271–283.

Westin, A. F. (2003). Social And Political Dimensions of Privacy. *Journal Of Social Issues*, *59*(2), 431–453.

White, G. E. (1980). *Tort law in America: An intellectual history*. Place of publication not identified: Oxford University Press.

White, J. J. (1997). E-Mail@Work.Com: Employer Monitoring of Employee E-Mail. *Alabama Law Review*, *48*(3), 1079–1104.
Whitmant, J. Q. (2004). The Two Western Cultures of Privacy: Dignity Versus Liberty. *The Yale Law Journal*, *113*(6), 1151–1222.
Wickberg, D. (2018). Conclusion. The Idea of Historical Context and the Intellectual Historian. In Raymond Haberski, Jr, & Andrew Hartman, *American Labyrinth*. Cornell University Press.
Wilborn, E. (1998). Revisiting The Public/Private Distinction: Employee Monitoring in the Workplace. *Georgia Law Review*, *32*(3), 825–888.
Wilka, R. (2018). Privacy Commitments. *Washington Law Review*, *93*, 63–101.
Willis, L. E. (2014). Why Not Privacy by Default? *Berkeley Technology Law Journal*, *29*, 61–133.
Winn, P. A. (2002). Confidentiality In Cyberspace: The HIPAA Privacy Rules and The Common Law. *Rutgers Law Journal*, *33*(3), 617–682.
Wolf, C. (2013). Delusions Of Adequacy? Examining The Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers. *Washington University Journal of Law & Policy*, *43*, 227–258.
Wong, R. Y., & Mulligan, D. K. (2019a). Bringing Design to The Privacy Table: Broadening "Design" In "Privacy By Design" Through The Lens Of HCI. *Proceedings Of The 2019 CHI Conference on Human Factors in Computing Systems*, 1–17.
Wong, R. Y., & Mulligan, D. K. (2019b). Bringing Design to the Privacy Table: Broadening "Design" In "Privacy By Design" Through The Lens Of HCI. *Proceedings Of The 2019 CHI Conference on Human Factors in Computing Systems*, 1–17.
Wood, A., Altman, M., Bembenek, A., Bun, M., Gaboardi, M., Honaker, J., Nissim, K., O'Brien, D., Steinke, T., & Vadhan, S. (2018). Differential Privacy: A Primer for a Non-Technical Audience. *Vanderbilt Journal of Entertainment & Technology Law Vanderbilt Journal of Entertainment & Technology Law*, *21*(1), 209–276.
Woodford, C. (2004). Trusted Computing or Big Brother—Putting the Rights Back in Digital Rights Management. *University Of Colorado Law Review*, *75*(1), 253–300.
Wu, F. T. (2013). Defining Privacy and Utility in Data Sets. *University Of Colorado Law Review*, *84*(4), 1117–1178.
Xu, H., Bagby, J. W., & Melonas, T. R. (2009). Regulating Privacy in Wireless Advertising Messaging: FIPP Compliance by Policy Vs. By Design. In I. Goldberg & M. J. Atallah (Eds.), *Privacy Enhancing Technologies*.
Yakovleva, S. (2020c). Personal Data Transfers in International Trade and EU Law: A Tale of Two 'Necessities.' *The Journal of World Investment & Trade*, *21*(6), 881–919.
Yakovleva, S., & Irion, K. (2020a). Pitching Trade Against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade. *International Data Privacy Law*, *10*(3), 201–221.
Yakowitz Bambauer, J. (2012). The New Intrusion. *Notre Dame Law Review*, *88*(1), 205–276.
Yoo, C. S. (2015). Cloud Computing, Contractibility, And Network Architecture. In C. S. Yoo & J.-F. Blanchette (Eds.), *Regulating the Cloud* (Pp. 115–134). The MIT Press.
Yung, J. (2005). Big Brother IS Watching: How Employee Monitoring In 2004 Brought Orwell's 1984 To Life and What the Law Should Do About It. *Seton Hall Law Review*, *36*(1), 163–222.
Zarsky, T. (2022, November 22). *Oral History Interview for the Intellectual History of American Privacy Law Scholarship Project* [Oral history interview].

Zarsky, T. Z. (2003). Mine Your Own Business: Making the Case for the Implications of the Data Mining of Personal Information in The Forum of Public Opinion. *Yale Journal of Law and Technology*, *5*, 1–56.

Zarsky, T. Z. (2015). The Privacy–Innovation Conundrum. *Lewis & Clarck Law Review*, *19*(1), 115–168.

Zarsky, T. Z. (2004a). Desperately Seeking Solutions: Using Implementation-Based Solutions for The Troubles of Information Privacy in the Age of Data Mining and the Internet Society. *Maine Law Review*, *56*(1), 13–60.

Zarsky, T. Z. (2004b). Thinking Outside the Box: Considering Transparency, Anonymity, And Pseudonymity as Overall Solutions to the Problems in Information Privacy in the Internet Society. *University Of Miami Law Review*, *48*(4), 991–1044.

Zeide, E. (2016). Student Privacy Principles for the Age of Big Data: Moving Beyond FERPA and FIPPs. *Drexel Law Review*, *8*, 338–393.

Zeide, E. (2017). The Structural Consequences of Big Data-Driven Education. *Big Data*, *5*(2), 164–172.

Ziegler, M. (2018). A History of Privacy Politics. In *Beyond Abortion: Roe v. Wadeand the Battle for Privacy* (pp. 15-40). Cambridge, Massachusetts; London, England: Harvard University Press.

Zimmeck, S., Wang, Z., Zou, L., Iyengar, R., Liu, B., Schaub, F., Wilson, S., Sadeh, N., Bellovin, S. M., & Reidenberg, J. (2017). Automated Analysis of Privacy Requirements for Mobile Apps. *Proceedings 2017 Network and Distributed System Security Symposium*. Network And Distributed System Security Symposium, San Diego, CA.

Zittrain, J. (2000). What The Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication. *Stanford Law Review*, *52*(5), 1201–1250.

Zubrzycki, C. M. (2021). Privacy From Doctors. *Yale Law & Policy Review*, *39*(2), 526–592.

Zuboff, S. (2019*). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.

Zuiderveen Borgesius, F. J., & Steenbruggen, W. (2019). The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, And Trust. *Theoretical Inquiries in Law*, *20*(1), 291–322.

Zuiderveen Borgesius, F., & Poort, J. (2017). Online Price Discrimination and EU Data Privacy Law. *Journal Of Consumer Policy*, *40*(3), 347–366.

**Appendix A—Informed consent**

<<DATE>>

<<FULL NAME>>

Dear Professor <<LAST NAME>>,

My name is María P. Angel. I am a Ph.D. Candidate at the University of Washington School of Law, conducting research under the supervision of Professor Ryan Calo. As part of my Ph.D. research project, I am documenting **the intellectual history of privacy law scholarship in America**, and I would like to invite you to participate in my research through an oral history exercise.

**What will you be asked to do?**

Let me outline for you the oral history process. Because so much historical information exists only in people's memories and not in the written record, the oral history method is used to preserve firsthand accounts of events through recorded interviews. Though based on careful preparation, the interviews are simply conversations, usually held over Zoom. Interviews can take anywhere from five minutes to two hours, but multiple sessions can be arranged if more time is needed. If you decide to take part, **I will ask you to talk about your professional career as a privacy scholar, the privacy issues you have explored over time, the people you have worked with, the evolution of the concept of privacy in your own scholarship, and the desirable futures you expect to achieve through privacy regulation**. You do not have to answer any questions that you do not wish to answer, for any reason. You can choose to stop the conversation at any time.

**What will happen to the information you provide?**

Typically, the interviews are transcribed either by me or by a hired human transcriber, lightly edited for continuity if necessary, and the draft transcript sent to the interviewee for review. I hope the interviewees will not delete important material or try to formalize the conversational tone of the interview, although I welcome additional details. The transcript, as returned to me by the interviewee, is the draft on which I will base any final document, as well as the research products (dissertation, journal articles, etc.) I may develop afterwards. If you participate, I will ask you to return your draft transcript within a specified time. If you do not return it, I will prepare the final text from my edited draft, but I much prefer to have your review. Regardless, you are free to withdraw from the exercise at any point in time prior to the completion of the final transcript, when it is made public.

Once you have read and made corrections to the edited transcript of the interview, an Oral History Agreement[107] is signed by you and me. Copyright to the tapes and transcripts will be assigned to María P. Angel. As the copyright holder, I will then respond to requests for permission to quote for publication. Interviewees have several options at the time the Oral History Agreement is signed, such as placing portions of the material under seal for a specified period of time to the extent permissible under the law. Any special provisions of this kind may be included in the Agreement to be signed by you and me. You are free to use the information in this interview as well as the interview itself for your own purposes, including publication.

The interviewee receives a copy of the final transcript for personal use. The final transcript of each complete oral history, along with some video clips from the interview (if applicable), are also deposited in The Internet Archive (archive.org), a non-profit digital library of cultural artifacts in

[107] The Oral History Agreement is the formal legal release agreement.

digital form. Therefore, researchers, historians, scholars, people with print disabilities, and the general public can freely access them online. However, their transmission or reproduction beyond that allowed by fair use require the written permission of the copyright owner.

**What can you do if you want more information?**

If you have questions about or feel you have been harmed by this research, you can contact me at mpangel@uw.edu or 202-913-5398.

**Talk to my Ph.D. advisor.** Professor Ryan Calo is my Ph.D. advisor at the University of Washington and can be contacted at rcalo@uw.edu or 206-543-1580.

**Talk to someone else.** If you want to talk with someone who is not involved in the research project about the study, your rights as a research subject, or to report problems or complaints about the study, contact the UW Human Subjects Division at hsdinfo@uw.edu or 206-543-0098.

---

Please sign this letter and return it to me by email if you would like to accept my invitation. Please bear in mind that this document acts as the **formal informed consent letter**. I do hope you'll do me the honor of collaborating with me, as I expect your oral history to be part of the intellectual history of the American privacy law scholarship I am currently working on. I look forward to hearing from you.

Sincerely,

María P. Angel

**Ph.D. Candidate | Fulbright Grantee**

**School of Law | University of Washington, Seattle**

**(202) 913-5398 | mpangel@uw.edu**

_____

(Signed: <<INTERVIEWEE NAME>>)

_____

(Address)

_____

(City, State, Zip)

**Appendix B—Interview guide**

**Intellectual History of American Privacy Law Scholarship Project**

**Interview Guide**

Interviewer: María P. Angel

Interviewee:

Date:

Themes

## I. Education and professional career as a privacy scholar

A. Undergrad

B. Graduate studies

C. Early career

D. Teaching

E. Scholarship

- Field
- Areas of work or expertise
- Other disciplines
- Types of privacy
- Jurisdictions

F. Advocacy

G. Conferences

- PLSC

**II. People you have worked with**

A. How you choose your co-authors

B. Interlocutors (informal reviewers)

C. Mentors

D. “Contradictors”

**III. Privacy scholarship**

A. First privacy issue addressed

B. Sociopolitical/sociotechnical contexts

C. How do you choose a topic

D. Privacy harms

E. Proposed privacy solutions

F. Future possibilities of your research work

**IV. Technologies you have mainly focused on and your perceptions about them**

A. Relevant technologies/innovations (over time)

B. Relevant practices

C. Strategies used to understand a given technology/practice

**V. Evolution of the concept of privacy in your own scholarship**

A. Own perception of the evolution

B. Initial understanding of the concept of privacy

C. Current understanding of the concept of privacy

D. Possible turning points

## VI. Desirable futures you expect to achieve through privacy regulation

A. Visions of desirable futures

B. Envisioned privacy regulation

- US exclusivity?

C. Values that should shape the legal regulation of privacy

D. Key actors

**Appendix C—Codebook of categories**

| Category | Description |
|---|---|
| IH - Technology | Technologies the author is addressing in this paper. |
| IH - Practice | Practices the author is addressing in this paper. |
| IH - Societal attitude | Reception/rejection of the technology by society. Attitudes shown towards sociotechnical developments. |
| IH – Legal System | Hard and soft law measures taken by the different government branches to protect information privacy. Applies in the US and abroad. |
| IH - Identified Harm | Harms the author cares about. |
| IH - Proposed tool | Solutions the author proposes to address the harms he/she is concerned with. It may also include the solutions the author dislikes and fights against. |
| IH - Reference to power | Mentions of power, power asymmetries, etc. |
| IH - Reference to the value of privacy | Instrumental approaches to privacy. References to the social values of privacy, which go beyond its inherent value. |
| TI - Narrative | Accounts of how things are or ought to be. |
| TI - Desirable Future | Vision of desirable future that the author/interviewee hopes we can achieve when it comes to information privacy. |
| TI - Key actor | Key actors that should be involved in achieving the author/interviewee's desirable future. |
| TI - Values involved | Values present in the author/interviewee's desirable future. |
| PLSC - Community | Individuals that are mentioned as part of PLSC. |
| PLSC - Outsiders | Individuals that are placed outside of PLSC. |

| | |
|---|---|
| PLSC - Origin | Historical data about how the conference came to be. |
| PLSC - Evolution | Changes and transformations of the conference over the years. Crises, turning points, milestones. |
| PLSC - Format | Characteristics about PLSC's discussion format. Interviewee's perceptions about it. |
| PLSC - Criticism | Interviewee's critiques about the conference. Drawbacks. Flaws. Improvement opportunities. |
| PLSC - Guiding principle | Ideas that guided the design of the conference. Ideas that guide the conference today. |
| PLSC - Mentorship dynamic | Relationships in which more knowledgeable scholars guide the professional development and growth of another. |
| PLSC - Interlocution dynamic | Relationships between scholars who reach out to each other to discuss ideas or request feedback on drafts. |
| PLSC - Relevance | Interviewee's perceptions about the conference. The conference v. the field. |