2024

The Broader Lessons of Privacy Law

Salome Viljoen
University of Michigan Law School, sviljoen@umich.edu

Recommended Citation

Viljoen, Salome. "The Broader Lessons of Privacy Law." *Boston University Law Review* 104, no. 4 (2024): 1131-1149.

THE BROADER LESSONS OF PRIVACY LAW

SALOMÉ VILJOEN*

ABSTRACT

This Article explores the trend of privacy—and what kind of techno-social or legal effect ought *to count as a "privacy harm"—expanding to encompass a growing set of social factors. This big-tent approach to privacy has several virtues. However, it also comes with a few costs. While others have explored the conceptual and doctrinal tradeoffs that an expansive approach to privacy may entail, this Article focuses on a secondary effect the trend toward expansiveness has had on the relationship between privacy scholarship and legal scholarship more broadly. This Article suggests that the internal expansiveness of privacy means that insights developed within the field that are of* general *import for the legal analysis of a digital society are being neglected by legal theory more broadly. Much of the recent development in "privacy law" presents a body of legal-theoretical work that, while holding divergent views on substantive conceptions of what privacy is for, shares a common approach to understanding how interpersonal relations and legal institutions are being impacted and remade in—and by—an increasingly digital society. This approach is not only relevant for scholars of privacy law but is generally useful for understanding and analyzing the legal issues that arise in a pervasively informationalized society. Relegating this common approach to even the expansive doctrinal tent of "privacy law" undersells the methodological value privacy scholarship has to offer a wider body of legal scholarly work.*

* Assistant Professor of Law, The University of Michigan Law School.

CONTENTS

INTRODUCTION

This Article considers the trend of privacy expansion—the tendency over the past several years in privacy scholarship and advocacy to include a growing set of social factors when considering the legal effects and normative stakes we count within the concept of a "privacy harm." This expanded approach has rightly emphasized the role of privacy as a precondition for other socially necessary or desirable goods.[1] It has provided a much-needed corrective to the view of privacy as a marginal concern and has endeavored to heighten the political and legal salience of legal protections for privacy (particularly for members of vulnerable social groups).[2] However, this big-tent approach to privacy and privacy harm also comes at a cost.

One cost—among others—is that insights being developed in the field of privacy law that are of *general* import for law in a digital society are being mistaken for insights that are only relevant to, or pertain to, matters of privacy law.[3] As a result, I believe such insights, particularly the methods that have developed within privacy law to understand how choices about information and law coproduce power, are underappreciated for the broader contributions to legal thought they might provide.

Unsurprisingly, data and digital technology have seen a notable uptick in interest from legal scholars across a broad swathe of fields—antitrust, tax, free speech, finance, corporate governance, etc.[4] Information and information technologies like AI are increasingly pervasive and are of growing generalized social, economic, and political importance. So, it follows that the impact of information and information technologies on various areas of law also becomes increasingly generalized. As a field that has been thinking about information, its relation to legal persons, and the conceptual and normative aspects of its cultivation and use for some time, privacy law has important *generalizable* jurisprudential insights and methods to offer on these topics that go well beyond the privacy concerns raised by these technologies.[5]

Taken together, much of the recent development in "privacy law" presents a body of legal theoretical work that shares a common approach to understanding how interpersonal relations and legal institutions are being impacted and remade in an increasingly digital society.[6] This body of work, while divergent in its substantive focus and even in its (implicit or explicit) theories of what privacy is, broadly shares a starting set of assumptions regarding the relationships

[1] *See infra* Section I.A.1.

[2] *See id.*

[3] *See infra* Part II.

[4] For example, the Institute for Technology Law & Policy at Georgetown Law has an expansive collection of recent paper submissions. *See The Scholarly Commons: ITLP Papers & Reports*, GEO. L., https://scholarship.law.georgetown.edu/itlp_papers/index.html (last visited May 14, 2024).

[5] *See infra* Part II.

[6] *See id.*

between new informational practices and legal or social change. Namely, a hallmark of "good" privacy scholarship is that it attends as carefully to how information about people—the conditions of data's cultivation and the institutional design that structures how it flows—can reallocate power between people or entities, as it does to how law—the interests law enacts, and its institutional design—reallocates power between its subjects.[7] This approach is not only relevant for scholars ultimately concerned with the privacy implications of such changes. Indeed, several excellent examples of legal scholarship that adopt this approach lie outside even the expansive boundaries of privacy law.[8] As such work suggests, this approach is generally useful for understanding and analyzing the legal issues that arise in a pervasively informationalized society.

Part I sets up the conceptual tensions and strategic puzzles that arise from a pluralistic concept like privacy. Part II canvasses current trends in privacy scholarship and litigation to expand the set of concerns we count as "privacy problems." This big-tent approach to privacy has conceptual value—it gets things "right" about today's privacy landscape. It has programmatic value, as it makes the case that privacy matters for a wider set of goals and reasons, and thus can win friends and allies to the privacy cause. But it also exacerbates the internalist tensions within privacy and can thus contribute to conceptual, programmatic, and doctrinal uncertainty regarding how to resolve internal conflicts about what privacy interests lie at privacy's core and which at the periphery, and which legal and political strategies are best pursued to vindicate privacy interests. In Part III, this Article takes up a different effect of privacy's tendency toward internal expansiveness. Namely, that slotting the developments and insights that have occurred in privacy law over the past ten years or so into the bucket of "privacy law" means we are missing the methodological and jurisprudential insights of general import being developed under the guise of "privacy law." These insights aren't just relevant to one doctrinal area or field, but can be of general value to legal scholars interested in exploring how digital tech built from human information, like AI, impacts law and vice versa.

[7] One compelling hypothesis for how and why this approach arose among privacy scholars is sociological. Privacy law is highly interdisciplinary, and many privacy law scholars engage closely and frequently with scholarship in science and technology studies, information science, communications and media studies, surveillance studies, sociology, and philosophy of science. Privacy-law scholarship in these fields engages in the study of how information and information systems' structure form our interpersonal, social, and political economic relations.

[8] For a by-no-means-exhaustive list, consider recent work in labor law such as BRISHEN ROGERS, DATA AND DEMOCRACY AT WORK: ADVANCED INFORMATION TECHNOLOGIES, LABOR LAW, AND THE NEW WORKING CLASS (2023), Zephyr Teachout, *Algorithmic Personalized Wages*, 51 POL. & SOC'Y 436 (2023), and Veena Dubal, *On Algorithmic Wage Discrimination*, 123 COLUM. L. REV. 1929, 1952-61 (2023).

I. THE PROBLEM OF PRIVACY'S MANY MEANINGS

This Part sets up how the growing universe of privacy problems can exacerbate the scope and stakes of internal contradiction that arise from a pluralistic concept like privacy.

A. *A Scenario: Ann Arbor Ordinance*

To start, let's consider a hypothetical scenario. Say that Ann Arbor, Michigan ("the City") passes an ordinance that requires all entities that hold themselves out to the public as sexual and reproductive health services to register and obtain a license to operate within the city. This ordinance applies to crisis pregnancy centers ("CPCs"), among other entities. As part of the registration process, entities must disclose any religious affiliation their organization has, and if a meaningful amount of their funding comes from religiously affiliated organizations, they must disclose those sources. Clearly this ordinance raises other legal issues, but let's put those aside and focus on privacy.

On the one hand, privacy advocates might be concerned about a state actor like the City requiring a private entity to disclose a deeply personal fact like religious belief, or worse, disclosing that fact about their supporters. Even if local privacy advocates are no great champions of CPCs, giving the City the authority to demand sensitive personal information about an entity or some of its stakeholders as a condition of entry seems like a dangerous privacy precedent to set. This ordinance violates substantive notions of privacy that protect the class of intimate knowledge that is no business of the state, such as religious belief. Advocates may argue that privacy protections for religious belief foster self-authorship and protect freedom of thought and action, and that they act as a buffer against the power asymmetry between individuals and state actors. Stripping such protections away from CPCs undermines the ability of CPCs and their donors to enact their beliefs and views and uses the power of the state to chill their free (and lawful) activity.[9]

This ordinance, advocates may further argue, also violates core procedural privacy principles like data minimization and purpose limitation, since presumably the donors funding CPCs' work did not disclose their beliefs to be shared with the City and used in this way. Indeed, use of their religious affinity to register CPCs, insofar as it chills use of CPCs in southeast Michigan, might go against the express purpose for which organizations or individual people shared such information with the CPCs to begin with. On this account, a law that seeks to constrain CPCs and chill the free sharing of religious affinity among CPCs and their donors, is deeply incompatible with a general principle of privacy that protects people's freedom to choose who they share what information with, and to control how that information goes on to be shared.[10]

[9] *See* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 854 (2022) (describing harm to individual privacy through chilling effects on civil liberties).

[10] *See id.* at 797 (describing harm to privacy by violating individuals' expectations that their data will not be shared with third parties).

Moreover, it undermines the capacity privacy affords for us to find spaces of trust and intimacy in which to foster community on the basis of shared values and goals.

On the other hand, proponents of reproductive and sexual privacy may argue that greater accountability for CPCs, even if it involves some privacy loss for those entities, is a win for privacy overall. First, such advocates would be quick to point out that CPCs are themselves very privacy invasive.[11] Because CPCs are not medical providers, they are not bound by HIPAA. As part of their intake, CPCs are known to collect lots of information from people and keep extensive records of everyone who comes into their clinics, and to share that information with other CPCs and anti-abortion groups.[12]

More substantively, proponents would argue that CPCs work to erode sexual and reproductive privacy in more systematic ways. Politically, they coordinate and work within a broader movement aimed at increasing restrictions on sexual and reproductive freedom, a legal goal which necessarily involves reduced sexual privacy. In their individual interactions with people, CPC counselors aim to influence what sexual privacy proponents view as a deeply personal choice about continuing a pregnancy—imposing an external agenda on precisely the kind of intimate and significant decision privacy law is meant to shield from the scrutiny of others. Thus, CPCs arguably undermine the very sexual and reproductive autonomy that reproductive privacy aims to secure. In sum, on this account, an ordinance that regulates the activity of CPCs enhances sexual and reproductive privacy for would-be patients and others. Laws that constrain the effectiveness that CPCs obtain via their obscurity are, on these grounds, compatible with the overall goal of greater sexual and reproductive privacy for all.

To which opponents might say that two privacy wrongs don't make a privacy right. And so on and so forth.

B. *The Internal Puzzles of Pluralism*

The problem highlighted by the scenario above is that we lack settled "internal to privacy" ways to say which view of this ordinance ought to "win out" *on privacy grounds*. To be clear, we have grounds *external* to privacy. One side can point to legal and moral grounds of religious freedom against state interference, another to grounds of sexual and reproductive equality which demands certain

[11] *See generally* Kassandra DiPietro, *Who Decides?: Informed Consent Doctrine Applied to Denial of Reproductive Health Care Information at Crisis Pregnancy Centers*, 107 IOWA L. REV. 1253 (describing harms to individuals' privacy at CPCs due to lack of informed consent).

[12] *See, e.g.*, Margi Murphy, *Anti-Abortion Centers Find Pregnant Teens Online, Then Save Their Data*, BLOOMBERG (June 27, 2022, 8:00 AM), https://www.bloomberg.com/news/articles/2022-06-27/anti-abortion-centers-find-pregnant-teens-online-then-save-their-data (describing how some CPCs collect data from potential patients and share it with antiabortion advocacy groups).

state protections. Choosing between these grounds may definitively settle why their view ought to win the day.

However, *qua privacy*—i.e. the common ground here—what ought we to do? Is this ordinance bad or good for privacy? The two accounts of privacy laid out here present what David Pozen calls a "privacy-privacy tradeoff," where privacy lacks common rules for settling what course of action is "required by" or "more compatible with" privacy.[13] To put it slightly differently, answering this question depends on whose view of privacy, or conception of privacy, we take to be of primary or core significance. Either side might plausibly charge the other with "winning the privacy battle to lose the privacy war." But this only begs the question of what privacy stands for, and what winning it would entail.

In fact, this scenario may present several possible clashes between conceptions of privacy. Along a substantive dimension, we might ask whether sexual privacy generally ought to win out over religious privacy, or, sticking closer to the facts at hand, whether better overall privacy in the reproductive context ought to win out over worse privacy overall in the religious context. But we might also hold the substantive dimension fixed to consider the tradeoffs between ends and means. We might ask whether reining in "bad privacy actors," in say the reproductive freedom context, outweighs the value of honoring good privacy procedural principles—in other words, if this is a case where the privacy-preserving ends justify the privacy-eroding means.

Finally, this scenario raises tradeoffs along the public/private divide: Should we approach data sharing imposed by public actors with special concern, or consider the risks of state surveillance evenly against the public interest in regulating forms of private surveillance, in the reproductive health context and beyond? Any answer requires not just picking one theory of privacy over another, but in doing so, losing out along one dimension or account of privacy to "gain" along another—and thus make a call about what kinds of privacy claims either strictly or locally dominate others.

C. *Overloading Privacy?*

What this scenario suggests is that privacy tradeoffs raise fundamental issues about what privacy is for and what securing it would entail. On the one hand, this is not a new concern, nor one that lacks for responses.[14] Thus, individual accounts offered by particular privacy scholars may well have a response available to the hypothetical above. Neil Richards and Woody Hartzog's work on loyalty and trust might reframe my hypothetical to foreground the duties CPCs owe would-be patients, and may conclude some disclosure serves as a helpful

[13] *See* David E. Pozen, *Privacy-Privacy Tradeoffs*, 83 U. CHI. L. REV. 221, 222-23 (2016) (explaining different conceptions and examples of "privacy-privacy tradeoffs").

[14] *See generally* Woodrow Hartzog, *What Is Privacy? That's the Wrong Question*, 88 U. CHI. L. REV. 1677 (2021).

corrective to temptations to violate such duties.[15] Helen Nissenbaum's theory of contextual integrity would likely settle the normative evaluation of what privacy requires here by reference to whether the operative context is one of health provision or religious civic activity.[16] Scott Skinner-Thompson's work, building on that of Khiara Bridges and Danielle Citron, would suggest that my framing of the hypothetical is a red herring: his substantive account takes a side in this debate, arguing that to understand what privacy requires, one must first consider how the background conditions of power protect the privacy of religious donors at the expense of would-be patients of CPCs.[17]

Privacy has long been taken to refer to multiple concepts, or, if taken as a condition, one that can be met by a variety of actions under the right circumstances.[18] Expansive or pluralistic concepts like privacy naturally introduce some likelihood of internal friction, or a plausible range of alternatively justifiable actions. And as a more general matter, there may be good reasons—of conceptual fidelity and of political expediency—to retain the pluralistic nature of privacy.

However, several years' worth of developments to expand the concept of privacy (along the two trends described below in Part II) may well increase both the number and the intensity of internal strains and tradeoffs of the kind posed above. As privacy has expanded to contain more and more kinds of interests and protect against a greater set of harms, there is some risk that privacy has become an overloaded concept. Stuffing too much into the privacy tent can undermine its usefulness and perhaps blunt the conceptual, programmatic, and pragmatic virtues of privacy pluralism.

At the most basic conceptual level, an overburdened privacy category can lead to lack of clarity regarding common semantic meaning across and between

[15] *See* Woodrow Hartzog & Neil M. Richards, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961, 989 (2021) (describing duty of loyalty as relational policy tool to problems of information capitalism, platform power, and manufactured consent); Woodrow Hartzog & Neil M. Richards, *Legislating Data Loyalty*, 97 NOTRE DAME L. REV. REFLECTION 356, 361 (2022) (describing "chain-link" approach to relational privacy linking disclosure rules to loyalty obligations); Woodrow Hartzog & Neil M. Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L. REV. 985, 996 (2022) (describing disclosure requirements as rules compelling or constraining behavior and distinguishing from prescriptive approaches focusing on demonstrating loyalty through affirmative duties to act).

[16] HELEN NISSENBAUM, PRIVACY IN CONTEXT 132-37 (2009) (outlining theory of contextual integrity where contexts overlap and conflict, altering prescribed norms).

[17] SCOTT SKINNER-THOMPSON, *No Privacy in Public = No Privacy for the Precarious*, *in* PRIVACY AT THE MARGINS 8, 16 (2021) (describing unequal distribution of surveillance and diminished right to privacy according to demographic factors).

[18] As would be the case under, for example, a contextual integrity theory of privacy, where what constitutes "private sharing" or an appropriate information flow in one context may not constitute one in others.

work; this in turn can confuse and obscure debates (and agreements).[19] Substantively, too many overlapping and conflicting meanings can leave privacy debates without sufficient common ground—by which I mean common grounding principles—from which to reason in a given setting where different "privacies" may point in competing or distinct directions. And politically, an overloaded concept can paper over sharply divergent political priorities and goals that may animate different privacy accounts, as well as empower bad actors who benefit from weaponizing a muddled and muddied concept.[20]

Doctrinally, the lack of conceptual clarity can more readily privilege certain privacy concepts over others. At the same time, the common language of privacy can obscure this effect and stymie attempts to push back on them as internal privacy-privacy conflicts, whether those conflicts occur via litigation or regulatory strategies. Doctrinal privileging can lead to "cracking" of privacy along fault lines carved by courts' willingness to take up certain privacy concepts and not others. Such cracks seem particularly likely to form along the different external grounds that more social or structural privacy arguments often implicate. For example, if sexual equality cuts against a given privacy argument, sexual privacy advocates face a tension in their internal account of sexual privacy that the "privacy purist" (whose account of privacy's political value does not bind it to that of sex equality) does not. Doctrinal privileging and subsequent cracking is especially an issue given the kinds of litigants that are better resourced and thus in a better position to develop and shape which privacies fall in and out of the core doctrinal conceptions.

In response, some have argued for a deflationary account of privacy, defining its core features, a coherent content and normative structure, or at least a family of concepts that have real value in expressing a set of legal interests and related normative concerns we may have about them.[21] Annoyingly, my main project here is not to take up such deflationary accounts or to offer my own.[22] Instead, I

[19] Recent work by María Angel and Ryan Calo documents this issue, among others, regarding privacy as social taxonomy. *See, e.g.*, María P. Angel & Ryan Calo, *Distinguishing Privacy Law: A Critique of Privacy as Social Taxonomy*, 124 COLUM. L. REV. 507, 513-14.

[20] *See* Rory Van Loo, *Privacy Pretexts*, 108 CORNELL L. REV. 1, 9-10 (2022) (explaining how strong privacy laws must consider potential for businesses to manipulate them for information control).

[21] *See* Lisa Austin, *Privacy and the Question of Technology*, 22 LAW & PHIL. 119, 121 (2003) ("I argue that technology need not force us to reinvent privacy although we must sharpen and clarify what we mean by privacy and why we are concerned about losses of privacy."); NISSENBAUM, *supra* note 16, at 6-7 (stating goal of articulating "foundation for . . . directions [in policy, law, and technological development] so we may answer questions not only of the form: *what* policies, *what* court decisions, *what* technical standards and design features, but *why* these, with answers rooted in humanistic moral and political traditions of contemporary liberal democracies").

[22] I am developing my own views regarding privacy as an overloaded concept in other work. This work suggests that we might need normative and legal categories for a class of social informational interests, and social informational harms that are not best catalogued as privacy harms. *See generally* Salome Viljoen, Privacy Puzzles (unpublished manuscript) (on

am going to first offer a brief explanation of how and why privacy has become an overloaded concept, what is gained from this big-tent approach, and what is lost.[23] Then I hope to make the case for one such loss: that the theoretical and methodological insights being developed under the auspices of "privacy law" are in fact of much broader, generalized value to legal scholars in other fields, for understanding and properly evaluating the causes and effects of law in a digital society like ours.[24]

II. GROWING THE UNIVERSE OF PRIVACY PROBLEMS

This Part takes a step back and considers how and why we got to such a capacious understanding of privacy harm. Two trends of the past several years have conspired to make privacy roughly synonymous with "not doing bad stuff with information about people."

A. *The Sociopolitical Nature of Privacy Harm*

One trend is that scholars and advocates have, rightfully, pointed out the social and political intersections with and dimensions of privacy.

There has been significant success, thanks in no small part to many of the scholars represented in this Symposium, in overcoming the popular (mis)conception of privacy as a stuffy, somewhat marginal right. This view—still held among some, but on the decline—is of privacy as essentially concerned with recourse against excessive, prurient curiosity a la peeping Toms, and thus

file with author). However, I am not alone in this view. Other scholars, notably María Angel and Ryan Calo, have similarly argued that privacy, at least in its current scholarly formulation, lacks coherence as a concept. *See* María P. Angel, *Privacy's Algorithmic Turn*, 30 B.U. J. SCI. & TECH. L. (forthcoming) (manuscript at 46-49) (on file with Social Science Research Network) (observing that broadening information privacy concept "risks diffusing the concept into a meaningless catchall term, or even worse, collapsing it into broader and more established fields of law, such as consumer protection" (citations omitted)); Angel & Calo, *supra* note 19, at 512 ("Yet this expansive, criteria-free approach to privacy has come to fold in information-based threats to self-expression, anti-subordination, and fairness as core privacy concerns."); Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1139-42 (2011) ("But without a limiting principle or rule of recognition, we lack the ability to deny that certain harms have anything to do with privacy or to argue that wholly novel privacy harms should be included, which in turn can be useful in protecting privacy and other values."). David Pozen has suggested and explored the tensions of a big-tent concept with his work on privacy-privacy tradeoffs. *See* Pozen, *supra* note 13, at 222 ("[I]n myriad social and regulatory contexts, enhancing or preserving privacy along a certain axis may entail compromising privacy along another axis. If they wish to be more analytically rigorous, theorists and decisionmakers must take such privacy-privacy tradeoffs into account."). Even scholars who embrace privacy's pluralism nod to the truism that it contains conceptual multitudes. *See* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1 (2008) ("Privacy, however, is a concept in disarray. Nobody can articulate what it means. Currently, privacy is a sweeping concept . . . .").

[23] *See supra* Sections I.A.1-3.

[24] *See infra* Part II.

an interest that expresses inchoate feelings of creepiness at being impermissibly observed—not a pressing matter of justice, but rather a preoccupation of the privileged, the paranoid, and the cranky.[25] Relatedly, privacy scholarship has definitively put to bed (at least in academic circles) flawed notions of privacy as (only) about individual control.[26]

Such work has comprehensively made the case that privacy is an enabling good for broader social values and is itself a value that emerges in symbiotic relation to background social contexts.[27] Beyond its intrinsic benefits, privacy is a vital precondition for any number of other goods—classic goods associated with individual selfhood such as self-authorship, dignity, and intellectual

[25] This traditional conception of privacy as a "right to be let alone" is, of course, Samuel Warren and Louis Brandeis's famous and influential account of privacy from their 1890 Harvard Law Review article. *See* Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (quoting THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS: OR THE WRONGS WHICH ARISE INDEPENDENTLY OF CONTRACT 29 (Chicago, Callaghan & Co. 2d ed. 1888)) ("Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone.'"); *see also* Harry Kalven, Jr., *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, 31 LAW & CONTEMP. PROBS. 326, 328-31 (1966) ("Yet while the view is long and the right is placed on high ground, there is a curious nineteenth century quaintness about the grievance, an air of injured gentility."). Even today, "[t]he image of Peeping Tom . . . is commonly invoked to highlight privacy harm." Calo, *supra* note 22, at 29. As Daniel Susser notes, with the development of information technology over the course of the twentieth century, this conception expanded to cover an individual's ability to control their personal information. Such expansion was contested on both conceptual and programmatic grounds from the start. *See* Daniel Susser, *From Procedural Rights to Political Economy: New Horizons for Regulating Online Privacy*, *in* THE ROUTLEDGE HANDBOOK OF PRIVACY AND SOCIAL MEDIA 281, 283 (Sabine Trepte & Philipp K. Masur eds., 2023) ("This approach was contested from the start, both for its theoretical understanding of privacy and as a policy framework for managing increasingly data-driven societies.").

[26] Alan Westin's 1967 book *Privacy and Freedom* was one canonical formulation of the notion of privacy, particularly privacy as individual control in the context of computational and information technologies. *See* ALAN F. WESTIN, PRIVACY AND FREEDOM 3, 7 (1967) (calling for "discussion of what can be done to protect privacy in an age when so many forces of science, technology, environment, and society press against it" and defining privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"). Scholars have pushed back on formulations like this. *See* Daniel Susser, *Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even if Consent Frameworks Aren't*, 9 J. INFO. POL'Y 148, 151 n.5 (2019) (noting "[p]hilosophers, legal theorists, and privacy advocates have argued for alternative definitions of privacy, such as privacy as limited access, privacy as secrecy, and privacy as contextual integrity" but observing that control-based understanding is "the operative definition at work in the vast majority of U.S. policy discussions").

[27] *See* discussion *supra* Section I.A.1 (listing goods for which privacy is precondition); NISSENBAUM, *supra* note 16, at 3, 10-11 (advancing "framework of contextual integrity" focusing on "finely calibrated systems of social norms" and distinguishing framework from other approaches).

freedom,[28] but also social goods like democracy[29] and equality. One common egalitarian claim about privacy is that its sphere of protection around individuals serves to lessen, or at least ameliorate, the "'power asymmetries caused by the industrial econom[ies]' of the twentieth and twenty-first centuries."[30] Other equality claims about privacy go deeper, arguing that privacy is inextricably linked to projects of antisubordination on the basis sex, gender, race, and class, work Jessica Silbey calls the "fourth generation of privacy scholarship."[31] In a recent review, Daniel Susser catalogs these developments along three recent shifts in privacy: to view privacy as a structural (social) condition, to foreground the political economy of surveillance in evaluating privacy erosion, and to acknowledge the challenges of social media platforms as our collective communication infrastructure for the kinds of responses needed to address privacy harm.[32] Each shift definitively identifies the study of privacy rights and privacy violation as one of broader social and political inquiry and import.[33]

Of course, this development did not spontaneously emerge in the past few years. It is the product of decades of intellectual groundwork pushing against the

[28] *See, e.g.*, Luciano Floridi, Editor Letter, *On Human Dignity as a Foundation for the Right to Privacy*, 29 PHIL. & TECH. 307, 307-08 (2016) ("The protection of privacy should be based directly on the protection of human dignity, not indirectly, through other rights such as that to property or to freedom of expression."); NISSENBAUM, *supra* note 16, at 74-88 ("In the remainder of this chapter I will discuss samples that link privacy to important human values by arguing that privacy is either functionally or necessarily related to other more traditionally recognized, entrenched moral and political values."); Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968) ("In general it is my thesis that in developed social contexts love, friendship and trust are only possible if persons enjoy and accord to each other a certain measure of privacy."); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 423 (1980) (identifying "functions privacy has in our lives: the promotion of liberty, autonomy, selfhood, and human relations, and furthering the existence of a free society"); NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 5 (2015) ("In fact, a specific kind of privacy is *necessary* to protect our cherished civil liberties of free speech and thought.").

[29] PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 42 (1995). My preferred definition for democracy (perhaps another overloaded, or at least essentially contested, concept) is that of Iris Marion Young: the condition of living in political equality, and thus being recognized as a political equal. *See* IRIS MARION YOUNG, THE JUSTICE AND THE POLITICS OF DIFFERENCE 38 (2011).

[30] Jessica Silbey, *Four Privacy Stories and Two Hard Cases*, 37 CONST. COMMENT. 221, 222 (2022) (quoting NEIL RICHARDS, WHY PRIVACY MATTERS 8 (2021)).

[31] *Id.* (defining fourth generation of privacy scholarship as work that "considers the intersection of privacy law and equality along the dimensions of gender, race, sexual orientation, and economic class").

[32] *See* Susser, *supra* note 25, at 282 (highlighting shifts in privacy scholarship in response to social media).

[33] *Id.* (emphasizing need for broadening of privacy rights to include "digital public sphere").

conceptual and programmatic mistakes of "privacy self-management."[34] Indeed, Neil Richards places the beginnings of privacy law's structural turn as early as the late 1990s and early 2000s, as information privacy law as a legal field was being formed.[35] Scholars have long noted the heightened privacy concerns of minoritized communities, and the close conceptual, normative, and doctrinal relationship between privacy as an interest and the unique vulnerabilities of those who occupy marginal positions in the social structure.[36] But I share the view of Silbey and Susser that there has been something of a tipping point—a transition from these arguments as a minor strain in privacy to a generally recognized set of features of the concept and the field. This shift corresponds to the changing material and social conditions of contemporary digital society—punctuated by the crises and anxieties that come from an information ecosystem fueled by commercial surveillance. This may be one reason for the increased receptiveness to these strains of analysis, and increased attention to developing on, and building from, such strains in newer work.

The result of this trend in privacy scholarship is that, for example, one cannot seriously discuss or address the challenge of sex and gender equality today without recognition of the systematic gendered vector of privacy violation. Patterned privacy violation is part of what it means to live in a society where gender and sex mark forms of durable political, social, and material inequality.[37]

---

[34] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1903 (2013) ("Privacy self-management cannot achieve the goals demanded of it, and it has been pushed beyond its limits.").

[35] *See* Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1088 (2006) (noting rise of Internet as catalyst for privacy law's change).

[36] *See, e.g.*, ANITA L. ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY 116 (1988) (remarking women's "concern for the right to family privacy in many case boils down to concern for women's right to decisional privacy"); *see also* Anita L. Allen, *Dismantling the "Black Opticon": Privacy, Race Equity, and Online Data-Protection Reform*, 131 YALE L.J.F. 907, 931 (2022) ("Existing guidance around data-privacy reform falls short of directly addressing the pervasive problems of African Americans in the digital economy–even when it purports to promote equity."). The early constitutional cases involving sexual intimacy and reproductive choice were often framed, at least in part, as cases establishing a right to intimate privacy. *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479, 486 (1965) (holding birth control law intrudes on right of privacy in marriage); Eisenstadt v. Baird, 405 U.S. 438, 453 (1972) (noting right to privacy in regards to contraceptive use, regardless of marital status); Roe v. Wade, 410 U.S. 113, 153 (1973) (holding right to abortion is privacy matter). Justice Anthony Kennedy notes in *Lawrence v. Texas*, 539 U.S. 558, 564 (2003), the right to privacy established in *Griswold* served as the most relevant starting point for *Lawrence*'s case establishing the constitutionality of same-sex relationships.

[37] *See* KHIARA M. BRIDGES, THE POVERTY OF PRIVACY RIGHTS 5 (2017) (noting frequency of Medicaid programs invading poor women's privacy with frequent questioning of sensitive topics); DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 12 (2014) (highlighting online harassment continues to increase); Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1898 (2019) (declaring "sexual-privacy invasions can lead to marginalization and discrimination"); Mary Anne Franks, *Democratic Surveillance*, 30 HARV. J.L. & TECH. 425,

Thus, in the wake of the *Dobbs* decision, one sees concern not only over how to advocate for and provide access to reproductive services, but also over fertility privacy—which is commonly recognized as a primary risk vector for those seeking to access reproductive care.[38]

B. *Privacy as Moral Intuition*

The second trend is that privacy has been called on to do more in naming what ordinary people (and policymakers) find wrongful about a commercial surveillance society. Here I suspect two things are at work. First, privacy is commonly, and I think correctly, taken to be a thickly normative concept: we reach for it in denoting the wrongness and rightness of an action or a state. Second, privacy is closely conceptually associated with information—the excessive, deceitful, or wrongful obtaining of knowledge about a person, or the kind of wrong one associates with information about oneself being put toward some purpose that one may find harmful, offensive, degrading, or otherwise disagrees with or finds objectionable on moral grounds.

Given a digital society wherein entities are doing a great deal with a whole lot of information about and from people, producing a whole lot of social effects and disruptions in the process, there's a strong collective intuition to reach for privacy in naming the objections lodged against the contemporary digital society. For example, Cambridge Analytica is a privacy scandal, though imbricated in anxieties about the 2016 U.K. and U.S. elections, and the then-growing set of concerns over how our society is to reproduce democratic institutions and societies in the face of eroding commonality, trust, and communication online.[39] Clearview AI is a privacy scandal, albeit one nested in and within anxieties about the racialized overreach of police power.[40] More recently, the harm of AI is cast as (among other things) privacy harm. For example, the White House's AI bill of rights, responding to both the excitement and the concerns over generative AI, emphasizes the foundational role of substantive privacy regulation for regulating AI, in a nod to what is perhaps the

441 (2017) ("Race, class, and gender have all helped determine who is watched in society, and the right to privacy has been unequally distributed according to the same factors.").

[38] *See* Aziz Z. Huq & Rebecca Wexler, *Digital Privacy for Reproductive Choice in the Post*-Roe *Era*, 98 N.Y.U. L. REV. 555, 598 (2023) (highlighting "abortion regulation will motivate an uptick in digital and physical searches for medical care across borders"); *see also* Dobbs v. Jackson Women's Health Org., 597 U.S. 215, 231 (2022) (overruling *Roe v. Wade* and constitutional protection of abortion).

[39] *See* Christina Pazzanese, *On the Web, Privacy in Peril*, HARV. GAZETTE (Mar. 21, 2018), https://news.harvard.edu/gazette/story/2018/03/facebooks-privacy-problem-may-erode-web-trust-harvard-analyst-says/ [https://perma.cc/YS6X-B4XZ] (discussing harm to online trust in wake of Cambridge Analytica scandal).

[40] *See* Nick Statt, *Controversial Facial Recognition Firm Clearview AI Facing Legal Claims After Damning NYT Report*, VERGE (Jan. 24, 2020, 12:09 PM), https://www.theverge.com/2020/1/24/21079354/clearview-ai-nypd-terrorism-suspect-false-claims-facial-recognition [https://perma.cc/JLE9-7DJH] (describing Clearview AI and its impact on racialized understandings of facial recognition technology).

"original sin" or "poisoned tree" of generative AI models—the mass ingestion of our digital lives.[41]

*****

To be clear, there are good reasons not to dismiss or abandon either the scholarly developments or the popular moral intuitions that underpin these two trends. Privacy as a "big-tent" concept wins political allies and sympathizers. It builds the privacy coalition, and makes the case that privacy is good and it is good for everyone (even if the most vulnerable among us need it more than others). Getting everyone on board for privacy in lots of different ways and for lots of different reasons is helpful to the cause. Moreover, that this big-tent view aligns with common sense and the "ordinary meaning" of how people understand and name informational wrongs is worth taking seriously as a source of moral and conceptual insight, if not authority.

III. SCHOLARLY UPSHOTS: THE CENTRAL ROLE OF DATA AND INFORMATION IN LEGAL ANALYSIS FOR THE DIGITAL SOCIETY

Privacy's big-tent approach has rightly emphasized the important role privacy rights play as a precondition for other socially necessary or desirable goods, particularly in light of an increasingly informationalized society. This trend has provided a much-needed corrective to the view of privacy as a marginal concern, particularly for members of vulnerable social groups. However, as discussed above, this expanding approach to privacy and privacy harm also places increased strain on the internal contradictions and tradeoffs within privacy law, and comes with a few costs.

One such cost is missing the methodological and jurisprudential insights of general import being developed under the guise of "privacy law." Insights being developed in the field of privacy law that are of *general* import for law in a digital society are being misjudged and misclassified as insights that are only relevant to, or pertain to, matters of privacy law.

As AI has—once again—emerged as a constant source of popular attention and discourse, legal scholars across a diverse range of fields, not just privacy law, are writing about information technologies and the data that fuels them.[42]

---

[41] *See generally* OFF. SCI. & TECH. POL'Y, BLUEPRINT FOR AN AI BILL OF RIGHTS (2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf [https://perma.cc/M7YT-7J58] (promulgating blueprint for AI bill of rights).

[42] *See, e.g.*, Maya C. Jackson, *Artificial Intelligence & Algorithmic Bias: The Issues with Technology Reflecting History & Humans*, 16 J. BUS. & TECH. L. 299, 299-300 (2021) (exploring influence of racial and gender discrimination on modern algorithmic bias); Robin Feldman & Kara Stein, *AI Governance in the Financial Industry*, 27 STAN. J.L. BUS. & FIN. 94, 98-100 (2022) (describing impacts of AI on financial markets and proposing regulatory framework for effective governance); Samuel D. Hodge, Jr., *The Medical and Legal Implications of Artificial Intelligence in Health Care–An Area of Unsettled Law*, 28 RICH. J.L. & TECH. 405, 435-38 (2022) (explaining issues raised by increased utilization of AI in

And while I'll admit I don't love everything I read, I generally think this surge in legal interest in the digital political economy is a good thing, and indicative that what privacy scholars write on is an important subject of considerable general legal interest. We live in a digital society—it is only natural that law, the institution that systematizes and structures how we relate to one another and what we owe and are owed—responds to that fact with increased intellectual interest and scrutiny.

It is therefore no surprise that privacy has produced some of the most-cited legal scholarship of the past several decades.[43] But the general theoretical import of this work has, I think, still been underappreciated. If privacy is at a transformational crossroads, one reason why is that it has long ceased (if it ever was) being a field solely interested in a single doctrinal area of law, but instead been the seeding ground for interdisciplinary legal approaches to explore the specific jurisprudential questions that arise within a digital society.[44] To be clear, a good bit of this work still is, at its heart, about privacy. But information privacy as a subject lends itself to thinking seriously and deeply about questions that are of general and growing interest to legal scholars writ large.

Given the big tent of diverse privacies, grounded in diverse normative justifications, one way to make sense of what binds privacy scholarship together is not common grounding principles for the concept, but a common approach or mode of analysis developed among the field's practitioners over time, applied to the intersection of law and digital surveillance technology. Privacy scholars have long been attentive to the transformations taking place in computing and digital technology.[45] The privacy field, as a whole, engages in scholarly analysis of law and digital technology that attends *as* carefully to how information about people can remake power relations among people, as it does to how law can remake power relations among people.[46] Though a systematic account of the reasons why such methods developed particularly widely within privacy law is beyond the scope of this Article, one imminently plausible reason is sociological. Privacy law is a deeply interdisciplinary field, engaging frequently and in close

healthcare, including challenges to traditional tort law conceptions of agency, control, and foreseeability).

[43] Fred R. Shapiro, *The Most-Cited Legal Scholars Revisited*, 88 U. CHI. L. REV. 1595, 1609 (2021) ("The tabulation of most-cited younger legal scholars naturally reflects the emphases of recent times. One subject area clearly dominates here: the cluster of technology, intellectual property, and privacy, spilling over into First Amendment law and law and economics. At least nine of the twenty fall into this category, highlighted by the first two, Professors Daniel Solove and Orin Kerr.").

[44] Silbey, *supra* note 30, at 222.

[45] *See, e.g.*, Schlomit Yanisky-Ravid & Sean K. Hallisey, *"Equality and Privacy by Design": A New Model of Artificial Intelligence Data Transparency Via Auditing, Certification, and Safe Harbor Regimes*, 46 FORDHAM URB. L.J. 428, 434 (2019) (discussing how inadequate regulatory schemes perpetuate existing discrimination and proposing model to increase awareness about discrimination and weakened societal expectations of privacy).

[46] *See, e.g.*, NEIL RICHARDS, WHY PRIVACY MATTERS 8 (2021) (describing impact of privacy on development of historical imbalances in industrial age).

intellectual contact with scholars of media and communication, surveillance studies, and science and technology studies, among others.[47] These fields' methods are designed to interrogate and analyze how informational design, production, and cultural effects implicate and remake social relations.

The interdisciplinary approaches adopted and, in turn, developed by privacy scholars pay as much analytic attention to the conditions of information cultivation and the institutional design that structures how it flows as it does to the way law enacts certain interests and how legal institutions are designed. In other words, it puts the study of law and the study of information and information technologies on equal footing. This approach is useful for understanding how law structures the production and use of information, is threatened and undermined by such activity, is remade by it, and can address it—*generally*.[48] To call the legal scholarship engaged in such work "privacy law" is therefore a bit of a misnomer. I take this to be a collection of legal scholars that have long paid keen attention to how the digitalization of social life impacts law, and vice versa. This, I think, goes beyond the study of a given legal area—even an overstuffed one—of "privacy law" to provide an approach to understanding the role of law in an information society that is of particular value for evaluating the legal causes and effects of the broader political economy of today.

The current approach to privacy casts this as a project of category expansion—widening the concept of privacy to incorporate the ever-growing effects of digitalizing social life. In other words, stretching "privacy" to fit a growing set of interests in how information enmeshes people in the creation, recreation, or amplification of a widening range of social problems. But one can view this trend from another perspective—widening the aperture of analysis beyond privacy to take in other issues arising from digital life that might be objectionable on independent grounds, or that implicate independent legal and social concerns. On this view, what binds "privacy law" together is not common grounding principles, but a common approach, emphasis, or mode of analysis developed in concert with interdisciplinary scholars, and applied to the intersection of law and digital surveillance technology.

This approach is not only relevant for scholars of privacy law but is useful for understanding and analyzing the legal issues that arise in a pervasively informationalized society across legal fields more broadly. To take one example, Daniel Susser notes the long trend of privacy scholars shifting attention from traditional worries about each particular "invasion" of privacy to the systemic

[47] María Angel's work on privacy's algorithmic turn, itself an interdisciplinary study *of* the privacy law community, provides evidence for this account. *See generally* Angel, *supra* note 22.

[48] Julie Cohen provides a forceful and sweeping example of this approach to engage in a wide-ranging analysis of how law structures and is remade by the same processes of transformation producing informational capitalism. *See* JULIE E. COHEN, BETWEEN TRUTH AND POWER 1 (2019) ("[A]s our political economy transforms, our legal institutions too are undergoing transformation, and the two sets of processes are inextricably related.").

conditions created by society-wide architectures of digital surveillance and data processing.[49] Systemic social architectures based on digital surveillance not only raise questions of privacy—they have implications for the law of commercial competition, free speech, administrative governance, and international trade, to name a few.[50] And to be clear, my contention here is not that privacy scholars are now, by dint of being experts of digital surveillance, experts in these legal fields. It is rather that the approaches and insights developed within privacy law—that take the causal effects and theoretical traditions of information and information technology as seriously as those of law—can be as useful for illuminating other legal issues of the digital society as they are for privacy.

To take another, privacy law has been characterized as a field that was "focusing less on individuals and individual rights and more on the power relationships between data collectors and data subjects" since at least the aughts.[51] Those power relationships not only implicate privacy interests—they can rematerialize any number of inequalities based on social group membership, like race, ethnicity, and gender, or reencode other kinds of legal relationships structured by inequality, such as creditor-lender, landlord-tenant, and worker-boss. Thus, the same power relationships that implicate privacy may—simultaneously and separately—implicate issues of racial or gender subordination.

Indeed, much of the recent development in "privacy law" presents a body of legal theoretical work that apprehends the growing entanglement of privacy—and its historical preoccupation with how information links people, constitutes, empowers and imperils them—with an ever-growing list of other social and legal concerns.[52] And, in attempting to make sense of this expanding entanglement, privacy scholarship has developed a common approach to understanding how interpersonal relations and legal institutions are being impacted and remade in an increasingly digital society.[53]

---

[49] Susser, *supra* note 25, at 283 (describing structural turn in privacy law scholarship focusing less on individual rights and more on systemic conditions); *see also* Richards, *supra* note 35, at 1095 (describing increased architectural focus on systemic information flow rather than individualized problems).

[50] *See, e.g.*, Raymond H. Brescia, *Social Change and the Associational Self: Protecting the Integrity of Identity and Democracy in the Digital Age*, 125 PENN ST. L. REV. 773, 835 (2021) (arguing digital threats also emerge from powerful private actors directed toward commercial and political ends). *See generally* Russell L. Weaver, *The Fourth Amendment and Technologically-Based Surveillance*, 48 TEX. TECH L. REV. 231 (2015) (describing interaction of technological advances and surveillance with Fourth Amendment).

[51] Susser, *supra* note 25, at 283; *see, e.g.*, DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 6 (2004) (arguing longstanding privacy law scholarship cannot resolve modern issues and calling for structural conceptualization).

[52] *See* Silbey, *supra* note 30, at 222 (describing "growing cadre of privacy law scholars focusing on the intersection of privacy and inequality, especially regarding the unequal treatment of marginalized communities").

[53] *See* Solove, *supra* note 34, at 1881 (summarizing scholarship on privacy's social impact and arguing privacy alters larger social values).

Relegating these insights to the category of "privacy law" alone—even an expansive category—undersells their general legal theoretical value for understanding legal relations in an informational society. In other words, the methods or approaches that have grown from decades of privacy analysis can describe, illuminate, or resolve many *other* kinds of legal issues.