2023 We Robot

UNDERSTANDING THE TECHNO-LEGAL IMAGINARIES OF AMERICAN PRIVACY LAW SCHOLARS

María P. Angel[*]

Dear We Robot 2023 participants,

Thank you so much for reading! This draft is still a work in progress, so I'd appreciate any feedback. It should be noted that I intend to submit this article to an STS journal (e.g., *Science, Technology & Human Values*). As a result, the article's structure, citation format, and extension differ from those of a law review article.

I am still unsure of how deep I should go in Part III. I have another paper (*Privacy's Algorithmic Turn* – workshopped at PLSC 2023) where I explain in detail the transformation of American privacy law scholars' regulatory approaches to information privacy. As such, I do not want to be repetitious here, but I feel it is also important to provide enough context so that the techno-legal imaginaries that follow in Parts IV and V can be understood fully. I would appreciate any advice on how to achieve this balance.

I look forward to your comments and questions!

María

[*] Ph.D. in Law Candidate, University of Washington School of Law. Support for this research came from the Tech Policy Lab at the University of Washington, where the author works as a Research Assistant.

Abstract

Like any other legal actor, privacy law scholars have visions about the desirable futures that could be achieved through the regulation of technoscientific innovation. These visions—here referred to as "techno-legal imaginaries"—have the power to shape how sociotechnical legal problems are imagined and shaped ("issue spotting" practices) and how they are answered by scholars. This article explores the change in American privacy law scholars' techno-legal imaginaries in the last thirty years, as they transitioned from studying the privacy risks of computers and networks to the risks associated with artificial intelligence (AI) and algorithmic decision-making systems.

Conceptually, the article builds on the Science, Technology, and Social Studies (STS) literature about "sociotechnical imaginaries" and the "sociology of expectations," joins the body of literature addressing the possible interactions between law and imagination, and expects to contribute to nascent legal scholarship about the Legal Construction of Technology. Empirically, it relies on document analysis of American privacy law scholars' scholarship and oral history interviews with a purposely drawn representative sample of them.

The results of this research show that back in the late 1990s, American privacy law scholars aimed for a pluralist, free, democratic society that promoted liberty, autonomy, and self-determination and empowered citizens to take control of their own data. In the wake of AI and algorithmic decision-making systems, however, their visions of a desirable future have radically changed. Nowadays, most American privacy law scholars envision a society that cares about social equality, justice, and fairness. They expect legal interventions to defend the vulnerable and marginalized, protect citizens against data extraction and its consequent power asymmetries, hold corporate power accountable, and promote trust in the digital environment.

It is through understanding these different normatively loaded visions of the future that we can better comprehend why, instead of the enforcement of the Fair Information Practices Principles (FIPs), American privacy law scholars are now proposing substantive, top-down interventions (e.g., the establishment of permissible and unacceptable uses of data) to rein in the data extraction economy.

INTRODUCTION

In the last thirty years, American privacy law scholars have written extensively about emerging technologies. From the emergence of personal computers and networks to the popularization of artificial intelligence ("AI") and algorithmic decision-making systems, their scholarship has covered a broad range of topics. Mostly through academic papers, scholars examine how these technologies pose sociotechnical legal problems and the different ways in which the legal system should respond to them. These papers, however, provide more than a mere analysis of potential legal avenues in the digital age: they represent an extraordinary combination of scholarship and discourse. They sketch the visions of the privacy legal scholars' community about the desirable futures that could be achieved through the regulation of technoscientific innovation.

These visions, here referred to as "techno-legal imaginaries," have the power to shape how sociotechnical legal problems are imagined and shaped ("issue spotting") and how they are answered in a given legal community. In that sense, they are one of the many possible reasons why legal scholars' regulatory approaches to information privacy have changed over time.

This Article portrays a longitudinal study of American privacy law scholarship over the last thirty years, looking to unravel the evolution of the scholars' techno-legal imaginaries over time. The key findings suggest that over the years, scholars have moved from envisioning a pluralist, democratic society that promotes liberty, autonomy, and self-determination and empowers citizens to take control of their own data; to picturing a society that besides being democratic, also guarantees social equality, justice, and fairness. A society, where the vulnerable and marginalized are protected from data extraction and its consequent power asymmetries, and where corporate power is held accountable.

To conduct this research, I have selected the papers presented at the Privacy Law Scholars Conference (PLSC) as my main object of study. PLSC is an annual paper workshop conference that has been taking place in the United States since 2008, annually assembling a wide array of privacy law scholars and practitioners who engage in scholarship related to information privacy law. However, given that this project intends to cover thirty years, I have conducted *document analysis* of (1) the papers presented at PLSC between 2008 and 2022;[1] and (2) the law review articles cited in that first set of papers and published between 1992 and 2007. Importantly, I was especially interested in analyzing articles focused on information privacy and the conceptualization of privacy more broadly, and largely avoided studying

[1] From them, I have specifically reviewed those that ended up being published either as a paper or a book chapter, or are available as drafts (*e.g.*, accessible on SSRN).

papers on the Fifth Amendment, the Fourth Amendment, government surveillance, intellectual property, the right to publicity, and decisional privacy. Likewise, when necessary, I have included additional articles that, while not presented at PLSC, were authored by the presenters there and provide a more comprehensive picture of their regulatory approaches and theoretical stances. Finally, in addition to the document analysis I have also conducted a series of *oral history interviews* with a representative sample of American privacy law scholars who authored those papers.

The Article is organized as follows. First, I introduce readers to the concept of "techno-legal imaginaries," its theoretical roots, related concepts, and importance for the field of Law & Technology. Second, I briefly summarize how American privacy law scholars' regulatory approaches to information privacy have changed in the last thirty years.[2] Having set the regulatory scene, Parts IV and V of the Article describe the techno-legal imaginaries that underlay the initial regulatory approaches of scholars thirty years ago, as well as those that seem to be driving current proposals. For this purpose, I analyze both the most popular techno-legal narratives and the visions of desirable futures of each era.

II. TECHNO-LEGAL IMAGINARIES: A THEORETICAL FRAMEWORK

In this Article, my object of study is 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 technoscientific innovation.

As other types of imaginaries, the concept of techno-legal imaginaries opens 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). And, when it comes to the techno-legal imaginaries in particular, studying them offers a possible avenue to investigate how the relationship between law and technology is socially shaped by legal actors.

[2] For a detailed explanation of this change and its possible drivers and implications, *see* María P. Angel, *Privacy's Algorithmic Turn* (forthcoming) (on file with author).

A. Theoretical roots

The notion of "techno-legal imaginaries" has a number of theoretical roots. It builds on the concepts of imaginaries, expectations, visions, and promises proposed in Science, Technology and Society (STS) literature that addresses the possible interactions between futures and technology. In particular, it draws on elements from the literature on "technoscientific imaginaries" (Marcus, 1995), "sociotechnical imaginaries" (Jasanoff & Kim, 2009; 2015), and the sociology of expectations (Van Lente & Rip, 1998; Brown & Michael, 2003; Borup, Brown, Konrad & Van Lente, 2006; Konrad at al. 2016; Konrad & Böhle, 2019).

As in George E. Marcus's "technoscientific imaginaries," the techno-legal imaginaries 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, and denote an evident faith in the potential of their corresponding work activity. Similar to Sheila Jasanoff and Sang-Hyun Kim's "sociotechnical imaginaries," the techno-legal imaginaries are mainly composed of visions of desired future realities. Additionally, they are also temporally situated and culturally particular. In that sense, they tend to be different among different social groups, evolve over time, and can be compared and contrasted among different legal communities.

However, 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, 2015, 4). Rather, they are underlaid by shared understandings of forms of social life and social order attainable *through rule-making* (understood in the broadest way, through law, social norms, the market, and architecture) (Reidenberg, 1997; Lessig, 1999). Likewise, in contrast to the "sociotechnical imaginaries," the techno-legal imaginaries are not necessarily involved in practices of state-making or national governance of innovation processes, and therefore, they are not always "collectively held, institutionally stabilized, and publicly performed" (Jasanoff, 2015, 4).

In that sense, the techno-legal imaginaries are closer to the future-oriented representations (technological expectations, promises, and visions) 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. Rather, they 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" (Borup, Brown, Konrad & Van Lente, 2006, 286). Thus, in order to be recognized as such, these visions of the future don't necessarily need to

occupy a dominant position for policy purposes, but simply exist in the minds of individuals 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," which have been defined in that field 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). 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, 194).

B. Related concepts

Evidently, I am not the first scholar to explore the imaginative capacities of legal actors. The body of literature that addresses the possible interactions between law and imagination includes work from Jack M. Balkin & Reva B. Siegel (2006), Kieran Tranter (2011), Daniel Susser (2022), and Kjetil Rommetveit & Niels van Dijk (2022), among others.[3]

Balkin & Siegel (2006), for example, propose 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, 928). In that sense, they 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).[4]

When it comes to the imagination of *the future*, law scholar Kieran Tranter (2011) has written 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

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

[4] Margot Kaminski has built on Balkin & Siegel's concept to offer one of the possible ways in which technology disrupts the law. In Kaminski's view,

> technology (or really, the social use of technology) can alter the imagined setting around which policy conversations take place —what Jack Balkin and Reva Siegal call the "imagined regulatory scene." Sociotechnical change can alter the imagined regulatory scene's architecture, upsetting a policy balance and undermining a particular regulation or regime's goals. (Kaminski, 2022, 883).

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." (Tranter, 2011, 817).

Relatedly, philosopher Daniel Susser (2022) has addressed the "sociotechnical imaginaries" of privacy and surveillance scholars. 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, 300).

Finally, Rommetveit & van Dijk (2022) talk 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, 856). Thus, it includes a vision of law and technology as interchangeable instruments to achieve privacy regulatory goals and is at the base of techno-regulation (and techno-solutionism).

Unlike these theoretical terms, the concept of techno-legal imaginaries does not focus on the visions of what *technology* can do to or for society. Rather, its focus is on the desirable futures that legal actors expect *legal regulation of technology* to achieve. However, same as all of them, the concept of techno-legal imaginaries makes evident the multiple ways in which the "legal" interacts and becomes entangled with a great variety of sociotechnical factors. In that sense, these concepts all contribute to what law and STS scholar Meg Leta Jones (2018) has coined as the "Legal Construction of Technology" (LCT) theory or "techno-legal construction."

According to Jones, "[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. 281). As part of this theoretical approach, Balkin (2015) has argued that "[t]he characteristics of a new technology, in short, are partly the product of current use and partly the work of human imagination about potential affordances and opportunities, dangers and threats." (p. 47). In a similar vein, Margot Kaminski (2017) has also highlighted the importance of considering the legal context and the process of legal construction of technology. In Kaminski's words, "we should identify and analyze how the law constructs technology, rather than yielding to a narrative that a technology is intrinsically disruptive" (p. 593).

The significance of the LCT approach lies in the fact that it foregrounds

how the characteristics of a given technology are not the only aspects that should be considered when analyzing a given change in tech-related law. Rather, the interplay of the social, the technical, the legal, and—as I hope to demonstrate here—the cognitive, should also be explored.

C. Importance

In general, imaginaries are patterns of thought that are collectively held by a community (McNeil et al., 2016). Most often, they are embedded in the sociotechnical phenomenon that is being investigated and contain the "deeper normative notions and images" (Taylor, 2004, 23) that the members of that community operate on. In the case of techno-legal imaginaries, these imaginaries are usually implanted in legal communities' regulatory discussions about tech policy, and reveal the ideological and normative commitments underpinning different legal proposals.

One of the most important characteristics of imaginaries is their performative character: the way they are brought into being and have an influence on wider social processes. As Lukas Schlogl, Elias Weiss, and Barbara Prainsack aptly explain, imaginaries 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). In that sense, they are sometimes referred to as practices of *imagineering* (Suitner 2015), that is, the processes of simultaneously imagining and engineering reality.

When it comes to imaginaries about technology, studying their performativity entails understanding "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, van Lente, Groves, and Selin, 2016, 468). With regards to techno-legal imaginaries, their performative character can be seen in the power they have to shape how sociotechnical legal problems are imagined and shaped and how they are answered in different legal communities.

When using anticipatory practices to study techno-legal imaginaries, it is key to take into account that "[t]hese practices show different kinds of performativity, understood as the process by which statements and their world are co-produced" (Alvial-Palavicino & Konrad, 2018, 200). For instance, law review articles, as the main anticipatory practices reviewed in this Article, may have a less mobilizing function in comparison to white papers or policy documents produced by policymakers. In any case, all anticipatory practices include "narrative infrastructuring work" (Sepehr &

Felt, 2023) that allows us to explore the normative commitments of the legal communities in charge of crafting them.

Thus, before proceeding to our case study, it is important to remember that the 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, 462). As such, studying them allows us to shed light on and make explicit the ideological and normative underpinnings of tech policy work. They serve as a theoretical lens to make better sense of the ideas and regulatory proposals of legal actors—such as privacy law scholars—involved in the tech policy sphere. And, when examined over time—as it is the case in this Article—, they are also useful for interpreting change in legal reasoning.

III. The Transformation of American Privacy Law Scholars' Regulatory Approaches to Information Privacy

In the early 1990s, American privacy law scholars witnessed at least two important advances in digital technologies: the transition from mainframe computers to personal computers, and the "shift from the use of 'stand-alone' computers to networked systems, integrating hundreds of terminals" (Rodríguez, 1998, 1440). These networked systems, which would be more and more referred to as the Internet (Hardy, 1994; Long II, 1994; Froomkin, 1996; Schwartz, 1999), the Information Superhighway (Long II, 1994), or the Global Information Infrastructure ("GII") (Kang, 1998), attracted the interest of a big portion of American privacy law scholars, who started to write extensively about them.

As a result of the—for the time—sophisticated information-processing capabilities of personal computers, the emerging possibility to have "real-time access to data and information services across borders" (Reidenberg & Gamet-Pol, 1995, 107), and the fact that the architecture of cyberspace allowed data to be "collected ceaselessly-invisibly, behind the scenes, efficiently, with no burden on the user" (Lessig, 1999a, 62), many scholars started to worry about the increased volume of personal information that was now available to public and private entities. Likewise, the fact that individuals were now subject to real-time, detailed, cumulative, invisible, automatic, continuous, omnipresent, and pervasive observation—referred by many of the scholars as surveillance—was also a cause for concern in legal academia. Finally, law scholars would call attention on how the accumulation, compilation, and aggregation of data into profiles could not only allow private and public entities to learn—and infer—much more about the private lives of individuals, but also generate "a spate of dire predictions" (Reidenberg & Gamet-Pol, 1995, 121-122).

For those reasons, as early as 1992 privacy scholars would talk about the need to abandon industry self-regulation. 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" (Reidenberg, 1992, 208-209; 1995; 1999).

As an alternative, a considerable portion of American privacy law scholars started calling for the mandatory implementation of the Fair Information Practices ("FIPs"). [5] The FIPs are a set of principles or standards for data collection and processing which were initially proposed by the U.S. Department of Health, Education and Welfare in 1973 and later included in a set of voluntary guidelines adopted by the Organization for Economic Cooperation and Development (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 of 1988).

Therefore, the goal of the scholars writing about personal computers and networks at the time was to finally make them nationally binding and mandatory. Nevertheless, approaches on how to make that possible were diverse. On the one hand, several scholars would encourage Congress to pass a comprehensive federal privacy law "structuring transparent data processing systems; granting limited procedural and substantive rights to the data subject; and creating independent governmental monitoring of data processing systems" (Schwartz, 1992, 1325).

The main objective that most of the scholars had in mind for this law was to "shift the protection of privacy toward individual control over information" (Bezanson, 1992, 1151). How so? Mainly, by granting individuals affirmative rights such as to receive notice when their data is collected, be informed about how the data holder will use the data obtained, have access to records about them, and have procedural mechanisms to correct errors in the information collected. Such rights, Robert G. Boehmer would claim, "might be labeled 'due process in the private sector'" (Boehmer, 1992, 813).

[5] To be fair, not every privacy law scholar writing during this epoch would agree with this approach. For example, a few of the scholars reviewed for this research would call for maintaining the prevalent self-regulation approach (Greenberg, 1994; Miller & Poe, 1996; White, 1997; Killingsworth, 1999). Scott Killingsworth (1999), 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. A few others 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 (Bezanson, 1992; Harvey, 1992; McClurg, 1995; Kim, 1996; Jurata, 1999). Finally, another selected group would opt for a market solution based on property-rights and contract law (Bibas, 1994; Shorr, 1995; Murphy, 1996; Kang, 1998; Lessig, 1999a, 1999b).

"What our government can do," argued Lawrence Gostin in 1995, "is create fair, comprehensive rules, applicable throughout the United States, to ensure that information is acquired, used, and disseminated according to clearly understood criteria and procedures, under mandated security arrangements" (Gostin, 1995, 517). Similarly, in 1999 Anita Allen would state: "It may also be a matter of regulating the corporate sector more aggressively, *requiring fair information practices* that give employees and consumers greater control over what information is collected and how it is used" (Allen, 1999a, 756).

According to Schwartz, "these elements must be set forth in 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, 1375). In fact, the latter was the case, for example, of privacy in the workplace. Since the early 1992, scholars would call for Congress to "draft affirmative legislation which grants employees specific rights" (Bindler, 1992, 881).[6] Likewise, in the case of genetic privacy, some scholars would call for statutory language that would regulate the collection, storage, and disclosure of genetic information (Annas, 1999).

On the other hand, another big portion of scholars would show skepticism about the ability of the law, by itself, to protect privacy on the Internet and in electronic commerce.[7] Therefore, they would propose what would be coined by Joel Reidenberg (1997) and Lawrence Lessig (1999) as "Lex Informatica" or "law as code:" to take advantage of the rule-making power of technology

[6] *See also* Boehmer, 1992, 751 ("we need to consider comprehensive workplace privacy legislation encompassing all of these techniques."); Baxi & Nickel, 1994, 145 ("There is a definite need for some regulation of electronic monitoring in the workplace given that these fundamental employee rights are not currently safeguarded by legislation.); Flanagan, 1994, 1274 ("To replace the current amorphous legal standards, Congress should announce a national policy addressing an employer's ability to monitor employees and an employee's countervailing right to privacy in the workplace."); Pincus & Trotter, 1995, 84 (proposing a "Federal Act for Employee Privacy Protection, applicable to both public and private sector employees").

[7] 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. (Froomkin, 1996, 490-491).

and implement the Fair Information Practices (FIPs) through code. Thus, instead of the law, the technology would be the one providing individuals with control over their personal data.

According to Michael Froomkin (1996), "[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." (p. 491). Similarly, in 1997 Reidenberg would highlight how "several technical solutions provide *valuable tools to establish fair information practice policy on global networks*" (p. 562). And, in a similar tone, in 1999 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.* (Cate, 1999, 231).

However, as digital technologies have developed, the regulatory approaches proposed by American privacy law scholars have also evolved. During the last few years, new technologies—such as artificial intelligence (AI) and algorithmic decision-making systems— have taken over society. As I describe in detail in *Privacy's Algorithmic Turn*, against the backdrop of these new technologies, American privacy law scholars have started to express novel concerns about massive data collection and processing. In particular, a big portion of American privacy scholars writing in these days worry about the discrimination (unfairness), algorithmic manipulation, procedural injustices, subordination, and economic exploitation that the use of these emerging technologies can create (Angel, forthcoming).

As a result, a big portion of American privacy law scholars have begun to reject the FIPs, describing them as insufficient (Nissenbaum, 2015; Hartzog & Richards, 2020; Waldman, 2021; Richards & Hartzog, 2020a; Allen, 2022a; Solove, 2023).[8] In particular, in the last few years, several scholars have started to question the effectiveness of the individual privacy

[8] As I explain in detail in *Privacy's Algorithmic Turn* (Angel, forthcoming) (in file with author), this process has gone through two different phases. During Phase I, scholars grappled with options to either modify the FIPs or complement them. Phase II, which has begun just recently, has seen a complete rejection of individual rights and a shift to substantive top-down rules. For the purpose of this article, I will concentrate here on the most recent Phase, which may be still in flux.

rights. As Margot Kaminski aptly describes in a 2022 article, "just as lawmakers in the United States have started to establish basic data privacy rights recognized the world over, the bulk of privacy law scholarship has conceded that these rights, or their close analogues, are useless" (Kaminski, 2022a, p. 385).

As an alternative, a considerable portion of scholars has started to advocate for substantive, top-down rules that instead of giving control to individuals to protect their own personal information, put in the government's hands the responsibility of protecting individuals—and groups—from data-exploitation activities (Hartzog, 2018; Hirsh, 2020; Hartzog & Richards, 2020; Bamberger & Mays, 2021; Richards & Hartzog, 2021a; Cohen, 2021; Waldman, 2021). In 2020, for example, Dennis D. Hirsch stated: "if privacy law is to offer meaningful protection, it must shift from a liberalist focus on individual control, to *a social protection model* in which public authorities set *substantive standards* that defend people against algorithmic threats" (Hirsch, 2020, 439). As Hirsch, the regulatory approach proposed by many other scholars is now focused on substantive rules and prohibitions rather than simply procedural requirements.

As an example, a quote from Neil Richards and Woodrow Hartzog might better illuminate this point:

> We think a relational turn for data protection would be superior to the current model, even of the GDPR, which is still FIPs-based in its bones. A relational turn would provide a path towards *more substantive rules that would limit how peoples' data could be used against them.* It would focus on the real problem that privacy and data protection law should tackle – the power consequences of information relationships, making legitimacy of processing a question of fundamental fairness rather than data hygiene. *Substantive data rules* would demand more than that data serve a 'legitimate interest' of the data processor. They would focus on the power consequences of processing on the data subject, whether we apply some version of the classic fiduciary duties of care, confidentiality, and loyalty, or the trust-promoting duties of honesty, protection, discretion, and loyalty that we have called for in other work (Richards & Hartzog, 2021a, 5).

Even earlier, in 2018 Hartzog alone had started to put forward this view. According to him,

> Lawmakers have more direct options. *Prohibit collection outright. Mandate deletion.* Get serious with purpose limitations

> and the concept of 'legitimate interest.' Change the nature of the relationship between users and companies entrusted with their data to one that is fiduciary in nature. Mandate non-delegable duties of loyalty, care, and honesty. In other words, because it is virtually impossible for people to be adequately informed of data risks and exert control at scale, *our rules should make sure companies cannot unreasonably favour their own interests at our expense.*
>
> The case against privacy control is an appeal to *more substantive and effective privacy-related values.* By expanding beyond the notion of privacy as control, lawmakers would be freed to *create some rules to ensure companies are trustworthy regardless of the control we are given* (Hartzog, 2018, 432).

Thus, instead of individual privacy rights, a considerable portion of American privacy law scholars are now asking the government to put in place clear, binding rules about what companies can and can't do with regards to the collection and processing of personal data.

IV. The Techno-legal Imaginary of American Privacy Law Scholars in the Era of Personal Computers and Networks

As Jascha Bareis and Christian Katzenbach aptly claim for the case of technological imaginaries articulated in national AI strategy papers, "looking at technology narratives serves as a means to look into desired futures, informing us about societal strivings and aspirations" (2022, 860). In a similar way, looking at techno-legal narratives can provide a glimpse into the visions of desirable futures that concern us here. For that reason, in this Part I will firstly portray the common *narratives* identified in my analysis of the privacy law scholarship written around personal computers and networks. Thereafter, I will briefly sketch the resulting vision of desirable future, as a projection of a social, cultural, and technological order enabled by information privacy regulation.

A. Narratives

1. Privacy as necessary for individual autonomy

As a first step of the narrative construction of the techno-legal imaginary, multiple manifestations in the scholarship published around personal computers and networks present privacy as an indispensable condition for

individual autonomy.

To set the stage, several American privacy law scholars situate privacy in the context of liberal individualism. According to M.J. van den Hoven, "[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, 36).

In that sense, in 1999 Anita Allen alerted that "numerous little consensual and nonconsensual privacy loses, too trivial to protest individually, aggregate into a large privacy loss that is a detriment to *the liberal way of life*" (Allen, 1999, 540). What does this way of life entail? According to Jeffrey H. Reiman (1995),

> 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 (p. 42).

As seen, liberal individualism revolves around the autonomy of individuals, and their ability to make choices in ways that are un-coerced by institutions or organizations. Besides, it also concretizes in the idea of individual control. In fact, Scott Shorr (1995) refers to those two elements as "the decisional and control dimensions of personal autonomy" (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 (p. 1768-1769).

In a similar tone, but referring solely to the former dimension, in 1992

Paul Schwartz defined autonomy as "the ability to make decisions and to act on these decisions through participation in social and political life" (Schwartz, 1992, 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 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" (Schwartz, 1995, 560). In that sense, information privacy was considered by him to allow individuals' self-government.

Furthermore, 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 form their own views and convictions. For example, in 2000 Julie Cohen would ague how ""privacy fosters (partial) self-determination. It enables individuals both to maintain relational ties and to develop critical perspectives on the world around them" (Cohen, 2000, 1906).

In the same way, the flip side of the coin is that surveillance risks eroding 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, according to Schwartz (1992),

> 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 (p. 1374).

At first sight, privacy seems to be depicted by several scholars of this period as a liberal, individualistic value. However, there is a second narrative that goes along this approach, to which I turn now.

2. Privacy as a social value

In the rhetorical construction of privacy as a necessary condition for individual autonomy, American privacy law scholars of the time would go even further: They would establish an interdependent connection between individual autonomy and certain collective benefits. "[A]utonomy matters for both the individual and society" (p. 1350), Schwartz would argue in 1992.

This creates a powerful rhetorical triangle that sheds 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" (p. 36).

Thus, under this narrative privacy is framed as a precondition for collective benefits such as democracy, creativity, and freedom. As mentioned earlier, in 1995 Paul Schwartz argued 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 (Schwartz, 1999, 561).

Likewise, inspired by Robert Post and anchored on civic republican theory, in 1999 Schwartz would proclaim: "information privacy is best conceived of as a constitutive element of civil society" (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'" (Schwartz, 1999, 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" (Schwartz, 2004, 2128). Thus, for Schwartz, the autonomy that information privacy allows is, in turn, a precondition for a deliberative democracy.

Similarly, in 2000 Julie Cohen stated: "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*" (Cohen, 2000, 1423). Regarding the types of collective ends it fosters, Cohen added: "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." (p.

1426). For her, autonomy generates concrete collective benefits such as democratic participation.

Later on, in her renown article *What Privacy is For* she would stress: "privacy does not only protect individuals. Privacy furthers fundamental public policy goals relating to liberal democratic citizenship, innovation, and human flourishing" (Cohen, 2001, 1928). In her view, the development of subjectivity that privacy enables also promotes innovative practices.

Another worth-citing example comes from Jeffrey H. Reiman, for whom "privacy is essential to a free society" (1995, 30). According to Reiman,

> 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" (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*" (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*" (1999a, 19).

As seen, privacy is portrayed by these scholars as of pivotal importance for democracy, innovation, and freedom. Through these collective benefits, information privacy receives the status of a social value that has to be fostered and protected for the sake of society.

B. Resulting vision of desirable future

The aforementioned narratives undergird the vision of a pluralistic, free, and democratic society where autonomous individuals thrive.

First, this techno-legal imaginary includes a society in which individuals are protected from coercive choices about how to live their lives. Based on a "fear of control of thought and social interaction" (Reidenberg, 1995, 537), this desired order is one where "protecting citizens against thought manipulation and abuses of power" (Reidenberg, 1995, 541) is a priority. In line with this vision, in 2000 Julie Cohen emphasized: "there are compelling

theoretical and practical justifications for legislating strong data privacy protection that creates and preserves *a zone of informational autonomy for individuals*" (p. 1428).

Furthermore, the desirable future sustained by these narratives also includes a society that "values and thrives on the diversity of its citizenry" (Boehmer, 1992, 771). Due to the protection of their individual autonomy, "individuals will develop their individual and unique characteristics" (Boehmer, 1992, 771). As a result, scholars envision the emergence of a pluralistic community of individuals who are free to grow and develop in different ways, and who are therefore able to create and innovate as they wish, without any external influence.

Finally, the desired order is a democratic one. Individual autonomy also allows for participation in the spheres of social and political life. In that sense, in this desired order individuals are "free from state or community intimidation that would destroy their involvement in the democratic life of the community" (Schwartz, 1995, 561). Describing this trend in privacy scholarship, which they noticed in 2003, Paul Schwartz & William Michael Treanor 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*" (Schwartz & Treanor, 2003, 2184).

V. The Techno-legal Imaginary of American Privacy Law Scholars in the Era of Artificial Intelligence and Algorithmic Decision-Making Systems

A. Narratives

Similar to Part IV, in this Part I will start by describing the common narratives that emerged from my analysis of the privacy law scholarship written around AI and algorithmic decision-making systems. Following this, I will briefly sketch the resulting vision of desirable future that appears to be guiding an important portion of American privacy law scholarship today.

1. Privacy as a necessary element of human flourishing

In this new era, information privacy is not only a necessary precondition for individual autonomy. As the narrative goes, privacy is indispensable for the realization of the person as a whole. In that sense, what privacy allows individuals to archive goes well beyond self-determination. For instance, Ari E. Waldman envisions: "[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" (Waldman, 2021a, p. 53).

Relatedly, in recent years, Woodrow Hartzog & Neil Richards have also stressed, both together and independently, that:

> 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).

And, in a draft paper presented in the 2022 PLSC, Neil Richards alone similarly points out:

> we should think about privacy in terms of the rules that shape the exercise of that power in (ideally) socially-beneficial directions *to promote human flourishing.* As a result, privacy should be seen as an instrumental value that gets us other things, and *we should try to craft our privacy rules to promote those human values – such as authentic identity formation, democratic political freedom, robust consumer protection, a trustworthy set of social institutions, and human equality*. (p. 4).

In a similar way, in a 2021 article Kenneth A. Bamberger & Ariel Evan Mayse invite their readers to consider "Jewish law's understanding of privacy as a societal value protected by multilateral obligations rather than individual rights, . . . and *its commitment to use societal behavior to protect, in a universal way, the privacy of each individual, and the ability of those individuals to flourish, grow and evolve as humans*" (p. 7).

As such, privacy has turned up to be considered an integral part of well-being. It is depicted as a big umbrella that can welcome and protect a broad range of values. "Properly understood," Hartzog and Richards add in a 2021 article, "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" (Richards & Hartzog, 2021a, 4).

2. Privacy law as an effective means to upset power asymmetries

For years, American privacy law scholars have claimed that privacy is

about power. As early as 1995, for example, when addressing the issue of workplace privacy Larry O. Natt Gantt (1995) stated: "[t]hese new monitoring technologies have intensified employee privacy concerns because the instruments *abolish the desirable balance of power* between employers and employees" (p. 346). Similarly, in 1996 Michael Froomkin noted: "in an imperfect market profiling *threatens to change the balance of power* between consumers and sellers" (Froomkin, 1996, 480). Likewise, at the turn of the century Paul Schwartz (2000) would also argue that "[i]n the absence of effective limits, legal or otherwise, on the collection and use of personal information on the Internet, *a new structure of power over individuals* is emerging" (p. 815). And in 2001 Daniel Solove (2001) would emphasize that "the problem with databases and the practices currently associated with them is that *they disempower people.* They make people vulnerable by stripping them of control over their personal information" (p. 1423).

In that sense, it is not new 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. Currently, scholars believe that privacy law could be more effective in upsetting power imbalances resulting from data exploitation.

In accordance with the narrative, it is not enough to give individuals control over their personal information. As Julie Cohen (2021) states, "[i]ndividual users asserting preferences over predefined options on modular dashboards have neither the authority nor the ability to *alter the invisible, predesigned webs of technical and economic arrangements under which their data travels among multiple parties*" (p. 5). In a similar way, Daniel Solove (2023) recently made clear:

> Rights cannot empower individuals enough to equalize the power imbalance between individuals and the organizations that collect and use their data. Effective privacy protection involves not just facilitating individual control but also *bringing the collection, processing, and transfer of personal data under control*. These two forms of control – individuals having control and the data ecosystem being under control – are very different, but they are often conflated in privacy policymaking. Individual control is important, but it is only achievable in a limited way. The more practical and effective aim is to *bring the data ecosystem under better control* (p. 6).

Thus, according to the new narrative privacy law can be used to actually intervene power imbalances. As argued by Rachel Wilka, "a new

system must not just create a consumer right but also balance the inequities in bargaining power between a consumer and a large corporation" (Wilka, 2018, 63). Relatedly, when I asked Woodrow Hartzog about his desirable future in relation to information privacy, part of the answer he gave me during his oral history interview was:

> "One *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*" (Oral interview with Woodrow Hartzog, February 2023).

How can information privacy law possibly achieve this? In her oral history interview Anita Allen told me that "[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 with Anita Allen, March 2023). In a similar fashion, Ari E. Waldman believes that, in order to rein in information industry power, privacy law should restructure the data-extractive business model and redistribute power to the rest of us. In his words, "privacy scholars and policymakers should look beyond the narrow confines of what passes for privacy regulation in the U.S. and consider new legal paradigms that can rein in data extraction and its attendant power asymmetries and injustices" (Waldman, 2021, 41). In that sense, information privacy law should provide "not just stronger privacy protections, but also an end to the information economy's role in perpetuating systemic injustices" (Waldman, 2021, 42).

Similarly, Hartzog & Richards (2021) consider that "[r]ather than treating all kinds of information relationships as equal and fungible," privacy law should "increase 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" (p. 10).

3. Privacy as an anti-oppression legal tool

In the rhetorical construction of privacy as a tool to intervene power imbalances, oppression plays a big role. The use of AI and algorithmic decision-making systems unequally affects certain social groups. In particular, data exploitation practices are said to reinforce racial, sexual, and similar social hierarchies. Likewise, it is acknowledged that data can contribute to oppress marginalized populations and to subordinate them,

"whether it is used to train totalitarian facial recognition models, surveil protestors, send people to jail, or subjugate vulnerable populations" (Waldman, 2021, 43). Moreover, they tend to be disproportionally targeted and impacted by state and private surveillance regimes. As Daniel Solove (2023) and many other acknowledge, "[t]here are larger societal problems caused or worsened by certain uses of personal data, such as discrimination as well as subordination of minority groups and the poor" (Solove, 2023, p. 14).

Consequently, in this last narrative information privacy is portrayed as a legal tool to protect the marginalized and vulnerable from oppression and subordination, and therefore, promote equality and justice. For example, in his book *Privacy at the Margins*, Scott Skinner-Thompson argues 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" (Skinner-Thompson, 2020, 6). More specifically, Anita Allen has claimed that "[t]he new generation of laws would ideally include provisions specifically geared toward *combatting privacy- and data-protection-related racial inequalities enabled by online platforms*" (Allen, 2022a, 910). 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 (p. 1273).

In fact, in the oral history interview conducted with Waldman in November 2023, he stressed:

> one of the best angles to getting people more engaged to build awareness, build what a Marxist would call "popular consciousness" about your oppression is that *we connect privacy*

> *to the, um, to the missions of every single civil rights organization in the country*. Right? There is no reason why the NAACP Legal Defense Fund to the Human Rights Campaign to whatever, any civil rights organization, *every civil rights organization should also have a privacy, um, project focusing on the privacy interests of the particular community that they serve*. And with that you're going to start seeing far more interest and far more dynamic solutions coming out of the civil, out of the, out of civil society (Oral interview with Ari Waldman, November 2022).

Related to this narrative is the idea that privacy, as a rhetorical tool, can give voice to marginalized populations, helping them to break free from oppressive practices. Adopting a "critical definitional facilitation" approach, for example, Anita Allen draws attention to "the political and urgent nature of privacy discourse in contemporary life" (Allen, 2022 forthcoming). According to Allen,

> "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 interview with Anita Allen, March 2023).

B. Resulting vision of desirable future

These narratives underpin a vision of a socially-just society where corporate power is held accountable and individuals—especially vulnerable ones—are protected and empowered to fully exercise their rights in the digital environment.

To begin with, the desirable future envisioned today by a big portion of American privacy law scholars is a society that cares about social equality, justice, and fairness. Therefore, it makes a special effort to protect marginalized groups, including minorities (e.g., racial, religious, sexual, etc.) and socioeconomically vulnerable individuals. 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, 182). 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" (Citron & Solove, 2022, 855).

Second, this envisioned society holds "the information economy . . . accountable 'to those who live' within it" (Citron & Solove, 2022, 855). In this envisioned reality, regulators work "on behalf of individuals to counter corporate power" (Waldman, 2021a, 1275). As mentioned by Ari Waldman in his oral history interview,

> [t]he future that I want is an economy that's not based on, uh, profiting from data extraction. . . . the better world that we need is a world that is, um, driven by, driven by people, so, democratic. Um, and it is not the, it is, it is without the presumption that access depends, access and benefits depend on extracting or giving up your data (Oral interview with Ari Waldman, November 2022).

In practice, this future entails, among other things, "redistribut[ing] power away from the information industry by facilitating critical research about data-extractive technologies" (Waldman, 2021a, 1275); "set[ting] boundaries and goals for technological design" (Hartzog, 2018, 7); "get[ting] 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" (Oral interview with Julie Cohen, February 2023); "giv[ing] advocacy organizations representing marginalized populations, and not corporations, a seat at the table" (Waldman, 2021a, 1277); 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" (Oral interview with Anita Allen, March 2023).

CONCLUSION

In this Article, I use document analysis and oral history interviews to study how the normative commitments of American privacy law scholars have changed over the last thirty years. Today, their envisioned future is less about autonomy and self-determination and more about social justice and reining in power imbalances.

Techno-legal imaginaries not only shape how a given techno-legal problem is framed, but also the types of measures and tools that legal actors choose from. Therefore, it is my hope that by understanding these different normatively loaded visions of the future of legal scholars, other actors in

computer science, law, social sciences, and humanities involved in the tech policy environment are now in a better position to comprehend why, instead of proposing the enforcement of the Fair Information Practices Principles (FIPs), American privacy law scholars are now recommending substantive, top-down interventions to curtail the data extraction economy (e.g., establishing permissible and unacceptable uses of data). In a world of increasing interdisciplinarity and multi-stakeholder discussions, having access to these insights contributes to better discussions, engagement, or contestation.

BIBLIOGRAPHY

Allen, Anita L. 1999. "Coercing Privacy." *William & Mary Law Review* 40(3): 723-757.

Allen, Anita L. 1999a. "Lying to Protect Privacy." Villanova Law Review 44(2): 161-187.

Allen, Anita L. 2022 forthcoming. "Privacy In Critical Definition and Racial Justice." In *Oxford Handbook of Applied Philosophy of Language*.

Allen, Anita L. 2022a. "Dismantling the 'Black Opticon': Privacy, Race, Equity, and Online Data-Protection Reform." *Yale Law Journal Forum*: 907-968.

Alvial-Palavicino, Carla & Kornelia Konrad. 2018. "The rise of graphene expectations: Anticipatory practices in emergent nanotechnologies." *Futures* 109: 192-202.

Angel, María P. (forthcoming). "Privacy's Algorithmic Turn." In file with author.

Annas, George J. 1999. "Genetic Privacy: There Ought to Be a Law." *Texas Review of Law & Politics* 4(1): 9-16.

Balkin, Jack. 2015. "The Path of Robotics Law." *California Law Review* 6: 45-60.

Balkin, Jack M. & Reva B. Siegel. 2006. "Principles, Practices, and Social Movements." *University of Pennsylvania Law Review* 154: 927-950.

Bamberger, Kenneth A. & Ariel Evan Mayse. 2021. “Pre-Modern Insights for Post-Modern Privacy: Jewish Law Lessons for the Big Data Age.” *Journal of Law and Religion* 36(3): 495–532.

Bareis, Jascha & Christian Katzenbach. 2022. “Talking AI Into Being: The Narratives and Imaginaries of National AI Strategies and their Performative Politics.” *Science, Technology, & Human Values* 47(5): 855-881.

Baxi, Shefali N. & Alisa A. Nickel. 1994. “Big Brother or Better Business: Striking Balance in the Workplace.” Kansas Journal of Law & Public Policy 4(1):137-150.

Bezanson, Randall P. 1992. “The Right to Privacy Revisited: Privacy, News, and Social Change, 1890-1990.” *California Law Review* 80(5): 1133-1175.

Bibas, Stephanos. 1994. “A Contractual Approach to Data Privacy.” *Harvard journal of Law & Public Policy* 17: 591-611.

Bindler, Susan Ellen. (1992). “Peek and Spy: A Proposal for Federal Regulation of Electronic Monitoring in the Work Place.” *Washington University Law Review* 70: 853-885.

Blanchette, Jean-François & Deborah G. Johnson. 2002. “Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness.” *The Information Society* 18(1): 33-45.

Boehmer, Robert 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, Mads, Nik Brown, Kornelia Konrad & Harro van Lente. 2006. “The sociology of expectations in science and technology.” *Technology Analysis and Strategic Management* 18: 285–298.

Brown, Nik & Mike Michael. 2003. “A Sociology of Expectations: Retrospecting Prospects and Prospecting Retrospects.” *Technology Analysis & Strategic Management* 15(1): 3–18.

Calo, Ryan. 2016. “Robots in American Law.” *University of Washington School of Law Research Paper* No. 2016-04.

Cate, Fred H. 1999. “The Changing Face of Privacy Protections in the

European Union and the United States." *Indiana Law Review* 33(1): 173-232.

Citron, Danielle K. & Daniel Solove. 2022. "Privacy Harms." *Boston University Law Review* 102: 793-863.

Cohen, Julie E. 2000. "Examined Lives: Informational Privacy and the Subject as Object." *Stanford Law Review* 52: 1373-1438.

Cohen, Julie E. 2001. "Privacy, Ideology, and Technology: A Response to Jeffrey Rosen." *Geo. L.J.* 89: 2029-2045.

Cohen, Julie E. 2021. "How (Not) to Write a Privacy Law." *Knight First Amendment Institute at Columbia University.*

Flanagan, Julie A. 1994. "Restricting Electronic Monitoring in the Private Workplace." *Duke Law Journal* 43(6): 1256-1281.

Froomkin, A. Michael. 1996. "Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases." Journal of Law & Commerce 15(2): 395-507.

Gostin, Lawrence O. 1995. "Health Information Privacy." 80 *Cornell Law Review* 80: 451-528.

Greenberg, Thomas R. 1994. "E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute." *American University Law Review* 44(1): 219-254.

Hardy, I. Trotter. 1994. "The Proper Legal Regime for Cyberspace." *University of Pittsburgh Law Review* 55(4): 993-1056.

Hartzog, Woodrow. 2018. "The Case Against Idealising Control." *EDPL* 4: 423-432.

Hartzog, Woodrow & Neil Richards. 2020. "Privacy's Constitutional Moment and the Limits of Data Protection." *Boston College Law Review* 61:1687-1761.

Hartzog, Woodrow & Neil Richards. 2021. "The Surprising Virtues of Data Loyalty." *Emory Law Journal* 71: 985-1033.

Harvey, G. Michael. "Confidentiality: A Measured Response to the Failure

of Privacy." *University of Pennsylvania Law Review* 140: 2385-2470.

Hirsch, Dennis D. (2020). "From Individual Control to Social Protection: New Paradigms for Privacy Law in The Age of Predictive Analytics." *Maryland Law Review* 79: 439-503.

Jasanoff, Sheila. 2015. "Future Imperfect: Science, Technology, and the Imaginations of Modernity." In *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power,* edited by Sheila Jasanoff & Sang-Hyun Kim,1-33. Chicago: University of Chicago Press.

Jasanoff, Sheila & Sang-Hyun Kim. 2009. "Containing the Atom: Sociotechnical Imaginaries and Nuclear Power in the United States and South Korea." *Minerva* 47: 119–146.

Jasanoff, Sheila & Sang-Hyun Kim (eds.). 2015. *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power.* Chicago: University of Chicago Press.

Jones, Meg L. 2018. "Does Technology Drive Law? The Dilemma of Technological Exceptionalism in Cyberlaw." *Journal of Law, Technology & Policy* 2018(2): 249-284.

Jurata, John A. Jr. 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, Margot E. 2017. "Authorship, Disrupted: AI Authors in Copyright and First Amendment Law." *U.C. Davis Law Review* 51(2): 589-616.

Kaminski, Margot E. 2022. "Technological 'Disruption' of the Law's Imagined Scene: Some Lessons from Lex Informatica." *Berkeley Technology Law Journal* 36: 883-914.

Kaminski, Margot E. 2022a. "The Case for Data Privacy Rights (Or, Please, A Little Optimism)." Notre Dame L. Rev. Reflection 97: 385-399.

Kang, Jerry. 1998. "Information Privacy in Cyberspace Transactions." *Stanford Law Review* 50: 1193-1294.

Killingsworth, Scott. 1999. "Minding Your own Business: Privacy Policies in Principle and in Practice." *Journal of Intellectual Property Law*, 7(1): 57-98.

Kim, Pauline T. 1996. "Privacy Rights, Public Policy, and the Employment Relationship." *Ohio State Law Journal* 57: 671-730.

Konrad, Kornelia, Harro van Lente, Christopher Groves, and Cynthia Selin. (2016). In *The Handbook of Science and Technology Studies*, edited by Ulrike Felt, et al. MIT Press.

Konrad, Kornelia & Knud Böhle. 2019. "Socio-technical futures and the governance of innovation processes—An introduction to the special issue." *Futures* 109: 101–107.

Lessig, Lawrence. 1999. *Code and Other Laws of Cyberspace*. New York: Basic Books.

Lessig, Lawrence. 1999a. "The Architecture of Privacy: Remaking Privacy in Cyberspace." *Vanderbilt Journal of Entertainment and Technology Law* 1: 56-65.

Lessig, Lawrence. 1999b. "The Law of the Horse: What Cyberlaw Might Teach." *Harvard Law Review* 113(2): 501-549.

Long, George P. III. 1994. "Who Are You: Identity and Anonymity in Cyberspace." *University of Pittsburgh Law Review* 55(4):1177-1214.

Marcus, George E. (ed). 1995. *Technoscientific Imaginaries: Conversations, Profiles, and Memoirs*. Chicago: University of Chicago Press.

McCartney, Donald R. 1994. "Electronic surveillance and the resulting loss of privacy in the workplace." *UMKC Law Review*, 62(4): 859-892.

McClurg, Andrew 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.

McNeil, Maureen, Michael Arribas-Ayllon, Joan Haran, Adrian Mackenzie & Richard Tutton. 2016. "Conceptualizing Imaginaries of Science, Technology, and Society" in *The handbook of science and technology studies*, Felt, U., Fouche, R., Miller, C. A., & Smith-Doerr, L. (Eds.) (MIT

Press).

Miller, Christopher S. and Brian D. Poe. 1996. “Employment Law Implications in the Control and Monitoring of E-mail Systems.” *U. Miami Bus. Law Review* 6(95): 95-118.

Murphy, Richard S. 1996. “Property Rights in Personal Information: An Economic Defense of Privacy.” *Georgetown Law Journal* 84(7): 2381-2418.

Natt Gantt, Larry O. 1995. “An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace.” *Harvard Journal of Law & Technology* 8(2): 345-425.

Nissenbaum, Helen. 1998. “Protecting Privacy in an Information Age: The Problem of Privacy in Public.” *Law and Philosophy* 17(5-6): 559-596.

Nissenbaum, Helen. 2015. “Respecting Context to Protect Privacy: Why Meaning Matters.” *Sci Eng Ethics*.

Pincus, Laura B. & Clayton Trotter. 1995. “The Disparity between Public and Private Sector Employee Privacy Protections: Call for Legitimate Privacy Rights for Private Sector Workers.” *American Business Law Journal* 33(1): 51-90.

Reidenberg, Joel R. 1992. “Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?” *Fed. Comm. L. J.* 44; 195- 243.

Reidenberg, Joel R. 1995. “Setting standards for fair information practice in the U.S. private sector.” *Iowa Law Review* 80(3): 497-552.

Reidenberg, Joel R. 1997. “Lex Informatica: The Formulation of Information Policy Rules through Technology.” *Texas Law Review* 76(3): 553-593.

Reidenberg, Joel R. 1999. “Restoring Americans’ Privacy in Electronic Commerce.” *Berkeley Technology Law Journal* 14(2): 771-792.

Reidenberg, Joel R. & Franqois Gamet-Pol. 1995. “The Fundamental Role of Privacy and Confidence in the Network.” *Wake Forest Law Review* 30: 105-125.

Reiman, Jeffrey H. 1995. “Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the

Future." *Santa Clara High Technology Law Journal* 11: 27-44.

Richards, Neil and Woodrow Hartzog. 2021a. "A Relational Turn for Data Protection?" *EDPL* 4: 1-6.

Rodríguez, Alexander. 1998. All bark, no byte: employee e-mail privacy rights in the private sector workplace. *Emory Law Journal* 47(4): 1439-1474.

Rommetveit, Kjetil & Niels van Dijk. 2022. "Privacy engineering and the techno-regulatory imaginary." *Social Studies of Science* 52(6): 853–877.

Schlogl, Lukas, Elias Weiss, & Barbara Prainsack. 2021. "Constructing the 'Future of Work': An analysis of the policy discourse." *New Technology, Work and Employment* 36: 307-326.

Schwartz, Paul M. 1992. "Data Processing and Government Administration: The Failure of the American Legal Response to the Computer." *Hastings law Journal* 43: 1321-1388.

Schwartz, Paul M. 1995. "Privacy and Participation: Personal Information and Public Sector Regulation in the United States." *Iowa Law Review* 80(3): 553-618.

Schwartz, Paul M. 1999. "Privacy and Democracy in Cyberspace." *Vanderbilt Law Review* 52: 1609-1701.

Schwartz, Paul M. 2000. "Internet Privacy and the State." *Connecticut Law Review* 32: 815-859.

Schwartz, Paul M. 2004. "Privacy, and Personal Data." *Harvard Law Review* 117(7): 2056-2128.

Schwartz, Paul M. & William M. Treanor, 2003. The New Privacy. *Michigan Law Review* 101: 2163-2184.

Sepehr, Pouya & Ulrike Felt. 2023. "Urban Imaginaries as Tacit Governing Devices: The Case of Smart City Vienna." *Science, Technology, & Human Values*: 1-23.

Shorr, Scott. 1995. "Personal Information Contracts: How to Protect Privacy Without Violating the First Amendment." *Cornell Law Review* 80(6): 1756-1850.

Skinner-Thompson, Scott. 2020. *Privacy at the Margins*. New York: Cambridge University Press.

Smith, Elta. 2009. "Imaginaries of Development: The Rockefeller Foundation and Rice Research." *Science as Culture* 18(4): 461-482.

Solove, Daniel J. 2001. "Privacy and Power: Computer Databases and Metaphors for Information Privacy." *Stanford Law Review* 53: 1393-1462.

Solove, Daniel J. 2023. "The Limitations of Privacy Rights." *Notre Dame Law Review* 98: 975-1036.

Suitner, Johannes. 2015. *Imagineering Cultural Vienna: Urban Studies*. Germany: Verlag Transcript.

Susser, Daniel. (2022). "Data and the Good?" *Surveillance & Society* 20(3): 297-301.

Taylor, Charles. 2004. *Modern Social Imaginaries.* UK: Duke University Press.

Tranter, Kieran. 2011. The Speculative Jurisdiction. The Science Fictionality of Law and Technology. *Griffith Law Review* 20(4): 817-850.

van den Hoven, M.J. 1997. "Privacy and the Varieties of Moral Wrong-doing in an Information Age." *Computers and Society.*

van Lente, Harro & Arie Rip, 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.

Waldman, Ari E. 2021. "The New Privacy Law." *UC Davis Law Review Online* 55:19-42.

Waldman, Ari E. 2021a. "Privacy, Practice, And Performance." *California Law Review* 110: 1221-1280.

White, Jarrod J. 1997. "E-Mail@Work.Com: Employer Monitoring of Employee E-Mail." *Alabama Law Review* 48(3): 1079-1104.

Wilka, Rachel. 2018. "Privacy Commitments." *Washington Law Review Online* 93: 63-101.