3-2024

# Distinguishing Privacy Law: A Critique of Privacy as Social Taxonomy

María P. Angel

Ryan Calo

# ESSAY

## DISTINGUISHING PRIVACY LAW: A CRITIQUE OF PRIVACY AS SOCIAL TAXONOMY

*María P. Angel* & Ryan Calo***

*What distinguishes privacy violations from other harms? This has proven a surprisingly difficult question to answer. For over a century, privacy law scholars labored to define the elusive concept of privacy. Then they gave up. Efforts to distinguish privacy were superseded at the turn of the millennium by a new approach: a taxonomy of privacy problems grounded in social recognition. Privacy law became the field that simply studies whatever courts or scholars talk about as related to privacy.*

*Decades into privacy as social taxonomy, the field has expanded to encompass a broad range of information-based harms—from consumer manipulation to algorithmic bias—generating many rich insights. Yet this approach has come at a cost. This Essay diagnoses the pathologies of a field that has abandoned defining its core subject matter and offers a research agenda for privacy in the aftermath of social recognition.*

*Our critique is overdue. It is past time to think anew about exactly what work the concept of privacy is doing in a complex information environment and why a given societal problem—from discrimination to misinformation—is worthy of study under a privacy framework. Only then can privacy scholars articulate what we are expert in and participate meaningfully in global policy discussions about how best to govern information-based harms.*



* Ph.D. in Law Candidate 2024, University of Washington School of Law.

** Lane Powell and D. Wayne Gittinger Professor of Law, University of Washington School of Law; Professor (by courtesy), University of Washington–Seattle–Paul G. Allen School of Computer Science and Engineering; and Professor (by courtesy), Information School, University of Washington. The authors would like to thank Kendra Albert, Ignacio N. Cofone, Rebecca Green, Meg Leta Jones, Karen Levy, Gianclaudio Malgieri, John Pane, Daniel Solove, Mark Verstraete, Stav Zeitouni, and other participants in the 2022 Privacy Law Scholars Conference for their thoughtful comments.

## INTRODUCTION

A police drone peers through a second-story apartment window to inspect whether an armed robbery suspect is there.[1] Facebook withholds advertising for financial services from older users and female users.[2] A consumer is tricked into sharing more personal information than they intended.[3] A family living in a predominantly Asian American neighborhood is charged a higher price for SAT test preparation.[4] Farm robots outfitted

1. See Cindy Chang, LAPD Deploys Controversial Drone for the First Time, L.A. Times (Jan. 15, 2019), https://www.latimes.com/local/lanow/la-me-lapd-drone-20190115-story.html (on file with the *Columbia Law Review*).

2. See Jonathan Stempel, Facebook Sued for Age, Gender Bias in Financial Services Ads, Reuters (Oct. 31, 2019), https://www.reuters.com/article/us-facebook-lawsuit-bias/facebook-sued-for-age-gender-bias-in-financial-services-ads-idUSKBN1XA2G8 [https://perma.cc/6GUT-VGJ7].

3. See Alicia Adamczyk, These Are the 'Potentially Unlawful' Tactics Retailers Use to Trick Customers Into Spending More Money, CNBC (Nov. 27, 2019), https://www.cnbc.com/2019/11/27/how-retailers-trick-customers-into-buying-more.html [https://perma.cc/F3ZL-XU5F].

4. See Julia Angwin, Surya Mattu & Jeff Larson, The Tiger Mom Tax: Asians Are Nearly Twice as Likely to Get a Higher Price From Princeton Review, ProPublica (Sept. 1, 2015), https://www.propublica.org/article/asians-nearly-twice-as-likely-to-get-higher-price-from-princeton-review [https://perma.cc/588H-PEHK].

with cameras and data processors collect and crunch data to optimize farming.[5] A pregnancy-tracking app grants pregnant users' employers a royalty-free license to mine their de-identified personal information.[6] A renter is denied an apartment after the screening company's automated background check system incorrectly pulls in criminal records for women with different middle names, races, and birth dates.[7]

Each of these scenarios, and countless others, have been recognized as problems involving "privacy." Are they? This vibrant, interdisciplinary field with decades of history possesses no real sense of what constitutes a privacy problem and what does not. Though these scenarios implicate different values and arise from different contexts, none would be out of place at a privacy law conference. Yet other types of information-based harms—TikTok users sharing a fake screenshot of a nonexistent CNN headline suggesting that climate change is seasonal,[8] for example—would be out of place. Why? No one can say.

Throughout the twentieth century, scholars sought to define and distinguish the concept of privacy. A parade of articles and books, from *The Right to Privacy* onward, offered varying definitions for this elusive idea.[9] Privacy amounts to a right "to be let alone,"[10] these works argued, or "the control we have over information about ourselves."[11] Privacy involves access to the self or self-determination.[12] Over one

---

5. Amanda Little, Opinion, Farm Robots Will Help Feed the World During Climate Change, Bloomberg L. (June 2, 2022), https://www.bloomberglaw.com/bloombergterminalnews/bloomberg-terminal-news/RCUO2CDWX2QK (on file with the *Columbia Law Review*).

6. Drew Harwell, Is Your Pregnancy App Sharing Your Intimate Data With Your Boss?, Wash. Post (Apr. 10, 2019), https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/ (on file with the *Columbia Law Review*).

7. Lauren Kirchner & Matthew Goldstein, How Automated Background Checks Freeze Out Renters, N.Y. Times (May 28, 2020), https://www.nytimes.com/2020/05/28/business/renters-background-checks.html (on file with the *Columbia Law Review*).

8. Tiffany Hsu, Worries Grow that TikTok Is New Home for Manipulated Video and Photos, N.Y. Times (Nov. 4, 2022), https://www.nytimes.com/2022/11/04/technology/tiktok-deepfakes-disinformation.html (on file with the *Columbia Law Review*).

9. See infra Part I.

10. Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193, 195 (1890) (internal quotation marks omitted) (quoting Thomas M. Cooley, A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract 29 (2d ed. 1888)).

11. Charles Fried, Privacy, 77 Yale L.J. 475, 482 (1968) (emphasis omitted).

12. See, e.g., Anita L. Allen, Uneasy Access: Privacy for Women in a Free Society 13–17 (1988) [hereinafter Allen, Uneasy Access] ("[P]ersonal privacy is a condition of inaccessibility of the person, his or her mental states, or information about the person to the senses or surveillance devices of others."); Edward J. Eberle, Human Dignity, Privacy, and Personality in German and American Constitutional Law, 1997 Utah L. Rev. 963, 1000 (defining "informational self-determination" as a conception of privacy that seeks to "preserve the integrity of human personality against the onslaught of the technological age and of prying eyes"); Ruth Gavison, Privacy and the Limits of Law, 89 Yale L.J. 421, 423 (1980)

hundred years of debating solitude[13] yielded no universally agreed-upon definition. But that did little to deter privacy scholars from trying.

At the turn of the millennium, a new voice arose that would come to shape the field of American privacy scholarship for decades. In a series of articles and books, Professor Daniel J. Solove dismissed attempts to define privacy as invariably over- or underinclusive.[14] Embracing a pragmatism similar to that of Justice Oliver Wendell Holmes, Jr.,[15] Solove exhorted the field to abandon the quixotic quest to attach a single definition to privacy.[16] In its place, Solove offered a taxonomy of "the specific activities that pose privacy problems," a loosely correlated set of concerns and concepts that have come to be associated with privacy in its many forms.[17]

The taxonomizing of privacy was not without precedent. Professor William Prosser famously distilled four privacy torts from decades of case law,[18] and Professor Alan Westin compiled a taxonomy of privacy attitudes.[19] Nor has the taxonomy of privacy entirely evaded critique.[20] But

---

[hereinafter Gavison, Privacy and the Limits of Law] (arguing that privacy "is related to our concern over our accessibility to others").

13. See Gabriel García Márquez, One Hundred Years of Solitude (Gregory Rabassa trans., Harper & Row 1970).

14. See Daniel J. Solove, Understanding Privacy 8 (2008) (criticizing privacy theories that characterize privacy as a "unitary concept with a uniform value that is unvarying across different situations" and explaining that the "attempt to locate the 'essential' or 'core' characteristics of privacy has led to failure"); Daniel J. Solove, Conceptualizing Privacy, 90 Calif. L. Rev. 1087, 1124 (2002) [hereinafter Solove, Conceptualizing Privacy] (arguing that settling on any of the six common conceptions of privacy described in the article would result in "either a reductive or an overly broad account of privacy"); Daniel J. Solove, A Taxonomy of Privacy, 154 U. Pa. L. Rev. 477, 485–86 (2006) [hereinafter Solove, Taxonomy of Privacy] (claiming that attempts to find a single essence of privacy are usually "too broad and vague").

15. See Louis Menand, The Metaphysical Club: A Story of Ideas in America 339–47 (2001) (describing Holmes's theory of the law, which claimed that decisions are fundamentally dictated by experience, not formal doctrinal logic).

16. See Solove, Taxonomy of Privacy, supra note 14, at 481–82 (arguing for a framework to evaluate privacy issues based on specific harmful activities instead of defaulting to a single definition that is too vague to be useful for effective policymaking and lawmaking).

17. Id. at 482, 489–91.

18. See William L. Prosser, Privacy, 48 Calif. L. Rev. 383, 389 (1960) (proposing "four distinct kinds of invasion of four different interests of the plaintiff, which are tied together by the common name, but otherwise have almost nothing in common except that each represents an interference with the right of the plaintiff . . . 'to be let alone'" (quoting Thomas M. Cooley, A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract 29 (2d ed. 1888))).

19. See Alan F. Westin, Privacy and Freedom 31–32 (1967) (identifying four psychological conditions or states of individual privacy).

20. See, e.g., Jeffrey Bellin, Pure Privacy, 116 Nw. U. L. Rev. 463, 465–68 (2021) (listing the drawbacks of not being able to define the term "privacy"); M. Ryan Calo, The Boundaries of Privacy Harm, 86 Ind. L.J. 1131, 1140–42 (2011) [hereinafter Calo, Boundaries of Privacy Harm] (highlighting the limitations of the taxonomic approach and the pressing need for principles that delimit privacy harm); David E. Pozen, Privacy–Privacy Tradeoffs, 83 U. Chi. L. Rev. 221, 226–27 (2016) (pointing out how the "capaciousness" of Solove's taxonomic approach "exacerbates the dilemma of privacy-privacy tradeoffs").

Solove's specific rejection of privacy conceptualization in favor of a taxonomic approach continues to exert a profound influence on the shape of contemporary privacy scholarship. As Professor Woodrow Hartzog recently explained, abandoning definition in favor of taxonomy helped breathe new life into the field.[21] Unburdened by a need to define privacy, the past two decades have seen a Cambrian explosion in the arguments and issues at the heart of mainstream privacy scholarship.

This Essay argues that the long-dominant social-taxonomic approach to privacy and privacy law is no longer serving the field. There are several important reasons why. First, social recognition alone is not—and never has been—a sufficient criterion for what counts as a privacy problem. Instead of comparing an information-based harm to a set definition of a privacy harm, the taxonomic approach asks whether the right people or institutions—typically courts, public officials, and established scholars—talk about the harm as involving privacy.[22] In and of itself, this approach raises critical questions about authority, legitimacy, and whose voices should be heard and valued when it comes to identifying new privacy harms.

The social-taxonomic approach also omits, and arguably impedes, the development of a sophisticated framework for interrogating the tension *between* the various values under the privacy umbrella. For example, many free speech scholars see privacy as an impediment to self-expression.[23] Other scholars in the critical tradition have explored how privacy is deployed as cover for subordination.[24] And a decade or more of work in

---

21. See Woodrow Hartzog, What Is Privacy? That's the Wrong Question, 88 U. Chi. L. Rev. 1677, 1687 (2021) ("By getting us past the threshold question of what privacy is, Solove's work provides room for scholars and lawmakers to tackle bigger phenomena . . . .").

22. See Calo, Boundaries of Privacy Harm, supra note 20, at 1141 ("Solove's criteria for inclusion involve recognition by the right sorts of authorities.").

23. See, e.g., Solveig Singleton, Privacy Versus the First Amendment: A Skeptical Approach, 11 Fordham Intell. Prop. Media & Ent. L.J. 97, 97 (2000) ("The courts should think twice before sacrificing the mature law of free speech to the less coherent concerns about privacy."); Eugene Volokh, Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You, 52 Stan. L. Rev. 1049, 1051 (2000) ("While privacy protection secured by contract is constitutionally sound, broader information privacy rules are not easily defensible under existing free speech law.").

24. See, e.g., Catharine A. MacKinnon, Privacy v. Equality: Beyond *Roe v. Wade*, *in* Feminism Unmodified 93, 102 (1987) [hereinafter MacKinnon, Privacy v. Equality] (describing the right to privacy as "a right of men 'to be let alone' to oppress women one at a time" (footnote omitted) (quoting Warren & Brandeis, supra note 10, at 205)); Lucinda M. Finley, Transcending Equality Theory: A Way Out of the Maternity and the Workplace Debate, 86 Colum. L. Rev. 1118, 1119 (1986) ("The notion that the world of remunerative work and the world of home—or the realms of production and reproduction—are separate, has fostered the economic and social subordination of women . . . ."); Elizabeth M. Schneider, The Violence of Privacy, 23 Conn. L. Rev. 973, 975 (1991) [hereinafter Schneider, Violence of Privacy] ("The notion of marital privacy has been a source of oppression to battered women and has helped to maintain women's subordination within the family.").

algorithmic accountability illustrates the tension between privacy and antidiscrimination or fairness.[25] Yet this expansive, criteria-free approach to privacy has come to fold in information-based threats to self-expression, antisubordination, and fairness as core privacy concerns.[26] The result is a proliferation of vexing "privacy–privacy tradeoffs"[27] with little hope of reconciliation.

Situating privacy law within the broader structure of information-based power has become a critical task for scholars and policymakers alike. American privacy law scholarship has yet to even reconcile the basic distinction between privacy and data protection,[28] let alone the new modes of information governance that European and other societies are exploring today.[29] Distinguishing privacy from data protection, content moderation, or antidiscrimination law would shed light on the precise goals societies are trying to meet, the range of approaches that exist to meet them, and the institutions best suited to address these issues. The FTC, for example, may be better positioned to address violations of information privacy, whereas the DOJ Civil Rights Division is better versed in antidiscrimination law. Only recently have the United States and the European Union agreed on a privacy framework to share data, and to this day, the European Union has not recognized any American federal agency as a data-protection authority.[30]

It is imperative that we try to understand what work the concept of privacy is doing in today's complex information environment. As it happens, some of the leading and emerging lights in privacy law scholarship are beginning to disentangle privacy from other information-based values, reminding the field just what we are experts in.[31] The time has come to leverage this literature in service of a new direction for the field.

---

25. See, e.g., Roger Allan Ford & W. Nicholson Price II, Privacy and Accountability in Black-Box Medicine, 23 Mich. Telecomms. & Tech. L. Rev. 1, 4 (2016) ("The solution to the accountability problem is to validate black-box models, but that requires access to more information, which can exacerbate the privacy problem. And the solution to the privacy problem is to limit [information] . . . but that can make it harder to validate models and easier to hide . . . problems."); Finale Doshi-Velez & Mason Kortz, Accountability of AI Under the Law: The Role of Explanation 10 (2017), https://dash.harvard.edu/bitstream/handle/1/34372584/2017-11_aiexplainability-1.pdf [https://perma.cc/E7NE-3E9C] (unpublished working paper) ("AI systems do not automatically store information about their decisions. . . . [U]nlike human decision-makers, AI systems can delete information to optimize their data storage and protect privacy. However, an AI system designed this way would not be able to generate *ex post* explanations the way a human can.").

26. See infra section I.C.

27. See Pozen, supra note 20, at 222.

28. See infra notes 285–294 and accompanying text.

29. See infra notes 295–300 and accompanying text.

30. See 2023 O.J. (C 4745).

31. See, e.g., Julie E. Cohen, What Privacy Is For, 126 Harv. L. Rev. 1904, 1905 (2013) [hereinafter Cohen, What Privacy Is For] (arguing that privacy is not a legal protection for the liberal self but instead a fundamental tool for protecting "the situated practices of

The Essay proceeds as follows. Part I traces the efforts of twentieth-century privacy scholars to define our subject matter, culminating in Solove's intervention in the early 2000s, and acknowledges the generative role of privacy's taxonomy paradigm. Part II argues that social recognition has always been a flawed means by which to distinguish privacy and that privacy as taxonomy stands in the way of identifying, reconciling, and distinguishing privacy harms in a diverse and complex information environment. Section II.A discusses information-based harms that privacy law was late to recognize, such as information-based discrimination and algorithmic manipulation. Section II.B discusses unresolved tensions between and among privacy and other values.

Part III outlines a post-taxonomy research agenda for privacy law, one that decouples classification from social recognition, foregrounds the role of reflexivity, and begins to answer the deep question of just what work privacy is doing in the context of information-based harms. Misinformation, hate speech, bias, data sovereignty, labor extraction, and many other contemporary concerns *implicate* or *involve* privacy but sound in different values altogether. By uncritically broadening the concept of privacy, most Americans are missing out on a global conversation around data protection, information governance, and harm mitigation. Only by distinguishing privacy can privacy law reach its full potential as a discipline and a body of law.

## I. PRIVACY AS SOCIAL TAXONOMY

Scholars understand themselves as participating in a conversation. The precise contours of this conversation—collectively, the field—are important. Thus, it should come as no surprise that the development of a robust privacy literature was attended by commentators' many attempts to conceptualize their object of study. Early privacy scholars asked, time and again, just what *is* privacy? How does privacy differ from other social facts, concepts, and values?

---

boundary management through which the capacity for self-determination develops"); Cynthia Dwork & Deirdre K. Mulligan, It's Not Privacy, and It's Not Fair, 66 Stan. L. Rev. Online 35, 36 (2013), https://review.law.stanford.edu/wp-content/uploads/sites/3/2016/08/DworkMullliganSLR.pdf [https://perma.cc/Q8JA-463Q] ("Regrettably, privacy controls and increased transparency fail to address concerns with the classifications and segmentation produced by big data analysis."); Paul Schwartz, Data Processing and Government Administration: The Failure of the American Legal Response to the Computer, 43 Hastings L.J. 1321, 1343–52 (1992) [hereinafter Schwartz, Data Processing] (discussing the weaknesses of the "privacy" paradigm and proposing instead to talk about bureaucratic justice and human autonomy); Salomé Viljoen, A Relational Theory of Data Governance, 131 Yale L.J. 573, 578 (2021) (critiquing privacy law's individualism, which fails to address data's population-level relational effects); Tal Z. Zarsky, Privacy and Manipulation in the Digital Age, 20 Theoretical Inquiries L. 157, 161–68 (2019) [hereinafter Zarsky, Privacy and Manipulation] (suggesting that manipulation-based arguments are preferable to privacy theories, which are plagued with substantial theoretical shortcomings and pitfalls).

How we conceptualize a problem also determines how we craft a solution. A good understanding of what is at stake helps ensure that we can effectively protect the interests involved. Conversely, "[m]isdiagnosing a problem makes it hard to fix."[32] With an uncertain concept, we may end up designing a policy that does not provide an adequate solution or that addresses the problem's symptoms but not its real cause. We may even distract from the problem altogether, failing to foreground the range of interconnected issues.

For these reasons and others, privacy scholars struggled for over a century to offer an adequate conceptualization of privacy. Eventually, however, after no definition managed to garner a consensus, when every effort felt over- or underinclusive, defining privacy became less and less holy a grail. Today, the field understands privacy to be an umbrella concept that spans a wide variety of issues, values, and goals. Under this approach, privacy is, at most, amenable to taxonomy.

### A. *The Field's Struggle to Define Privacy*

Scholars have not always considered the search for a definition of privacy quixotic. In the wake of a famous and early formulation of the right to privacy furnished by then–law partners Samuel Warren and Louis Brandeis in 1890,[33] several scholars set about the task of proposing an adequate and encompassing definition. Warren and Brandeis's definition is well known: The right to privacy can be understood as "the right 'to be let alone.'"[34] Yet from the start, this formulation was repeatedly criticized as too vague or as merely describing a single attribute of privacy.[35] And it was followed by innumerable efforts to identify the "essence" or "core" features of privacy.

---

32. Calo, Boundaries of Privacy Harm, supra note 20, at 1136.

33. See Warren & Brandeis, supra note 10, at 195.

34. Id. (quoting Cooley, supra note 10, at 29).

35. See, e.g., Allen, Uneasy Access, supra note 12, at 7 (stating that "[i]f privacy simply meant 'being let alone,' any form of offensive or harmful conduct directed toward another person could be characterized as a violation of personal privacy," from a "punch in the nose" to "a peep in the bedroom"); Edward J. Bloustein, Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser, 39 N.Y.U. L. Rev. 962, 970 (1964) (observing that instead of developing an understanding of privacy, Warren and Brandeis focused mostly on gaps in existing tort law); Gavison, Privacy and the Limits of Law, supra note 12, at 437–38 (arguing that "[t]he great simplicity of this definition gives it rhetorical force and attractiveness, but also denies it the distinctiveness that is necessary for the phrase to be useful in more than a conclusory sense"); Tom Gerety, Redefining Privacy, 12 Harv. C.R.-C.L. L. Rev. 233, 263 (1977) (asserting that the definition of privacy as the right to be left alone is too broad); Solove, Conceptualizing Privacy, supra note 14, at 1101 (explaining that describing privacy as the right to be let alone only describes one aspect of privacy and doesn't explain how privacy should be measured against other values or "inform us about the matters in which we should be let alone").

Attempts to conceptualize privacy during this period, while many and varied, largely follow along two veins. For one group of twentieth-century privacy theorists, control acts as a common denominator.[36] Under this view, privacy can be reduced to the control we have over information relating to or about ourselves. A second group has highlighted access as the essence of privacy.[37] Inspired by Professors Ruth Gavison and Anita Allen,[38] scholars in this tradition understand privacy to involve managing access to the self, especially to prevent unauthorized access by third parties to people's lives, feelings, personal goods and properties, and experiences.

---

36. See, e.g., Julie C. Inness, Privacy, Intimacy, and Isolation 91 (1992) (describing privacy as "the state of the agent having control over decisions concerning matters that draw their meaning and value from the agent's love, caring, or liking," including "choices on the agent's part about access to herself, the dissemination of information about herself, and her actions"); Arthur R. Miller, The Assault on Privacy 25 (1971) (characterizing privacy as "the individual's ability to control the circulation of information relating to him"); Westin, supra note 19, at 7 ("Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."); Fried, supra note 11, at 482 ("Privacy is not simply an absence of information about us in the minds of others; rather it is the *control* we have over information about ourselves."); A. Michael Froomkin, The Death of Privacy?, 52 Stan. L. Rev. 1461, 1463 (2000) (describing informational privacy as "the ability to control the acquisition or release of information about oneself"); Gerety, supra note 35, at 236 (describing privacy as "autonomy or control over the intimacies of personal identity"); Jerry Kang, Information Privacy in Cyberspace Transactions, 50 Stan. L. Rev. 1193, 1203 (1998) (characterizing information privacy as "an individual's control over the processing—i.e., the acquisition, disclosure, and use—of personal information"); Richard B. Parker, A Definition of Privacy, 27 Rutgers L. Rev. 275, 281 (1974) ("[P]rivacy is control over when and by whom the various parts of us can be sensed by others." (emphasis omitted)).

37. See, e.g., Allen, Uneasy Access, supra note 12, at 10 (noting that "a degree of inaccessibility is an important necessary condition for the apt application of 'privacy'"); Sissela Bok, Secrets 10–11 (1982) (describing privacy as "the condition of being protected from unwanted access by others—either physical access, personal information, or attention"); David M. O'Brien, Privacy, Law, and Public Policy 16 (1979) (describing privacy as "an existential condition of limited access to an individual's life experiences and engagements"); Gavison, Privacy and the Limits of Law, supra note 12, at 428 (describing privacy as "a limitation of others' access to an individual"); Jeffrey H. Reiman, Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future, 11 Santa Clara Comput. & High Tech. L.J. 27, 30 (1995) (characterizing privacy as "the condition in which other people are deprived of access to either some information about you or some experience of you"); Ernest Van Den Haag, On Privacy, *in* Nomos XIII: Privacy 149, 149 ( J. Roland Pennock & John W. Chapman eds., 1971) (describing privacy as "the exclusive access of a person (or other legal entity) to a realm of his own").

38. See generally Allen, Uneasy Access, supra note 12, at 13–17 ("My own restricted-access definition of 'privacy' is this: personal privacy is a condition of inaccessibility of the person, his or her mental states, or information about the person to the senses or surveillance devices of others."); Gavison, Privacy and the Limits of Law, supra note 12, at 423 ("Our interest in privacy, I argue, is related to our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention.").

A subset of this second vein also identifies privacy with secrecy.[39] For theorists in this tradition, privacy protects the right to conceal personal information and is violated through unwanted access or disclosure. Supreme Court jurisprudence about the third-party doctrine adheres to this notion of privacy. This doctrine holds, roughly, that there is no reasonable expectation of privacy over information that is no longer completely secret.[40] Consequently, this type of information is less likely to be protected by the Fourth Amendment.[41]

Together, control and access cover considerable ground. Yet focusing exclusively on these two approaches neglects other important conceptions of privacy. Although pivotal, conceptions of control and access largely address flows of personal information.[42] They concern the conditions

---

39. See, e.g., Adam Carlyle Breckenridge, The Right to Privacy 1 (1970) (describing privacy as "the rightful claim of the individual to determine the extent to which he wishes to share of himself with others"); Amitai Etzioni, The Limits of Privacy 196 (1999) (characterizing privacy as "the realm in which an actor (either a person or a group, such as a couple) can *legitimately* act without disclosure and accountability to others"); Richard A. Posner, Economic Analysis of Law 46 (5th ed. 1998) (describing privacy as a person's "right to conceal discreditable facts about himself"); Sidney M. Jourard, Some Psychological Aspects of Privacy, 31 Law & Contemp. Probs. 307, 307 (1966) (describing privacy as "an outcome of a person's wish to withhold from others certain knowledge as to his past and present experience and action and his intentions for the future"); Solove, Conceptualizing Privacy, supra note 14, at 1106 ("The privacy-as-secrecy conception can be understood as a subset of limited access to the self."); E.L. Godkin, Libel and Its Legal Remedy, 46 Atl. Monthly 729, 736 (1880) (characterizing privacy as "the right of every man to keep his affairs to himself, and to decide for himself to what extent they shall be the subject of public observation and discussion").

40. See, e.g., Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."); United States v. Miller, 425 U.S. 435, 443 (1976) (explaining that the Fourth Amendment doesn't protect information "revealed to a third party and conveyed by him to Government authorities," even when "revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed").

41. This rough conception is undergoing change in the digital age. See, e.g., Carpenter v. United States, 138 S. Ct. 2206, 2217, 2220 (2018) (refusing to apply the third-party doctrine to the collection of cell-site location information and noting that "when *Smith* was decided . . . few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier . . . a detailed and comprehensive record of the person's movements"); Matthew Tokson, Automation and the Fourth Amendment, 96 Iowa L. Rev. 581, 585 (2011) ("The Third Party Doctrine precedents, and *Smith* in particular, are problematic in an age where an ever-growing proportion of personal communications and transactions are carried out over the Internet.").

42. It is important to acknowledge, though, that Professors Sissela Bok's, Tom Gerety's, and Richard Parker's definitions of privacy go beyond informational privacy to include other senses of the term. See Bok, supra note 37, at 10–11 (noting that access by others may come in the form of "physical access, personal information, or attention"); Gerety, supra note 35, at 272–73 (describing "intimacies" as highly personal decisions "over which no one wishes to grant the state the right of regulation"); Parker, supra note 36, at 281 (describing being "sensed" by others as encompassing being "seen, heard, touched, smelled, or tasted" and noting that this may apply to "the parts of our bodies, our voices, and the products of our bodies," as well as "objects very closely associated with us").

under which firms, governments, and others collect, transfer, and analyze information about people and groups. Left on the table are other dimensions of privacy less focused on how or where information travels, such as decisional, physical, and proprietary privacy. As Allen rightly points out, these conceptions of privacy capture other patterns of actual usage of the term in the United States.[43]

Decisional privacy "establishes a space for manoeuvre in social action that is necessary for individual autonomy."[44] Within this ontological space, people can make decisions about life projects, modes of behavior, and ways of life without uninvited intervention. This is generally how the Supreme Court has conceptualized privacy in case law involving decisions such as intimate sexual relations, marriage, contraception, and, up until *Dobbs v. Jackson Women's Health Organization*, abortion.[45] Adopting a decisional privacy perspective in *Union Pacific Railway Co. v. Botsford*,[46] *Griswold v. Connecticut*,[47] *Eisenstadt v. Baird*,[48] *Roe v. Wade*,[49] *Planned Parenthood v. Casey*,[50] and other cases, the Court protected the freedom to make the most intimate and personal choices under the label of constitutional privacy. Professor Solove has referred to this as the "[i]ndividuality, [d]ignity, and [a]utonomy" dimension of personhood.[51]

---

43. See Anita L. Allen, Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm, 32 Conn. L. Rev. 861, 866 (2000) ("The actual contemporary usage of 'privacy' in the United States is particularly broad. 'Privacy' can mean informational privacy, but also physical, informational, and proprietary privacy.").

44. Beate Rössler, The Value of Privacy 80 (R.D.V. Glasgow trans., Polity Press 2005) (2001).

45. In *Dobbs*, the Supreme Court overturned Roe v. Wade, 410 U.S. 113 (1973), and Planned Parenthood of Southeastern Pennsylvania v. Casey, 505 U.S. 833 (1992), concluding that the right to abortion could not be constitutionally grounded in the right to privacy. Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228, 2242–43 (2022) (holding that the Constitution does not protect the right to abortion and noting that abortion is "fundamentally different" from other substantive due process rights involving sex, contraception, and marriage).

46. 141 U.S. 250, 251 (1891) (holding that ordering a plaintiff to undergo a surgical examination regarding the extent of the injury sued for violates "the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law").

47. 381 U.S. 479, 486 (1965) (holding that a Connecticut statute forbidding use of contraceptives violates "the notions of privacy surrounding the marriage relationship").

48. 405 U.S. 438, 453 (1972) (holding a ban on distribution of contraceptives to unmarried persons impermissible because "[i]f the right of privacy means anything, it is the right of the *individual* . . . to be free from unwarranted governmental intrusion into matters so fundamental[] . . . as the decision whether to bear or beget a child").

49. 410 U.S. at 153 (holding that the right to privacy encompasses a person's choice to have an abortion until the fetus becomes viable).

50. 505 U.S. at 846 (holding that "the essential holding of *Roe v. Wade* should be retained and once again reaffirmed").

51. See Solove, Conceptualizing Privacy, supra note 14, at 1116.

Physical privacy entails "allowing people who want to reduce their social interactions to choose a 'retiring' mode of life."[52] This approach, also reflected in case precedent, focuses on physical access to people and personal spaces. The tort of intrusion upon seclusion, for example, seems to adopt this conception, applying to "physical intrusion into a place"; "the use of [one's] senses, with or without mechanical aids, to oversee or overhear . . . private affairs"; and "other form[s] of investigation or examination into . . . private concerns."[53] This restrictive conception of privacy also guided the Supreme Court's reasoning in *Olmstead v. United States*,[54] though the decision was later supplanted by *Katz v. United States*.[55] In *Olmstead*, the Court held that wiretapping was not a search or seizure under the Fourth Amendment, which is addressed to searches of "material things—the person, the house, his papers or his effects."[56]

Finally, proprietary conceptions of privacy underpin the right to publicity. Initially, this dimension of privacy encompassed "issues relating to the appropriation of individuals' possessory and economic interests in their genes and other putative bodily repositories of personality."[57] Therefore, proprietary privacy concerns arose in relation to people's ownership of parts and products of their bodies, such as their genes, genomes, biobanked tissue specimens, gametes, zygotes, and frozen embryos. This conception has come to involve "control over names, likenesses, and repositories of personal identity" as well[58] and may be vindicated through the tort of appropriation of name or likeness.[59]

Scholars have introduced important variants and subcategories to these traditional dimensions of privacy. Professor Neil Richards, for example, refers to intellectual privacy, defining it as "the ability, whether protected by law or social circumstances, to develop ideas and beliefs away

---

52. Richard A. Posner, Privacy, Secrecy, and Reputation, 28 Buff. L. Rev. 1, 5 (1979) [hereinafter Posner, Privacy, Secrecy, and Reputation].

53. See Restatement (Second) of Torts § 652B cmt. b (Am. L. Inst. 1977).

54. 277 U.S. 438, 466 (1928).

55. In *Katz*, the Supreme Court overturned *Olmstead*, holding that, since the Fourth Amendment protects people rather than places, its reach "cannot turn upon the presence or absence of a physical intrusion into any given enclosure." Katz v. United States, 389 U.S. 347, 353 (1967). Consequently, the *Katz* Court determined that attaching an eavesdropping device to the outside of a public phone booth used by the petitioner breached the privacy on which the petitioner justifiably relied while using the telephone booth and thus violated the Fourth Amendment. Id.

56. 277 U.S. at 464.

57. Anita L. Allen, Genetic Privacy: Emerging Concepts and Values, *in* Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era 31, 34 (Mark A. Rothstein ed., 1997) [hereinafter Allen, Genetic Privacy].

58. Anita L. Allen, Coercing Privacy, 40 Wm. & Mary L. Rev. 723, 723–24 (1999).

59. See Restatement (Second) of Torts § 652C (Am. L. Inst. 1977).

from the unwanted gaze or interference of others."[60] Professor Danielle Keats Citron calls for the protection of sexual privacy, involving the "social norms (behaviors, expectations, and decisions) that govern access to, and information about, individuals' intimate lives."[61] Interestingly, these novel variants bring together two or more elements of the previously described conceptions of privacy. Neither Richards nor Citron purports to define privacy generally—only to acknowledge and develop an undertheorized dimension.

### B. *A Pragmatic Approach to Conceptualizing Privacy*

Ultimately, a shared and satisfying definition of the concept of privacy has proven elusive. The various—and sometimes competing and contradictory[62]—dimensions of privacy (informational, decisional, physical, and proprietary) are hard to cover with a singular characterization.[63]

Solove (and not just he[64]) sees a futility in the search for the "essence" of privacy. In Solove's view, any selected common denominator of privacy (e.g., control, access, or secrecy) will wind up being either too narrow to include other aspects of privacy; too broad to exclude matters that are not considered private; or too vague to specify what types of information, behaviors, expectations, and decisions are protected.[65] Thus, in 2002, Solove came up with a pragmatic solution: Privacy is better understood by drawing

---

60. Neil M. Richards, Intellectual Privacy, 87 Tex. L. Rev. 387, 389 (2008) [hereinafter Richards, Intellectual Privacy]; see also Neil M. Richards, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age 5 (2015) [hereinafter Richards, Rethinking Civil Liberties] ("Intellectual privacy is protection from surveillance or interference when we are engaged in the processes of generating ideas—thinking, reading, and speaking with confidants before our ideas are ready for public consumption.").

61. Danielle Keats Citron, Sexual Privacy, 128 Yale L.J. 1870, 1874 (2019).

62. Robert C. Post, Three Concepts of Privacy, 89 Geo. L.J. 2087, 2087 (2001) (reviewing Jeffrey Rosen, The Unwanted Gaze (2000)) (explaining how privacy is "entangled in competing and contradictory dimensions").

63. As Solove points out, though, there have been some efforts to group these different dimensions. Solove, Conceptualizing Privacy, supra note 14, at 1125 ("Other scholars also recognize that privacy cannot be consolidated into a single conception, and instead they cluster together certain of the conceptions."); see also Judith Wagner DeCew, In Pursuit of Privacy 73–80 (1997) (identifying the categories of informational privacy, accessibility privacy, and expressive privacy); Allen, Genetic Privacy, supra note 57, at 33 (identifying decisional privacy, physical privacy, informational privacy, and proprietary privacy); Anita L. Allen, Taking Liberties: Privacy, Private Choice, and Social Contract Theory, 56 U. Cin. L. Rev. 461, 461, 464–66 (1987) (noting two usages of privacy that have emerged in the law: "conditions of restricted access" and liberty from "interference with decisionmaking and conduct, especially respecting appropriately private affairs"); Kang, supra note 36, at 1202–05 (identifying the categories of physical space, choice, and "flow of personal information").

64. See, e.g., Hartzog, supra note 21, at 1679 (arguing that "a broad and singular conceptualization of privacy is unhelpful for legal purposes").

65. Solove, Conceptualizing Privacy, supra note 14, at 1099–124.

from philosopher Ludwig Wittgenstein's notion of "family resemblances."[66] According to Wittgenstein's account, certain concepts might not have a single common characteristic but might instead draw from a common pool of similar elements.[67] Therefore, members of a family share "overlapping and criss-crossing" characteristics instead of an essential element.[68]

Building on this theory and other aspects of pragmatism[69] familiar to lawyers since the turn of the twentieth century,[70] Solove proposed a "method of philosophical inquiry" to understand privacy from the bottom up in specific contextual situations.[71] On this view, we should conceptualize privacy by (1) examining specific problematic situations that involve "disruptions to certain practices";[72] (2) focusing on the specific types of disruption (privacy invasions) and the specific practices (private matters[73]) disrupted; and (3) evaluating the latter "empirically, historically, and normatively."[74] "If privacy is conceptualized as a web of interconnected types of disruption of specific practices," argued Solove, "then the act of conceptualizing privacy should consist of mapping the typography of the web."[75]

In 2006, as an alternative to defining privacy, Solove published *A Taxonomy of Privacy*, an article proposing a taxonomy of activities that pose privacy problems.[76] According to Solove, the many troubling activities recognized under the rubric of privacy differ from one another but share enough commonalities to bear a "family resemblance."[77] In this sense, privacy problems become "a cluster of related activities that impinge upon

66. Ludwig Wittgenstein, Philosophical Investigations §§ 66–67 (G.E.M. Anscombe trans., 3d ed. 1967).

67. See id.

68. See id.

69. Solove, Conceptualizing Privacy, supra note 14, at 1127 ("My approach to conceptualizing privacy draws from a few recurring ideas of pragmatism: a recognition of context and contingency, a rejection of a priori knowledge, and a focus on concrete practices." (footnote omitted)).

70. See Menand, supra note 15, at 337–75, 435–42 (explaining that this familiarity was fostered through Justice Holmes, Jr., who was a student, friend, or contemporary of public intellectuals John Dewey, Charles Peirce, Jane Addams, and others).

71. Solove, Conceptualizing Privacy, supra note 14, at 1154–55.

72. Id. at 1129 (explaining that the "practices" encompass "various activities, customs, norms, and traditions," such as "writing letters, talking to one's psychotherapist, engaging in sexual intercourse, making certain decisions, and so on").

73. Solove has acknowledged that this cannot be a fixed term, since the matters we consider private change over time as well as across cultures and historical periods. In that sense, "there is no consistent set of practices that should be considered private." Id. at 1142.

74. Id.

75. Id. at 1130.

76. Solove, Taxonomy of Privacy, supra note 14, at 482.

77. Id. at 486.

people in related ways,"[78] and privacy "an umbrella term, referring to a wide and disparate group of related things."[79]

What are those activities, and how are they related? Using *social recognition* as the determining criterion, Solove identified in 2006 a total of sixteen harmful activities,[80] classifying them in four basic groups.[81] Solove explained that

> [a]lthough the primary focus will be on the law, this taxonomy is not simply an attempt to catalog existing laws, as was Prosser's purpose. Rather, it is an attempt to understand various privacy harms and problems *that have achieved a significant degree of social recognition*. I will frequently use the law as a source for determining what privacy violations society recognizes. However, my aim is not simply to take stock of where the law currently stands today, but to provide a useful framework for its future development.[82]

Based on what jurists and scholars had discussed under the rubric of privacy as of the time of his article, Solove furnished courts, lawmakers, and scholars with a taxonomy intended to serve as a framework to address privacy violations.[83] The taxonomy not only catalogues the activities of individuals, corporations, and the government that can cause privacy problems but also identifies possible privacy harms (both dignitary and architectural) that can be derived from each type of activity. Solove's ultimate purpose was to enable us all to "see privacy in a more multidimensional way."[84]

Taxonomies were not an entirely new phenomenon in privacy. After reviewing more than three hundred cases, Prosser concluded in 1960 that the law of privacy consisted of four types of invasions of four distinct inter-

---

78. Id. at 484.

79. Id. at 486; see also Danielle Keats Citron & Daniel J. Solove, Privacy Harms, 102 B.U. L. Rev. 793, 830 (2022) [hereinafter Citron & Solove, Privacy Harms] ("Privacy is an umbrella concept that encompasses different yet related things.").

80. These activities are: surveillance, interrogation, aggregation, identification, insecurity, secondary use, exclusion, breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, distortion, intrusion, and decisional interference. Solove, Taxonomy of Privacy, supra note 14, at 490–91.

81. The four basic groups are: information collection, information processing, information dissemination, and invasion. Id. at 489.

82. Id. at 484 (emphasis added).

83. According to Solove,

> The full equation for a privacy violation or problem is the existence of a certain activity that causes harms or problems affecting a private matter or activity. This taxonomy focuses on the first part of the equation (harmful or problematic activities) rather than on what constitutes a private matter or activity.

Id. at 484 n.27.

84. Id. at 562.

ests: intrusion upon seclusion, public disclosure, false light, and appropriation.[85] Prosser's criterion for recognition was court precedent.[86] And as part of his renowned 1967 book *Privacy and Freedom*, Westin proposed a taxonomy of privacy attitudes, identifying four psychological conditions or states of individual privacy that a person might strive for at different times or in different circumstances: solitude, intimacy, reserve, and anonymity.[87]

Yet Solove's ambitions were greater still: He sought to reorient privacy from an individual concept based on formal definitional criteria to an umbrella concept based in social recognition. And more so than Prosser or Westin, Solove's taxonomic approach appears to have exerted an extraordinary influence on the shape and scope of contemporary privacy law scholarship—the subject of the next section.

### C. *The New Boundaries of Privacy Law Scholarship*

Solove's approach of foregrounding troublesome activities and harms and eschewing boundaries appears to have helped the field of privacy law grow and evolve. "By getting us past the threshold question of what privacy is," wrote Hartzog in a recent essay recognizing Solove's profound influence, "Solove's work provides room for scholars and lawmakers to tackle bigger phenomena."[88]

Making peace with the uncertainty about privacy's core elements has relieved scholars and policymakers of a stressful intellectual burden. In particular, it has freed scholars to explore and engage in broader discussions around concepts such as informational capitalism[89] and the role of information in racial, gender, and other forms of discrimination.[90] Novel data-exploitation practices—from data mining to the application of machine learning and artificial intelligence to consumer and government decisionmaking—have become fundamental to privacy discourse, resulting in a Cambrian explosion of topics. Over the last twenty years, American privacy scholars have started to study the use of automated hiring processes, watchlists, air passenger screening, price discrimination in

85. See Prosser, supra note 18, at 389.

86. See id. at 388–89 ("Today, with something over three hundred cases in the books, the holes in the jigsaw puzzle have been largely filled in, and some rather definite conclusions are possible. What has emerged from the decisions is no simple matter. It is not one tort, but a complex of four.").

87. See Westin, supra note 19, at 31.

88. Hartzog, supra note 21, at 1687.

89. See generally Julie E. Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism 1 (2019) (arguing that "[t]o understand what technology signifies for the future of law, we must understand how the design of networked information technologies within business models reflects and reproduces economic and political power").

90. See Hartzog, supra note 21, at 1687 (explaining that Solove's work has facilitated scholars' interrogation of the way in which "capitalistic incentives cause companies to leverage information in harmful ways . . . and how marginalized populations are affected first and hardest by privacy-invasive actors").

e-commerce, digital redlining (also known as "weblining"[91]), genetic discrimination by insurers and employers, social scoring, online harassment, the attention economy, content personalization, targeted advertising, recidivism predictions, the influence of algorithms on political and dating decisions, mis- and disinformation, dark patterns, and more.[92]

As part of this process, novel harms from emerging technology, especially algorithms, have been adopted into the privacy family. For some time now, the field has been undergoing an "algorithmic turn."[93] Partly enabled

---

91. Paul M. Schwartz, Beyond Lessig's *Code* for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices, 2000 Wis. L. Rev. 743, 757 (defining "weblining" as the "Information Age version of that nasty old practice of redlining, where lenders and other businesses mark whole neighborhoods off-limits" (internal quotation marks omitted) (quoting Marcia Stepanek, Weblining, Bus. Wk. (Apr. 3, 2000), https://www.bloomberg.com/news/articles/2000-04-02/weblining (on file with the *Columbia Law Review*))).

92. See, e.g., Danielle Keats Citron, The Fight for Privacy, at xii (2022) (delineating "intimate privacy," or the "social norms (attitudes, expectations, and behaviors) that set and fortify the boundaries around our intimate lives," encompassing "the extent to which others have access to, and information about, our bodies; minds (thoughts, desires, and fantasies); health; sex, sexual orientation, and gender; and close relationships"); Neil Richards, Why Privacy Matters 141 (2021) [hereinafter Richards, Why Privacy Matters] (describing "liquid surveillance," or "the spread of surveillance beyond government spying to a sometimes private surveillance in which surveillance subjects increasingly consent and participate"); Ifeoma Ajunwa, An Auditing Imperative for Automated Hiring Systems, 34 Harv. J.L. & Tech. 621, 625, 628 (2021) (arguing for mandated auditing of automated hiring systems and updates to antidiscrimination law that acknowledge this duty while also taking workers' data privacy interests seriously); Ifeoma Ajunwa, Kate Crawford & Jason Schultz, Limitless Worker Surveillance, 105 Calif. L. Rev. 735, 738–39 (2017) (noting that "rapid technological advancements and diminishing costs now mean employee surveillance occurs both inside and outside the workplace—bleeding into the private lives of employees"); Anita L. Allen, Dismantling the "Black Opticon": Privacy, Race Equity, and Online Data-Protection Reform, 131 Yale L.J. Forum 907, 911 (2022), https://www.yalelawjournal.org/pdf/F7.AllenFinalDraftWEB_6f26iyu6.pdf [https://perma.cc/LQ7Z-VVL5] (describing the "Black Opticon," which the author uses "to denote the complex predicament of African Americans' vulnerabilities to varied forms of discriminatory oversurveillance, exclusion, and fraud — aspects of which are shared by other historically enslaved and subordinated groups in the United States and worldwide"); Danielle Keats Citron & Frank Pasquale, The Scored Society: Due Process for Automated Predictions, 89 Wash. L. Rev. 1, 3 (2014) (describing the growing use of predictive algorithms and "scoring" that mine a person's personal on- and offline activities); Margaret Hu, Big Data Blacklisting, 67 Fla. L. Rev. 1735, 1738 (2015) (describing the privacy and liberty implications of the government's big data blacklisting programs, such as air passenger screenings); Matthew Tokson, Inescapable Surveillance, 106 Cornell L. Rev. 409, 412 (2021) (arguing against the adoption of an "inescapable" standard for evaluating personal data disclosures under the Fourth Amendment); Tal Z. Zarsky, "Mine Your Own Business!": Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion, 5 Yale J.L. & Tech. 1, 5 (2003) [hereinafter Zarsky, Mine Your Own Business] (arguing that "[i]n the interaction between [data mining] and traditional privacy claims, we should pay special attention to public opinion").

93. See María P. Angel, Privacy's Algorithmic Turn, 30 B.U. J. Sci. & Tech. L. (forthcoming 2024) (manuscript at 2), https://ssrn.com/abstract=4602315 [https://perma.cc/73QT-G953] (describing a transformation in American privacy law scholars' conception of

by privacy's multidimensionality and lack of clear boundaries—what Professor David Pozen refers to as the "pluralistic turn"[94]—scholars have begun to identify different types of information-based harms as privacy harms without reference to any specific criteria. Though examples of this sociotechnical phenomenon abound, this Essay focuses on two recently labeled privacy harms: *information-based discrimination* and *algorithmic manipulation*.[95] The Essay frequently returns to these two harms in the following pages to illustrate how the boundaries of privacy law scholarship have broadened over time.

---

information privacy); Hartzog, supra note 21, at 1681 (noting the "algorithmic turn in privacy scholarship, which opened the door for discussions of how privacy issues impact marginalized and vulnerable populations"). Although she does not do so in relation to privacy, Professor Ifeoma Ajunwa also uses the term "algorithmic turn" to refer to "the profusion of algorithmic decision-making in our daily lives, even in the absence of established regulatory or ethical frameworks to guide the deployment of those algorithms." See Ifeoma Ajunwa, The Paradox of Automation as Anti-Bias Intervention, 41 Cardozo L. Rev. 1671, 1683–84 (2020).

94. See Pozen, supra note 20, at 225 (defining the "pluralistic turn" as many privacy theorists' tendency to "reject[] approaches to privacy that strive to identify its essence or its core characteristics and settling, instead, 'on an understanding of privacy as an umbrella term that encompasses a variety of related meanings'" (quoting Richards, Rethinking Civil Liberties, supra note 60, at 9)).

95. Procedural unfairness is yet another area of study pursued by privacy scholars. See, e.g., Kate Crawford & Jason Schultz, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, 55 B.C. L. Rev. 93, 109 (2014) (arguing for "procedural data due process," which would "regulate the fairness of Big Data's analytical processes with regard to how they use personal data . . . in any adjudicative process, including processes whereby Big Data is being used to determine attributes or categories for an individual"). Coined by Citron in 2008, "technological due process" refers to restoring constitutional or statutory process guarantees in light of technological change. See Danielle Keats Citron, Technological Due Process, 85 Wash. U. L. Rev. 1249, 1258, 1305–13 (2008) [hereinafter Citron, Technological Due Process] (highlighting the threat automation poses to procedural due process and suggesting new procedural models). Scholars in this area write about the ways law and code interact within algorithmic or software-based decisionmaking to deny people the ability to understand or challenge adverse decisions. See, e.g., Ryan Calo & Danielle Keats Citron, The Automated Administrative State: A Crisis of Legitimacy, 70 Emory L.J. 797, 800 (2021) (describing problems caused by automation of public benefits determinations, including the difficulty of challenging decisions); Daniel J. Steinbock, Data Matching, Data Mining, and Due Process, 40 Ga. L. Rev. 1, 3 (2005) ("We have entered the age of decision by algorithm—the computer application of statistical formulas to large bodies of data to identify relationships or patterns.").

The technological due process conversation has spilled over into many other disciplines and contexts. See, e.g., Aparna Balagopalan, Haoran Zhang, Kimia Hamidieh, Thomas Hartvigsen, Frank Rudzicz & Marzyeh Ghassemi, The Road to Explainability Is Paved With Bias: Measuring the Fairness of Explanations, 2022 Ass'n for Computing Mach. Conf. on Fairness Accountability & Transparency 1194, 1202(demonstrating how "[u]nfair explanation models can have negative effects on real-world decision making"); Gayane Grigoryan, Explainable Artificial Intelligence: Requirements for Explainability, 2022 Ass'n for Computing Mach. SIGSIM Conf. on Principles of Advanced Discrete Simulation 27, 27–28 (identifying four requirements that have to be met for the information provided by a machine-learning model to be considered explainable).

Information-based discrimination harms encompass the unequal treatment of members of marginalized communities (such as women, sexual and gender minorities, and people of color) that results from profiling, the misuse of their personal information, or both.[96] They can also refer to privacy violations' disproportionate effects on marginalized populations. This disparate treatment (or the disparate effects of apparently neutral processing of information) can lead to loss of opportunities—such as education, jobs, promotions, housing, and affordable insurance—and can increase exposure to certain types of targeting (such as policing, surveillance, airport scrutiny, price discrimination, vicious online harassment, and cybermobbing).[97] Likewise, information-based discrimination harms can exacerbate disadvantages and patterns of inequality that members of these groups already experience and even cause psychological harms through the "searing wound of stigma, shame, and loss of esteem that can turn into permanent scars."[98]

Algorithmic manipulation refers to the use of personal information, data mining tools, and cognitive and behavioral science tactics to unacceptably influence people's decisions or behaviors, impairing their autonomy and free will.[99] Either by taking advantage of a person's cognitive limitations or contextual vulnerabilities[100] or by influencing the way in which they would normally behave or make choices, these techniques leverage information to channel behavior and bypass the person's

---

96. See Zarsky, Mine Your Own Business, supra note 92, at 22 (explaining how vendors use data to profile and discriminate between present and prospective customers, such as by promoting certain products or creating pricing schemes).

97. For example, Professor Andrew Guthrie Ferguson describes how big data policing disproportionally affects poor people and people of color. See Andrew Guthrie Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement 93 (2017) ("By and large, it is people of color who are populating the growing police databases. If these racially skewed databases of past police contacts become the justification for future police contacts, then biased data collection will distort police suspicion."). Similarly, Citron explains how cyberharassment and cyberstalking disproportionately target women. Danielle Keats Citron, Hate Crimes in Cyberspace 13–14 (2014) (discussing various studies showing that women are more at risk for cyberstalking and noting that "for lesbian, transgender, or bisexual women and women of color, the risk may be higher").

98. Citron & Solove, Privacy Harms, supra note 79, at 855–56.

99. See Neil Richards & Woodrow Hartzog, A Duty of Loyalty for Privacy Law, 99 Wash. U. L. Rev. 961, 967 (2021) [hereinafter Richards & Hartzog, A Duty of Loyalty] ("Insufficiently constrained by the law, companies can deploy a potent cocktail of techniques derived from cognitive and behavioral science to 'nudge' or otherwise influence the choices we make.").

100. See Ryan Calo, Digital Market Manipulation, 82 Geo. Wash. L. Rev. 995, 1001 (2014) [hereinafter Calo, Digital Market Manipulation] (explaining that "companies and other firms will use what they know about human psychology to set prices, draft contracts, minimize perceptions of danger or risk, and otherwise attempt to extract as much rent as possible from their consumers"); Shaun B. Spencer, The Problem of Online Manipulation, U. Ill. L. Rev. 959, 980 ("[M]arketers can already identify some individual biases and vulnerabilities in real time, and the emerging research suggests that they will rapidly expand their ability to do so.").

capacity for reflection and deliberation.[101] Such techniques "circumvent[] the subject's rational decision-making process,"[102] leading the subject to depart from the self-interested course they would usually follow[103] and turning them into a puppet.[104] As a result, scholars argue, the person's behaviors or decisions end up playing to their disadvantage, in favor of the manipulator's ends and preferences.[105]

1. *Information-Based Discrimination's Path Into the Privacy Literature.* — Information-based discrimination did not appear in Solove's original taxonomy but quickly came to be represented in the literature.[106] In particular, the idea that information-based discrimination constitutes a core privacy concern has intensified in the last decade. In 2014, for example, Professors Kate Crawford and Jason Schultz proposed the term "predictive privacy harms" to describe harms that, although not necessarily within the conventional conception of privacy boundaries, "are still derived from collecting and using information that centers on an individual's data behaviors."[107] While describing this new type of harm—which results from "[t]he generative data-making practices of Big Data"[108]—they made clear that predictive privacy harms can manifest as discriminatory practices.[109] Similarly, Professor Frederik Zuiderveen Borgesius included discrimination as one of the three "privacy problems" addressed in his 2015 book about privacy in behavioral targeting (along with chilling

---

101. See Cass R. Sunstein, Fifty Shades of Manipulation, 1 J. Mktg. Behav. 213, 216 (2015) (suggesting that "an effort to influence people's choices counts as manipulative to the extent that it does not sufficiently engage or appeal to their capacity for reflection and deliberation" (emphasis omitted)).

102. See Spencer, supra note 100, at 989.

103. See Calo, Digital Market Manipulation, supra note 100, at 1033 (describing digital market manipulation's goal of catching a consumer in a moment of irrationality and seizing upon that vulnerability to turn a profit).

104. See Citron & Solove, Privacy Harms, supra note 79, at 846 ("A coerced person understands that they are coerced; on the other hand, a manipulated person might not realize that they are being turned into a puppet . . . .").

105. See Calo, Digital Market Manipulation, supra note 100, at 1030 ("All that is necessary to trigger either category of privacy harm is the belief or actuality that the person is being disadvantaged—that her experience is changing in subtle and material ways to her disadvantage.").

106. As Part II explores, there were already examples in the literature (by Professors Batya Friedman, Helen Nissenbaum, and Tal Zarsky)—but they did not amount to enough social recognition to be considered significant enough for inclusion in the taxonomy. See infra Part II.

107. Crawford & Schultz, supra note 95, at 95; see also Alicia Solow-Niederman, Information Privacy and the Inference Economy, 117 Nw. U. L. Rev. 357, 361 (2022) (discussing the rise of the "inference economy in which organizations use available data collected from individuals to generate further information about both those individuals and about other people" (emphasis omitted)).

108. Crawford & Schultz, supra note 95, at 105.

109. Id. at 99.

effects and a lack of control over data).[110] And in his 2019 article *Antidiscriminatory Privacy*, Professor Ignacio Cofone claimed that "discrimination can also be viewed as an information problem" and can therefore be addressed through antidiscriminatory privacy rules.[111]

Information-based discrimination has also been linked to privacy during this period in other ways. Scholars may not explicitly frame discrimination as a privacy harm, but they do present discrimination as a consequence of one of the activities at the heart of many privacy problems: surveillance. In his 2020 book *Privacy at the Margins*, Professor Scott Skinner-Thompson argued that "privacy can serve as a liminal or transitional right [against surveillance] until [marginalized] communities gain both formal antidiscrimination protections and lived equality."[112] The same can be seen outside of legal academia. For instance, in Professor Simone Browne's book *Dark Matters: On the Surveillance of Blackness*, Browne proposed the concept of "racializing surveillance" to describe "those moments when enactments of surveillance reify boundaries, borders, and bodies along racial lines, and where the outcome is often *discriminatory treatment* of those who are negatively racialized by such surveillance."[113]

Yet another line of scholarship relates discrimination with privacy harms through the disproportionate effects that privacy violations have on certain minority groups.[114] Mothers experiencing poverty, for example, have been dispossessed of privacy rights, argues Professor Khiara M. Bridges's magisterial book *The Poverty of Privacy Rights*, in part because their economic position is considered indicative of "flawed character."[115] These mothers are trapped in a catch-22 that makes it impossible for them to escape invasive state intrusion, whether or not they receive public assistance.[116] Professor Christen A. Smith has described Black women's right to be let alone as an "impossible privacy": Police violence against Black women tends to happen in "homes

110. Frederik J. Zuiderveen Borgesius, Improving Privacy Protection in the Area of Behavioural Targeting 2 (2015).

111. See Ignacio N. Cofone, Antidiscriminatory Privacy, 72 SMU L. Rev. 139, 142 (2019).

112. Scott Skinner-Thompson, Privacy at the Margins 181 (2020).

113. Simone Browne, Dark Matters: On the Surveillance of Blackness 16 (2015) (emphasis added).

114. Professors Michele Gilman and Rebecca Green refer to this line of scholarship with the term "differentiated privacy harms," or "the idea that different groups experience privacy harms in different ways." See Michele Gilman & Rebecca Green, The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization, 42 N.Y.U. Rev. L. & Soc. Change 253, 281 (2018).

115. Khiara M. Bridges, The Poverty of Privacy Rights 9 (2017).

116. Id. at 9–10 (explaining that mothers experiencing poverty "lose their privacy if they accept government assistance (because safety net programs demand access to private areas of beneficiaries' lives)" but also if they reject it, as "they will be unable to provide their children with basic necessities, thus making them vulnerable to . . . CPS").

and in what should be private places."[117] Professors Michele Gilman and Rebecca Green, in turn, shine a light on a countervailing reality—namely, the "discrimination that arises from the lack of data inputs from marginalized groups."[118] For Gilman and Green, this type of information inequality or "surveillance gap"—faced by many undocumented people, day laborers, people experiencing homelessness, people with conviction histories, and others—should also be considered a privacy concern.[119]

2. *The Emergence of Algorithmic Manipulation as a Privacy Issue.* — As with information-based discrimination, many scholars today understand algorithmic manipulation as a privacy problem. For example, Professor Ido Kilovaty has called attention to the challenges online manipulation poses to privacy, autonomy, and democracy.[120] Similarly, Professors Sandra Wachter and Brent Mittelstadt have argued that "due to companies' widespread implementation of inferential analytics for profiling, nudging, *manipulation*, or automated decision-making, these 'private' decisions can, to a large extent, impact the privacy of individuals."[121] The prospect of extractive manipulation also sits at the heart of Professor Shoshana Zuboff's popular summative work *The Age of Surveillance Capitalism*.[122]

Additionally, another line of scholarship has started to see algorithmic manipulation as a danger against which privacy can protect. In his recent book *Why Privacy Matters*, Richards framed blackmailing, discrimination, and manipulation as the "dangers of surveillance" against which privacy serves as a bulwark.[123] Similarly, Professor Shaun B. Spencer

---

117. Christen A. Smith, Impossible Privacy: Black Women and Police Terror, 51 Black Scholar no. 1, 2021, at 20, 21 ("We are not safe in our homes because there is no such thing as privacy for Black women, at least in the eyes of the state. Ours is an impossible privacy.").

118. See Gilman & Green, supra note 114, at 286.

119. See id. at 295 ("The surveillance gap is not a failure to adhere to privacy norms, but rather a failure—be it purposeful or accidental, benign or malignant—of data and information to follow the same flows for residents of the surveillance gap as nonresidents.").

120. See Ido Kilovaty, Legally Cognizable Manipulation, 34 Berkeley Tech. L.J. 449, 468–73 (2019) (arguing that online manipulation "impairs the ability of individuals to make independent and informed opinions and decisions," which, collectively, may distort the democratic process).

121. Sandra Wachter & Brent Mittelstadt, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI, 2019 Colum. Bus. L. Rev. 494, 541 (emphasis added).

122. See Shoshana Zuboff, The Age of Surveillance Capitalism 8 (2019) ("[T]he most-predictive behavioral data come from intervening in the state of play in order to nudge, coax, tune, and herd behavior toward profitable outcomes. Competitive pressures produced this shift, in which automated machine processes not only *know* our behavior but also *shape* our behavior at scale.").

123. Richards, Why Privacy Matters, supra note 92, at 146–62 (asserting that privacy protections can help prevent the types of discrimination, sorting, and inequality threatened by new technologies).

has recommended "using the threat of online manipulation as another argument for comprehensive regulation of the data sharing ecosystem."[124]

Finally, scholars have also related manipulation to privacy when it comes to the use of manipulative techniques to induce consumers to consent to the collection and processing of their personal data. For example, privacy scholars Alessandro Acquisti, Curtis Taylor, and Liad Wagman have underscored how "the same policy can nudge individuals to disclose varying amounts of personal data simply by manipulating the format in which the policy itself is presented to users."[125] In a similar vein, Professor Julie Cohen has highlighted how the design of digital interactive environments can be used to manipulate consumers and encourage "broad forward-looking consent to processing and use."[126]

Hartzog credits Solove for opening the door to new types of privacy harms.[127] Indeed, it does appear as though information-based discrimination and algorithmic manipulation have come to be recognized over time by the right people and institutions as privacy problems. In fact, a recent paper by Solove and Citron outlines a "typology" of privacy harms that explicitly includes algorithmic manipulation and discrimination alongside legacy concerns.[128] Despite the lack of specific criteria, these problems, as well as many others, have made it into the taxonomy—adopted into the family, so to speak. But hasn't the taxonomic approach to privacy begun to wear thin? This is the subject to which this Essay turns next.

## II. THE TROUBLE WITH SOCIAL TAXONOMY

Though it facilitated the growth and proliferation of privacy scholarship, the big-tent taxonomic approach has come at a cost to the field. A deeper look into the recent evolution of privacy law—including the adoption of discrimination and algorithmic manipulation into the privacy family—casts doubts on the wisdom of using social recognition as the sole gatekeeper for the field. Social recognition alone cannot furnish a principled approach for determining whose voices are heard and valued when it comes to identifying new privacy harms. Nor does the taxonomic approach provide a framework for recognizing or addressing the internal tensions between conflicting values included in the growing privacy family.

---

124. Spencer, supra note 100, at 1001–02.

125. Alessandro Acquisti, Curtis Taylor & Liad Wagman, The Economics of Privacy, 54 J. Econ. Literature 442, 480 (2016) (citing Idris Adjerid, Alessandro Acquisti, Laura Brandimarte & George Loewenstein, Sleights of Privacy, Symposium on Usable Privacy and Security (SOUPS), July 2013, at 1, 2).

126. Julie E. Cohen, Turning Privacy Inside Out, 20 Theoretical Inquiries L. 1, 7 (2019).

127. See Hartzog, supra note 21, at 1681 (explaining that conceiving of privacy as "a pluralistic, fluid concept . . . furthers diverse values and is capable of having both intrinsic and utilitarian worth and coexisting with many different policy goals," which allows us to "solve complex information problems without constantly relitigating privacy's meaning").

128. Citron & Solove, Privacy Harms, supra note 79, at 831 fig.1, 846, 855.

For the reasons that follow, privacy's big-tent approach has begun to show rips in its fabric.

### A. *The Limits of Social Recognition*

To welcome a new harm into the privacy family, the taxonomic approach asks whether the right people or institutions talk about it as involving privacy. But what does it take for an information-based phenomenon to achieve a significant degree of social recognition as a privacy harm? Whose attention counts as valuable? How much talk is enough to be considered significant?

The big privacy tent Solove envisioned in 2006 sheltered one set of privacy problems.[129] Today's tent has welcomed several more, not because the problems did not exist in 2006 but because the core privacy community did not talk about them enough or in the right way. Meanwhile, other kinds of information-based harms still do not count as privacy problems because they haven't been socially recognized as such.[130]

A taxonomic approach to privacy grounded in social recognition may relieve the burden of defining privacy but necessarily raises a range of critical and unanswered questions about legitimacy and authority in the field. Who decides how much recognition is enough for a harm to be considered a privacy harm? Whose recognition counts? Whose approaches are sidelined? Current answers to these interrogations might reflect "imbedded hierarchical racist [sexist, homophobic, etc.] paradigms that currently exist in our society."[131]

Critically assessing these answers would allow the field to engage with criticism and insights coming from critical race and feminist theorists in the context of diversity and inclusivity in academia.[132] Interrogating the

---

129. See supra notes 14–17 and accompanying text.

130. See infra section II.A.3.

131. See Payne Hiraldo, The Role of Critical Race Theory in Higher Education, 31 Vt. Connection 53, 55 (2010).

132. See Angela P. Harris & Carmen G. González, Introduction to Presumed Incompetent: The Intersections of Race and Class for Women in Academia 1, 8 (Gabriella Gutiérrez y Muhs, Yolanda Flores Niemann, Carmen G. González & Angela P. Harris eds., 2012) ("[W]hat is required is transforming academic culture so that it welcomes and embraces those who are currently regarded as 'other' and increases the opportunity for alternative points of view to challenge dominant ideologies and deep-rooted social hierarchies."); Dolores Delgado Bernal & Octavio Villalpando, An Apartheid of Knowledge in Academia: The Struggle Over the "Legitimate" Knowledge of Faculty of Color, 35 Equity & Excellence Educ. 169, 176–77 (2002) ("[B]y marginalizing the knowledges of faculty of color, higher education has created an apartheid of knowledge where the dominant Eurocentric epistemology is believed to produce 'legitimate' knowledge, in contrast to the 'illegitimate' knowledge that is created by all other epistemological perspectives."); Hiraldo, supra note 131, at 54–58 (using the tenets of critical race theory to evaluate the racist perspectives embedded in higher education programs and highlight how to overcome these inequitable policies); Caroline Sotello Viernes Turner, Samuel L. Myers, Jr. & John W. Creswell, Exploring Underrepresentation: The Case of Faculty of Color in the Midwest, 70 J. Higher

"social recognition" approach at the heart of the social taxonomy may contribute to "revealing the social inequities that exist within the structure of higher education"[133] and, in particular, within "the traditionally white male establishment of legal academia."[134] The time has come to be wary of social recognition as the "sacred canon[] of objective truth"[135] and the sole gatekeeper for the privacy field.

As explained in section I.C, information-based discrimination and algorithmic manipulation have come to be recognized as privacy harms in the last few years. Sections II.A.1 and II.A.2, however, seek to show how both harms had been addressed in other fields' literature—and even in the privacy law field—for a long time before. Why, then, didn't they find their way into Solove's taxonomy of privacy in 2006? Similarly, section II.A.3 provides examples of other information-based harms that, despite being present in the privacy field for a while, were not included in Solove and Citron's 2022 typology of privacy harms.[136] What amount of social

---

Educ. 27, 28 (1999) ("Challenges to the successful recruitment, retention, and development of faculty of color include . . . a pervasive racial and ethnic bias that contributes to unwelcoming and unsupportive work environments for faculty of color.").

133. See Hiraldo, supra note 131, at 57.

134. See Meera E. Deo, The Ugly Truth About Legal Academia, 80 Brook. L. Rev. 943, 951 (2015) (presenting evidence of the many ways in which racial and gender discrimination persist in legal academia). See generally Marina Angel, Women in Legal Education: What It's Like to Be Part of a Perpetual First Wave or the Case of the Disappearing Women, 61 Temp. L. Rev. 799 (1988) (analyzing data at five law schools to identify barriers to women in law schools, both as faculty members and students); Katherine Barnes & Elizabeth Mertz, Is It Fair? Law Professors' Perceptions of Tenure, 61 J. Legal Educ. 511 (2012) ("[F]emale professors and professors of color perceive the tenure process more negatively than their white male counterparts across cohorts, with some changes in the strength of these differences over time. But the nuance of when an individual was reviewed for tenure is quite important in describing that individual's perceptions."); Richard Delgado, Minority Law Professors' Lives: The Bell–Delgado Survey, 24 Harv. C.R.-C.L. L. Rev. 349 (1989) ("Large numbers of minority law professors are overworked, excluded from informal information networks and describe their work environment as hostile, unsupportive, or openly or subtly racist. Many face increasing challenges to their legitimacy in the classroom."); Paul M. George & Susan McGlamery, Women and Legal Scholarship: A Bibliography, 77 Iowa L. Rev. 87 (1991) (providing a lengthy bibliography of sources about women in the legal profession and legal academia as well as feminist theory more broadly); Deborah Jones Merritt, Are Women Stuck on the Academic Ladder? An Empirical Perspective, 10 UCLA Women's L.J. 249 (2000) (comparing data of male and female law professors over time to showcase how female candidates fare at each step of the law school tenure track); Judith Resnik, A Continuous Body: Ongoing Conversations About Women and Legal Education, 53 J. Legal Educ. 564 (2003) ("The legal academy has to address how assumptions about gender, race, and ethnicity shape the law and, in turn, about what role law plays, has played, and should play in making those concepts meaningful.").

135. See Delgado & Villalpando, supra note 132, at 169 (quoting Teresa Córdova, Power and Knowledge: Colonialism in the Academy, *in* Living Chicana Theory 16, 18 (Carla Trujillo ed., 1998)) (discussing the biases that have traditionally influenced the perceived legitimacy of faculty of color).

136. See Citron & Solove, Privacy Harms, supra note 79, at 830–61 ("Our typology groups privacy harms into seven basic types: (1) physical harms; (2) economic harms; (3)

recognition is enough for a given information-based harm to be considered a privacy harm? As these examples demonstrate, the criteria are still unclear.

1. *Social Recognition of Bias and Unfairness.* — Privacy scholarship is not the only place where bias and unfairness have been socially recognized. In 1996, for instance, computer scientist Batya Friedman and philosopher Helen Nissenbaum—today a prominent privacy scholar—published the article *Bias in Computer Systems*.[137] Friedman and Nissenbaum's groundbreaking paper examines what bias in computer systems could look like.[138] According to the authors, bias in computer systems can arise from "social institutions, practices, and attitudes" ("preexisting bias"); "technical constraints or considerations" ("technical bias"); or the same "context of use" ("emergent bias").[139] In all these cases, "biased computer systems are instruments of injustice."[140]

Decades later, information and social scientists also began to raise awareness of automated decisionmaking systems' disparate impact on vulnerable populations, proposing critiques of algorithms as political artifacts.[141] In 2017, political scientist Virginia Eubanks was among the first scholars to pick up the bias discussion.[142] Using three case studies of public-assistance sorting and monitoring systems in Indiana, Los Angeles, and Pittsburgh, Eubanks exposed how these "[t]echnologies of poverty management are not neutral."[143] In particular, these case studies revealed the disparate impact of predictive algorithms, risk models, and automated

---

reputational harms; (4) psychological harms; (5) autonomy harms; (6) discrimination harms; and (7) relationship harms.").

137. Batya Friedman & Helen Nissenbaum, Bias in Computer Systems, 14 Ass'n for Computing Mach. Transactions on Info. Sys. 330 (1996).

138. See id. at 330–32 (providing an example of computer systems' bias and introducing the authors' framework for understanding it). For other, more superficial, approaches to bias, see generally Deborah G. Johnson & John M. Mulvey, Computer Decisions: Ethical Issues of Responsibility and Bias (Stat. & Operations Rsch. Ser. Technical Report SOR-93-11, 1993) (highlighting implicit biases as one of three ethical issues in computer systems that may lead to their abuse); James H. Moor, What Is Computer Ethics?, 16 Metaphil. 266 (1985) (noting the problem of the "invisibility factor" in computer systems, which facilitates intentional invisible abuse, the importation of programming values and biases that may not be apparent to users, and invisible miscalculations that may be too complex to verify completely).

139. Friedman & Nissenbaum, supra note 137, at 332.

140. Id. at 345.

141. See Langdon Winner, Do Artifacts Have Politics?, Dædalus 121, Winter 1980, at 121, 121 (noting the "provocative" argument that technology "can embody specific forms of power and authority").

142. See Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor 11 (2017) (describing how automated eligibility systems target poor and working-class people, collecting personal information and labeling them as "risky investments" while simultaneously discouraging them from accessing resources to survive in the changing socioeconomic reality).

143. Id. at 9.

eligibility systems on poor and working-class people.[144] That same year, law professor Andrew G. Ferguson published an account analyzing the use of big data technologies and predictive analytics for policing, similarly uncovering their discriminatory effects against people of color, immigrants, religious minorities, people experiencing poverty, protesters, and government critics.[145]

Internet studies scholar Professor Safiya Umoja Noble's important work sheds light on the data discrimination generated by internet search engines.[146] Besides showing how algorithms privilege whiteness and discriminate against people of color, particularly women of color, Noble also showed how search engines reproduce a vicious cycle of "technological redlining."[147] Society's racist perceptions of Black women and girls are embedded in computer code and artificial intelligence technologies, which then influence societal perceptions.[148]

Researcher Mounika Neerukonda and information, technology, and society scholar Professor Bidisha Chaudhuri, among others, highlighted the dangers of considering technologies (gender) neutral.[149] Algorithms governing artificial intelligence systems often reproduce or reiterate human biases, including gender biases.[150] These biases, Neerukonda and Chaudhuri argued, can result either from the data used to feed and train the algorithms or from the highly male-dominated technology industry responsible for developing them.[151]

Could this acknowledgement of bias in the computer and social sciences be considered *significant* in terms of social recognition of discrimination? Interestingly, in the social sciences literature reviewed here,

---

144. Id. at 11.

145. See Ferguson, supra note 97, at 3–5 (2017) (explaining that "black data," a term the author uses to denote hidden, racially coded data collected by police on communities of color, affects all marginalized communities by collecting, selling, and surveilling detailed personal data, which can contain inaccurate information for police to act upon).

146. Safiya Umoja Noble, Algorithms of Oppression: How Search Engines Reinforce Racism 5 (2018) (explaining how algorithmically designed searches readily suggest racist and sexist results and reflect "a corporate logic of either willful neglect or a profit imperative that makes money from racism and sexism").

147. See id. at 1.

148. Id. at 9–10 (arguing that algorithmic oppression, often in the form of racism and sexism, is part of the web's fundamental design and that the missing social and human context in these algorithmic decisions results in "erroneous, stereotypical, or even pornographic" portrayals of marginalized people that "reinforce oppressive social and economic relations").

149. See Mounika Neerukonda & Bidisha Chaudhuri, Are Technologies (Gender)-Neutral?: Politics and Policies of Digital Technologies, 47 Admin. Staff Coll. India J. Mgmt. 32, 39–41 (2018) (arguing that technology is designed with gender biases and thus reflects these biases in the production of knowledge and practices of power associated with technology).

150. Id. at 32.

151. See id.

worries about information-based discrimination are generally framed in terms of justice and fairness rather than privacy.[152] Why did privacy scholars decide to start talking about this harm as involving privacy? What "social recognition" counts for these matters? When is it sufficiently consolidated to be considered social? These are the types of questions Solove's pragmatic approach does not help us resolve. Confronting them would open the door to facing and questioning hidden power imbalances reinforced and perpetuated through academic research.

2. *Social Recognition of Data-Driven Manipulation.* — Today, many scholars understand digital manipulation as a privacy problem or as a danger against which privacy can protect—so much so that it made its way into Solove and Citron's 2022 typology of privacy harms.[153] But, as with discrimination, discussions about this harm already existed in the privacy literature long before it was formally included in the typology. In the early 1970s, Professor Arthur Miller predicted that computers, data banks, and dossiers could eventually blur the distinction between deploying cybernetics to understand a person and using it to control them.[154] "[I]t does not require a vivid imagination," Miller noted, "to conjure up a number of simulation activities involving the prediction of an individual's or a group's behavior that may lead to attempts at human manipulation."[155] Similarly, in 1980, Gavison suggested that unequal distribution of privacy could lead to manipulation.[156] In 2003, then–J.S.D candidate Tal Zarsky "describe[d] the current privacy debate, highlighting the issues most relevant to the new reality data mining creates,"[157] including manipulation[158] (and discrimination) among them. A year later, he would label those issues as "privacy-based concerns," which he defined as "those stemming from fears of the actual detrimental uses of personal data collected by commercial entities."[159]

---

152. See, e.g., Noble, supra note 146, at 31 ("I am building on the work of previous scholars of commercial search engines such as Google but am asking new questions that are informed by a Black feminist lens concerned with *social justice* for people who are systemically oppressed." (emphasis added)); Cathy O'Neil, Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy 13 (2016) ("This book will focus sharply in the other direction, on the damage inflicted by [opaque mathematical models] and the *injustice* they perpetuate." (emphasis added)).

153. Citron & Solove, Privacy Harms, supra note 79, at 831 fig.1.

154. See Miller, supra note 36, at 42–43 (explaining that widespread computer use not only enables corporations to map patterns of consumer behavior but also allows firms to determine people's desires and decisions by "making palatable what industry or government already has decided to offer the public").

155. Id.

156. Gavison, Privacy and the Limits of Law, supra note 12, at 444.

157. Zarsky, Mine Your Own Business, supra note 92, at 2.

158. Zarsky referred to such manipulations as "the autonomy trap," as they hinder individual and societal autonomy. Id. at 35–36.

159. See Tal Z. Zarsky, Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet

In 2014, Calo explored manipulation in the context of behavioral economics.[160] Looking to update the concept of market manipulation[161] for a technology-mediated marketplace, Calo unpacked why and when leveraging data against the consumer becomes a problem worthy of consumer protection law intervention.[162] Digital market manipulation "has the potential to generate economic and privacy harms and to damage consumer autonomy in a very specific way."[163] In light of these harms, Professor Ryan Calo argued that law should look for ways to realign the incentives of consumers and firms.[164] In 2019, privacy scholars Daniel Susser, Beate Roessler, and Helen Nissenbaum dove deep into what exactly it means to manipulate someone as well as the harms that manipulation inflicts on people and social institutions.[165] Like Calo, the authors considered whether the new forms of manipulative practice made possible by information technology should be cause for serious worry, since "[s]ubverting another person's decision-making power undermines his or her autonomy."[166] Manipulation has also been a topic of exploration for constitutional and administrative law scholar Cass Sunstein since at least 2014.[167]

At what point did algorithmic manipulation become a privacy harm? Apparently, Miller and Zarsky's early acknowledgments of the harm were not enough to merit recognition in Solove's 2006 taxonomy of privacy

---

Society, 58 U. Miami L. Rev. 991, 1005 (2004). Interestingly, Zarsky has more recently come to question whether manipulation-based concerns justify the risks of expanding information privacy law. See Zarsky, Privacy and Manipulation, supra note 31, at 168 ("[W]hat will stop information privacy laws, doctrines and concepts from mushrooming uncontrollably?").

160. See Calo, Digital Market Manipulation, supra note 100, at 999 ("The interplay between rational choice and consumer bias that is at the heart of behavioral economics helps illustrate how information and design advantages might translate into systematic consumer vulnerability.").

161. This term was initially coined in 1999 by Professors Jon Hanson and Douglas Kysar. See Jon D. Hanson & Douglas A. Kysar, Taking Behavioralism Seriously: Some Evidence of Market Manipulation, 112 Harv. L. Rev. 1420, 1424–25 (1999) ("[B]ecause individuals exhibit systematic and persistent cognitive processes that depart from axioms of rationality, they are susceptible to manipulation by . . . actors in a position to influence the decisionmaking context. Moreover, the actors in the dominant position *must* capitalize on this manipulation or eventually be displaced from the market.").

162. Calo, Digital Market Manipulation, supra note 100, at 999.

163. Id. at 1025.

164. Id. at 1044.

165. Daniel Susser, Beate Roessler & Helen Nissenbaum, Online Manipulation: Hidden Influences in a Digital World, 4 Geo. L. Tech. Rev. 1, 2 (2019).

166. Id. at 4.

167. See, e.g., Sunstein, supra note 101, at 216–17 ("The principal goal of this article is to make progress in understanding what manipulation is and what is wrong with it. If we can make progress on those tasks, we should be better equipped to assess a wide range of problems in ethics, policy, and law.").

harms.[168] Did later discussion about manipulation amount to enough social recognition, even when scholars' main emphasis was not on privacy but rather on autonomy concerns? Was it enough for authors to be invited to FTC workshops on the topic,[169] to present at the right conferences,[170] or to speak to the popular press?[171] A taxonomic approach grounded exclusively in social recognition furnishes no criteria by which to answer these important questions.

3. *Information-Based Harms Still Outside the Periphery of Privacy Law.* — Like information-based discrimination and algorithmic manipulation, many other data-driven practices, such as procedural injustices or fragmentation of the public sphere, also rely on personal information about individuals. But they have not yet achieved enough social recognition to register as privacy harms.

Take the case of procedural injustice. As early as 1993, Professor Paul Schwartz set off alarm bells on the government's use of data processing to distribute welfare and its possible implications for bureaucratic justice.[172] Years later, Professor Daniel Steinbock followed suit, looking to identify "the due process effects of using data matching and mining to identify persons against whom official action is taken."[173] In 2008, Citron published her germinal article *Technological Due Process*, in which she raised awareness of the threats that automated decisionmaking poses to the last century's procedural protections, particularly for the fairness, accountability, transparency, and participation values that these protections are meant to ensure.[174] And building on Citron's article, Crawford and Schultz, along

168. See Solove, Taxonomy of Privacy, supra note 14, at 489–91 (describing privacy harms encompassed by Solove's taxonomy and omitting algorithmic manipulation).

169. See, e.g., Exploring Privacy: A Roundtable Series, FTC, https://www.ftc.gov/news-events/events/2010/03/exploring-privacy-roundtable-series [https://perma.cc/3GD4-YHXY] (last visited Oct. 22, 2023) (featuring Allen and others); The Internet of Things—Privacy and Security in a Connected World, FTC, https://www.ftc.gov/news-events/events/2013/11/internet-things-privacy-security-connected-world [https://perma.cc/GJ34-XEPQ] (last visited Oct. 22, 2023) (featuring Calo and others).

170. See, e.g., Privacy Law Scholars Conference, https://privacyscholars.org/ [https://perma.cc/Q2VC-GB5Y] (last visited Feb. 6, 2024).

171. See, e.g., Joanna Kavenna, Shoshana Zuboff: 'Surveillance Capitalism Is an Assault on Human Autonomy', The Guardian (Oct. 4, 2019), https://www.theguardian.com/books/2019/oct/04/shoshana-zuboff-surveillance-capitalism-assault-human-automomy-digital-privacy [https://perma.cc/3YDX-86FN] (interviewing Zuboff about the dangers of widespread data collection by large technology companies).

172. See Schwartz, Data Processing, supra note 31, at 1348–49. Schwartz defines bureaucratic justice as "administrative decisionmaking that pays appropriate attention to accuracy, cost-effectiveness, and the dignity of the participants." Id. at 1349.

173. Steinbock, supra note 95, at 7.

174. Citron, Technological Due Process, supra note 95, at 1258. Citron further developed this idea in subsequent coauthored articles. See, e.g., Calo & Citron, supra note 95, at 820 ("[A]utomation has led to the adoption of inexpert tools that waste government resources and deny individuals any meaningful form of due process."); Citron & Pasquale, supra

with many others, proposed a right to procedural data due process to mitigate predictive privacy harms.[175]

Some of these authors—like Crawford and Schultz—have addressed the threats to due process as a privacy problem.[176] Others have completely omitted privacy in their discussion of technological due process, talking instead about fairness and justice.[177] Indeed, Schwartz's early work explicitly states that privacy is not an ideal normative concept to frame these threats, since "[p]rivacy does not help once the issue becomes not *whether*, but *how* personal data should be collected and processed."[178]

Another example is nondiscriminatory social inequality. In her recent article *A Relational Theory of Data Governance*, Professor Salomé Viljoen maintains that data production facilitates social inequality.[179] In particular, the relational nature of data collection and use—and the population-based relations and data flows they give rise to—can have harmful and subordinating consequences for less-socially-advantaged groups.[180] Many other scholars have supported this view and have highlighted the oppressive effects that data processing can have at both the individual and societal levels.[181]

Certain scholars discuss this harm within the periphery of privacy law, calling for "the third way"[182] or "a 'third wave' for Privacy Law"[183] to

---

note 92, at 19 ("If law and due process are absent from this field, we are essentially paving the way to a new feudal order of unaccountable reputational intermediaries.").

175. See Crawford & Schultz, supra note 95, at 109 ("[P]rocedural data due process would regulate the fairness of Big Data's analytical processes with regard to how they use personal data (or metadata derived from or associated with personal data) in any adjudicative process . . . .").

176. See id. at 96 ("Alongside its great promise, Big Data presents serious privacy problems.").

177. See, e.g., Citron, Technological Due Process, supra note 95, at 1253–54 (discussing automation's erosion of individual due process rights, including notice and the opportunity to be heard).

178. Schwartz, Data Processing, supra note 31, at 1347.

179. See Viljoen, supra note 31, at 581.

180. See id. at 616.

181. See, e.g., Woodrow Hartzog & Neil Richards, Privacy's Constitutional Moment and the Limits of Data Protection, 61 B.C. L. Rev. 1687, 1695 (2020) (criticizing data protection regimes that assume that fair data processing is "eternally virtuous" and ignore the damage being done by large-scale data processing); Daniel J. Solove, The Limitations of Privacy Rights, 98 Notre Dame L. Rev. 975, 989 (2023) [hereinafter Solove, Limitations of Privacy Rights] ("[P]rivacy issues extend beyond threats to individual privacy. There 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."); Ari Ezra Waldman, The New Privacy Law, 55 U.C. Davis L. Rev. Online 19, 39 (2021), https://lawreview.law.ucdavis.edu/sites/g/files/dgvnsk15026/files/media/documents/55-online-Waldman.pdf [https://perma.cc/2GXE-PTGM] (observing that "[t]echnology companies conscript us in the commodification and subordination of others").

182. Hartzog & Richards, supra note 181, at 1694 (internal quotation marks omitted).

183. Waldman, supra note 181, at 40–41.

address it. Viljoen, on the other hand, invites us to look outside the predominant legal regimes that govern data collection and use—contract and privacy law—for "collective institutional forms of [democratic] ordering."[184] In fact, instead of referring to privacy harms, she strategically frames these issues as individual and social informational harms.[185]

A final example of an information-based harm that still falls outside the scope of privacy is the fragmentation of the public sphere. Scholars have long called attention to how content personalization decreases our exposure to differing perspectives.[186] Often referred to as the "filter bubble," this information-based harm threatens to control how society consumes and shares information, narrowing people's worldviews and ultimately interfering with the realization of our democracy.[187] While some theorists have addressed social fragmentation within the context of privacy discourse,[188] others, like Professors Cynthia Dwork and Deirdre Mulligan,

---

184. See Viljoen, supra note 31, at 584, 586.

185. See id. at 586.

186. See, e.g., Eli Pariser, The Filter Bubble: What the Internet Is Hiding From You 6–10 (2011) (revealing how the computer monitor is becoming a one-way mirror); Christoph Bezemek, Filter Bubble and Fundamental Rights, *in* Fundamental Rights Protection Online: The Future Regulation of Intermediaries 16, 24–26 (Bilyana Petkova & Tuomas Ojanen eds., 2020) (exploring the filter bubble phenomenon through a fundamental rights perspective); Engin Bozdag & Jeroen van den Hoven, Breaking the Filter Bubble: Democracy and Design, 17 Ethics & Info. Tech. 249, 254–63 (2015) (analyzing the design of different software tools that try to break filter bubbles against the backdrop of different theories of democracy); Dwork & Mulligan, supra note 31, at 37 (exploring legal concerns around "the social fragmentation of 'filter bubbles' that create feedback loops reaffirming and narrowing individuals' worldviews" (footnote omitted)); Lucas D. Introna & Helen Nissenbaum, Shaping the Web: Why the Politics of Search Engines Matters, 16 Info. Soc'y 169, 182 (2000) (noting that segmentation of search engines may "fragment the very inclusiveness and universality of the Web that we value" and lead to the internet "merely mirror[ing] the institutions of society with its baggage of asymmetrical power structures, privilege, and so forth"); Janice Richardson, Normann Witzleb & Moira Paterson, Political Micro-Targeting in an Era of Big Data Analytics, in Big Data, Political Campaigning and the Law: Democracy and Privacy in the Age of Micro-Targeting 1, 4 (Normann Witzleb, Moira Paterson & Janice Richardson eds., 2020) (investigating whether the use of internet data and political microtargeting "exacerbate[s] the issue of 'filter bubbles'" and thus "undermine[s] some of the inherently collective processes underpinning democratic governance"); Markus Zanker, Laurens Rook & Dietmar Jannach, Measuring the Impact of Online Personalisation: Past, Present and Future, 131 Int'l J. Hum.-Comput. Stud. 160, 161–66 (2019) (summarizing multidisciplinary research on the impact of personalization and recommendation systems); Frederik J. Zuiderveen Borgesius, Damian Trilling, Judith Möller, Balázs Bodó, Claes H. de Vreese & Natali Helberger, Should We Worry About Filter Bubbles?, Internet Pol'y Rev., Mar. 31, 2016, at 1, 3–6 (summarizing empirical research on the effects of personalization).

187. See Bozdag & van den Hoven, supra note 186, at 249 ("As a consequence [of filter bubbles], the epistemic quality of information and diversity of perspectives will suffer and the civic discourse will be eroded.").

188. See, e.g., Bezemek, supra note 186, at 24 ("It may seem self-explanatory that from a fundamental rights perspective—as a practical matter—[filter bubbles] not only affect[] freedom of speech, but also tend[] to pose a problem for the individual's pursuit of self-fulfillment inherent to the right to privacy.").

explicitly deny that the issue is a privacy problem.[189] "While targeting, narrowcasting, and segmentation of media and advertising, including political advertising, are fueled by personal data, they don't depend on it," Dwork and Mulligan claim in an essay titled *It's Not Privacy, and It's Not Fair*.[190]

Procedural injustice, social inequality, and the fragmentation of the public sphere still have not found their way under the umbrella.[191] What keeps these information-based harms and others from being adopted into the privacy family? Should we not—as Schwartz attempted to do decades ago[192]—talk through what makes privacy an unsuitable paradigm to address these harms? Or examine what makes them different from information-based discrimination or algorithmic manipulation harms, which also stem from the use of personal data for decisionmaking?

4. *Privacy Over-Inclusion and Value Dilution.* — How a problem is conceptualized has profound implications on the legal approaches we choose to prevent and address it. A certain conceptualization can determine whether we should recur to information privacy law to regulate and address it.

Likewise, harm conceptualization has significant effects on the conditions under which the claimants of a given harm are heard in court and receive relief.[193] Unlike other harms, when it comes to privacy harms, "courts and some scholars require a showing of harm . . . out of proportion with other areas of law."[194] As Solove and Citron have aptly explained,

> Through harm requirements, courts have made the enforcement of privacy laws difficult and, at times, impossible. They have added requirements for harm via standing. They have required

189. See Dwork & Mulligan, supra note 31, at 36–37 (arguing that privacy measures "fail to address concerns with the classifications and segmentation produced by big data analysis" and that the effects of those classifications—"decreased exposure to differing perspectives, reduced individual autonomy, and loss of serendipity"—are in any case "not privacy problems").

190. Id. at 37.

191. This is especially remarkable in the case of procedural injustice, considering Citron's forerunner position among what others would later call the "technological due process scholars." See supra note 174 and accompanying text; Jay Thornton, Note, Cost, Accuracy, and Subjective Fairness in Legal Information Technology: A Response to Technological Due Process Critics, 91 N.Y.U. L. Rev. 1821, 1833–34 (2016) (noting that scholars of technological due process phrase their two main critiques of automated decision systems in terms of accuracy and justice, not privacy).

192. See supra note 178 and accompanying text.

193. As Professors Ignacio Cofone and Adriana Robertson point out, "a clear conception of [privacy] harms is essential for determining both standing and remedies." Ignacio N. Cofone & Adriana Z. Robertson, Privacy Harms, 69 Hastings L.J. 1039, 1041 (2018).

194. Ryan Calo, Privacy Harm Exceptionalism, 12 Colo. Tech. L.J. 361, 361 (2014) ("[H]arm presents an especially acute challenge in the context of privacy. Courts generally demand that privacy plaintiffs show not just harm, but concrete, fundamental, or 'special' harm before they can recover." (quoting Doe I v. Individuals, 561 F. Supp. 2d 249, 257 (D. Conn. 2008))).

> harm for statutes that do not require such a showing. They have mandated proof of harm even for statutes that include statutory damages, undercutting the purpose of these provisions. They have adopted narrow conceptions of cognizable harm to exclude many types of harm, including emotional injury and dashed expectations.[195]

An overinclusive theory of privacy also opens the door to a skeptical court devaluing a harm by painting it with the privacy brush and obscuring the true value at stake.[196] In prior work, one of us critiqued the taxonomic approach on this basis.[197] Thus, for example, cases concerning the right to contraception or abortion may be on firmer legal footing when premised on liberty and equality than on privacy.[198] And indeed, the *Dobbs* majority referred to privacy's absence from the Constitution in deconstitutionalizing a pregnant person's right to choose.[199]

At a broader level, the ability to distinguish privacy is important for privacy law as a field. Clearly identifying what—besides social recognition—makes a harm relevant to privacy would allow us to better determine what type of privacy law we need and should aim for.[200] It would give scholars the opportunity to confront fears concerning the abuse of the concept

---

195. Citron & Solove, Privacy Harms, supra note 79, at 800 (footnotes omitted). Other scholars have also observed courts' reluctance to address and remedy privacy harms. See, e.g., Lauren Henry Scholz, Privacy Remedies, 94 Ind. L.J. 653, 654 (2019) ("Courts struggle to determine when privacy infringements that occur in cyberspace are sufficiently 'concrete' to allow standing in federal courts."); Daniel J. Solove & Danielle Keats Citron, Risk and Anxiety: A Theory of Data-Breach Harms, 96 Tex. L. Rev. 737, 739 (2018) (noting that suits seeking redress for data breaches have often turned on issues of harm instead of whether defendants are at fault for failing to protect plaintiffs' data).

196. See Calo, Boundaries of Privacy Harm, supra note 20, at 1137–38 ("If too many problems come to be included under the rubric of privacy harm—everything from contraception to nuisance—we risk losing sight of what is important and uniquely worrisome about the loss of privacy.").

197. See id. at 1141–42 ("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.").

198. See id. at 1134 (noting that "ruling out privacy harm may force courts and theorists to confront other basic values such as autonomy or equality" because privacy may "obviate[] the perceived need to grapple with other crucial, yet perhaps more politically contestable, values" in cases involving contraception, abortion, and antisodomy laws).

199. See Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228, 2245 (2022) ("*Roe*, however, was remarkably loose in its treatment of the constitutional text. It held that the abortion right, which is not mentioned in the Constitution, is part of a right to privacy, *which is also not mentioned*." (emphasis added)).

200. According to Charles Fried, "legal [privacy] norms are more or less incomprehensible without some understanding of what kind of a situation is sought to be established with their aid. Without this understanding we cannot sense the changing law they demand in changing circumstances." Fried, supra note 11, at 493; see also María P. Angel, Are Individual Privacy Rights the Appropriate Approach?, Wash. J.L. Tech. & Arts Blog (Apr. 20, 2022), https://wjlta.com/2022/04/20/are-individual-privacy-rights-the-appropriate-approach/

of privacy. As one of us has argued, overuse of the term "risks its diffusion into a meaningless catchall."[201] Similarly, Zarsky has questioned whether the "expansive dynamic [of privacy] might lead information privacy law to eventually merge with other fields of law such as consumer protection or broader notions of protecting individual autonomy—or perhaps collapse into these broader and more established fields of law."[202] Privacy's current unarticulated expansion deserves a thorough discussion within the field. Otherwise—as Professor Morgan Weiland warned regarding the expansion of First Amendment speech doctrine—"we risk diluting it not only through its broad application but also by undermining its internal coherence."[203]

### B. *Unresolved Tensions*

Agnosticism toward the nature of privacy has allowed privacy scholars and others to include many values under the large and expanding um brella of privacy. Personal autonomy, self-expression, equality, antisubordination, and fairness have come to be recognized, to greater or lesser extents, as furthered or protected by privacy in the information context. Unfortunately, this approach seems to disregard—and even obscure—longstanding and emerging tensions *within* this capacious conception of privacy and *among* privacy problems, or what Pozen has coined as "privacy–privacy tradeoffs."[204] Further, it gives courts, lawmakers, and scholars no framework for interrogating or resolving those tensions.

"The more sorts of privacy claims that there are," writes Pozen, "the greater the risk that there will be conflicts among them."[205] This Essay expands on Pozen's work to make the case that holding a giant umbrella over myriad, sometimes-conflicting values exacerbates the dilemma of privacy–privacy tradeoffs while giving no clues about how to unpack or reconcile internal tensions between family members.

The following sections address three tensions that are obscured and remain unresolved under the large umbrella of privacy problems: (1) privacy versus equality, (2) privacy versus algorithmic accountability, and (3) privacy versus freedom of expression.

---

[https://perma.cc/37XS-Z96H] (noting that current proposed data privacy laws overlook the "social/relational dimensions" of privacy).

201. Calo, Boundaries of Privacy Harm, supra note 20, at 1137.

202. Zarsky, Privacy and Manipulation, supra note 31, at 168.

203. Morgan N. Weiland, Expanding the Periphery and Threatening the Core: The Ascendant Libertarian Speech Tradition, 69 Stan. L. Rev. 1389, 1400 (2017).

204. According to Pozen, privacy–privacy tradeoffs arise when "enhancing or preserving privacy along a certain axis . . . entail[s] compromising privacy along another axis." Pozen, supra note 20, at 222.

205. Id. at 227.

1. *Historical Tensions Between Privacy and Equality.* — Privacy has never been thought of as an unambiguously positive societal force. Economic theorists bemoan privacy's capacity to withdraw information from the marketplace and cause inefficiency.[206] Other scholars offer critiques of privacy grounded in equity and inclusion. Feminist and queer legal studies have long called attention to the capacity of privacy (or claims of privacy) to harm and impair equality.[207] For years, these scholars have understood privacy as a convenient cover for violence and subjugation—for example, shielding domestic abusers from the state and justifying regressive bathroom segregation.[208]

Since the Supreme Court recognized a privacy-based right of reproductive freedom,[209] feminist theorists such as Justice Ruth Bader Ginsburg and Professors Sylvia Law and Catharine MacKinnon have contended that constitutional privacy can operate to obscure what they have argued is the core interest at the heart of contraception and abortion debates[210]—namely, a woman's "ability to stand in relation to man, society, and the state as an independent, self-sustaining, equal citizen."[211] These scholars argue that considering these issues under privacy doctrine "blunts our ability to focus on the fact that it is *women* who are oppressed when abortion is denied."[212] By focusing on a presumably universal value such

206. See, e.g., Richard A. Posner, The Economics of Privacy, 71 Am. Econ. Rev. 405, 406 (1981) ("[C]oncealment of personal information is a form of fraud."); Posner, Privacy, Secrecy, and Reputation, supra note 52, at 8 ("As a detail, it may be noted that if there is a taste for solitude as an end in itself it is a *selfish* emotion in a precise economic sense that can be assigned to the concept of selfishness. Solitary activity (or cessation of activity) benefits only the actor."); Richard A. Posner, The Right of Privacy, 12 Ga. L. Rev. 393, 403 (1978) ("[T]here is a prima facie case for assigning the property right away from the individual where secrecy would reduce the social product by misleading the people with whom he deals."). But see Acquisti et al., supra note 125, at 478–85 (arguing that advancements in information technology raise increasingly nuanced and complex issues to the economic analysis of privacy); Ryan Calo, Privacy and Markets: A Love Story, 91 Notre Dame L. Rev. 649, 665–90 (2016) (arguing that privacy and markets should be considered as sympathetic and interdependent).

207. See infra notes 209–229 and accompanying text.

208. See infra notes 209–229 and accompanying text.

209. See Griswold v. Connecticut, 381 U.S. 479, 486 (1965) (holding that a Connecticut statute forbidding use of contraceptives violated "the notions of privacy surrounding the marriage relationship").

210. In 2022, in *Dobbs v. Jackson Women's Health Organization*, the Court overruled Roe v. Wade, 410 U.S. 113 (1973), and Planned Parenthood of Southeastern Pennsylvania v. Casey, 505 U.S. 833 (1992), holding instead that the Constitution does not confer the right to obtain an abortion. 142 S. Ct. 2228, 2242–43 (2022); see Isabelle G. Horn, Student Case Note, *Dobbs v. Jackson Women's Health Organization* 142 S. Ct. 2228 (2022), 49 Ohio N.U. L. Rev. 231, 245 (2022) ("[T]he majority holding in *Dobbs* . . . poses a significant threat to other rights rooted in the Fourteenth Amendment's Due Process Clause.").

211. Ruth Bader Ginsburg, Some Thoughts on Autonomy and Equality in Relation to *Roe v. Wade*, 63 N.C. L. Rev. 375, 383 (1985) (citing Kenneth Karst, The Supreme Court, 1976 Term—Foreword: Equal Citizenship Under the Fourteenth Amendment, 91 Harv. L. Rev. 1, 57–59 (1977)).

212. Sylvia A. Law, Rethinking Sex and the Constitution, 132 U. Pa. L. Rev. 955, 1020 (1984).

as privacy, reproductive rights doctrine overlooks the specific role of gender—including all the nuanced ways that this oppression intersects with people who can become pregnant who do not identify as women.

Situating the choices to pursue an abortion or use contraception under privacy law "reinforces a public/private [dichotomy] that is at the heart of the structures that perpetuate the powerlessness" of individuals who can become pregnant.[213] Thus, by conceiving privacy as a right against public intervention in the private sphere, these decisions situate pregnant individuals within a realm that is inaccessible to the state, hermetic, and unaccountable. Yet reproductive "equality will require intervention, not abdication, to be meaningful."[214] Otherwise, MacKinnon forcefully claims, "[T]he legal concept of privacy can and has shielded the place of battery, marital rape, and women's exploited labor."[215] For this reason, and despite some later pro-privacy views based on a more affirmative concept of privacy linked to autonomy enhancement,[216] feminist theorists have continuously tried to shed light on "the dark and violent side of privacy."[217]

---

213. See id.

214. See MacKinnon, Privacy v. Equality, supra note 24, at 100; see also Catharine A. MacKinnon, Toward a Feminist Theory of the State 191 (1989) ("The right to privacy looks like . . . a sword in men's hands presented as a shield in women's. Freedom from public intervention coexists uneasily with any right that requires social preconditions to be meaningfully delivered."); Catharine A. MacKinnon, Reflections on Sex Equality Under Law, 100 Yale L.J. 1281, 1311 (1991) ("[W]hile the private has been a refuge for some, it has been a hellhole for others . . . . In gendered light, the law's privacy is a sphere of sanctified isolation, impunity, and unaccountability. . . . It belongs to the individual with power. Women have been accorded neither individuality nor power."); Catharine A. MacKinnon, The Road Not Taken: Sex Equality in *Lawrence v. Texas*, 65 Ohio St. L.J. 1081, 1090 (2004) ("Privacy works to protect systematic inequality, whether structurally in reinforcing the public/private line or in express doctrine in substantive due process liberty." (footnote omitted)).

215. MacKinnon, Privacy v. Equality, supra note 24, at 101.

216. See, e.g., Allen, Uneasy Access, supra note 12, at 36 ("[O]pportunities for privacy and the exercise of liberties that promote privacy have special importance for women. Privacy can strengthen traits associated with moral personhood, individuality, and self-determination. It can render a woman more fit for contributions both in her own family and in outside endeavors."); Ruth Gavison, Feminism and the Public/Private Distinction, 45 Stan. L. Rev. 1, 43 (1992) ("[F]ighting the verbal distinction between public and private, rather than fighting invalid arguments which invoke them, or the power structures which manipulate them in unjustifiable ways, is as futile as seeking individual therapy for problems of social structure."); Elizabeth M. Schneider, The Synergy of Equality and Privacy in Women's Rights, 2002 U. Chi. Legal F. 137, 138 ("[C]oncepts of equality are necessary for a robust understanding of privacy, and concepts of privacy are necessary for the full realization of equality."); Laura W. Stein, Living With the Risk of Backfire: A Response to the Feminist Critiques of Privacy and Equality, 77 Minn. L. Rev. 1153, 1155 (1993) ("[T]o avoid even greater dangers, feminists must try to transform these doctrines. There is no reason why feminists must choose between privacy and equality or between equality and some other way of claiming entitlements. Instead, feminists can and should use the whole range of legal arguments available.").

217. Schneider, Violence of Privacy, supra note 24, at 974.

Feminist theorists have also surfaced privacy's prejudicial effects on equality outside reproductive matters. For instance, in the labor market sphere, Professor Lucinda Finley has argued that the apparent dichotomy between the "public" world of work and the "private" world of family and home "has fostered the economic and social subordination of women," ultimately contributing to their discriminatory treatment in the workplace.[218] Similarly, in the case of mothers who are poor, single, or both, Professor Martha Albertson Fineman has maintained that a "continued emphasis on privacy as the concept to constitutionally protect certain sorts of intimate behavior will serve to deter the development of other legal principles that might help to limit state regulation of poor and single mother families."[219]

Various scholars have also highlighted the gendered character of privacy to showcase how it can be used as a tool of female oppression, objectification, and subordination.[220] Theorists have repeatedly stressed how both the tort of privacy's reliance on outdated expectations about women's modesty and seclusion, as well as "[t]he Fourth Amendment's overarching standard of reasonableness and its epistemological stance of objectivity,"[221] make evident the "unmistakable mark of an era of male hegemony."[222] Professor Jeannie Suk Gersen has suggested that the judicial and public policy debate over privacy is really about determining the type of woman we envision and "which feminist idea of the woman will shape constitutional doctrine."[223]

Queer critical legal studies have also addressed the multiple ways in which privacy can impair gender equality. Scholars such as Professors

---

218. Finley, supra note 24, at 1119.

219. Martha Albertson Fineman, Intimacy Outside of the Natural Family: The Limits of Privacy, 23 Conn. L. Rev. 955, 956 (1991).

220. See, e.g., Anita L. Allen & Erin Mack, How Privacy Got Its Gender, 10 N. Ill. U. L. Rev. 441, 441 (1991) ("The privacy tort was the brainchild of nineteenth-century men of privilege, and it shows."); I. Bennett Capers, Unsexing the Fourth Amendment, 48 U.C. Davis L. Rev. 855, 858 (2015) ("[T]raditional notions of sex and gender inform much of Fourth Amendment practice and jurisprudence."); Dana Raigrodski, Reasonableness and Objectivity: A Feminist Discourse of the Fourth Amendment, 17 Tex. J. Women & L. 153, 156 (2008) ("[T]his article seeks to flesh out the invisible biases that underlie the facially objective and neutral legal standards of search and seizure law."); Victoria Schwartz, Leveling Up to a Reasonable Woman's Expectation of Privacy, 93 U. Colo. L. Rev. 115, 117 (2022) ("In the real world, however, the role that gendered privacy norms should play in privacy law remains a valid question in need of an answer."); Jeannie Suk, Is Privacy a Woman?, 97 Geo. L.J. 485, 488 (2009) ("Privacy is figured as a woman, an object of the male gaze."); Kristen M.J. Thomasen, Beyond Airspace Safety: A Feminist Perspective on Drone Privacy Regulation, 16 Can. J.L. & Tech. 307, 308 (2016) ("[T]he ways in which the drone might enhance or undermine women's privacy in particular have not yet been the subject of significant academic analysis.").

221. Raigrodski, supra note 220, at 156.

222. See Allen & Mack, supra note 220, at 442.

223. Suk, supra note 220, at 506.

Shannon Gilreath, Kendall Thomas, Susan Hazeldean, and Kenji Yoshino have contended that the secrecy and invisibility privacy provides to LGBTQI+ people and communities is not always empowering.[224] Rather, the rhetoric of privacy obscures the real debates that should be held about, for example, LGBTQI+ individuals' right "to be free from state-legitimated violence at the hands of private and public actors" (also referred to as the right to "corporal integrity").[225]

Notably, the secrecy of "the closet" has actually allowed heterosexual people to make decisions that negatively affect the LGBTQI+ community under the cover of a state of ignorance about LGBTQI+ people's intimate lives.[226] In that sense, what was supposed to be a safeguard has turned out to be "an ideological anchor for the oppression of gays and lesbians."[227]

---

224. See Shannon Gilreath, The End of Straight Supremacy 76 (2011) ("Privacy is, of course, the perfect vehicle for dominance."); Susan Hazeldean, Privacy as Pretext, 104 Cornell L. Rev. 1719, 1741 (2019) ("When transgender people seek permission to use facilities that accord with their gender identity at their school or work, privacy concerns are often used to justify denying access."); Kendall Thomas, Beyond the Privacy Principle, 92 Colum. L. Rev. 1431, 1435 (1992) ("[T]he lack of close attention to the actual human beings whose bodies are touched by laws like that challenged in *Hardwick* deprives privacy analysis of an important and indispensable conceptual resource."); Kenji Yoshino, Assimilationist Bias in Equal Protection: The Visibility Presumption and the Case of "Don't Ask, Don't Tell", 108 Yale L.J. 485, 492 (1998) ("Whether a group's visibility (or invisibility) empowers or disempowers it in the political process is a deeply contextual inquiry. It is therefore impossible to generalize about the effects of visibility (or invisibility) across those contexts."); Cathy A. Harris, Note, Outing Privacy Litigation: Toward a Contextual Strategy for Lesbian and Gay Rights, 65 Geo. Wash. L. Rev. 248, 251 (1997) ("By focusing on the right of privacy, litigators . . . dilute the power of those assertions that strike at the heart of the legal obstacles facing gays and lesbians. Specifically, equal protection and freedom of expression claims more directly address the discrimination against lesbians and gays.").

Notably, some scholars, despite these arguments, maintain that privacy may provide temporary protection for LGBTQI+ people against discrimination and surveillance. See, e.g., Toby Beauchamp, Going Stealth: Transgender Politics and U.S. Surveillance Practices 22 (2018) (observing that increased visibility of transgender people may end up optimizing public agencies' ability to monitor them); Anita L. Allen, Privacy Torts: Unreliable Remedies for LGBT Plaintiffs, 98 Calif. L. Rev. 1711, 1762–64 (2010) (acknowledging that though privacy tort suits have had limited utility for LGBTQI+ plaintiffs, they still may have had a deterrent effect on attacks against the LGBTQI+ community and noting that privacy rights for the LGBT community will be necessary as long as homophobia is alive).

225. Thomas, supra note 224, at 1435 (internal quotation marks omitted) (discussing the limitations of privacy rhetoric as a conceptual resource for analyzing homophobic antisodomy laws, which are better understood "as a kind of 'body politics'").

226. See, e.g., Bowers v. Hardwick, 478 U.S. 186, 192 (1986), overruled by Lawrence v. Texas, 539 U.S. 558 (2003) (holding that a Georgia antisodomy law could not be invalidated by the Court, since the Constitution does not grant "a fundamental right to homosexuals to engage in acts of consensual sodomy"). In *Lawrence v. Texas*, the Court overturned its decision in *Bowers*, explaining that it had misapprehended the fundamental liberty interest at stake, which "touch[es] upon the most private human conduct, sexual behavior, and in the most private of places, the home." 539 U.S. at 567.

227. Thomas, supra note 224, at 1456.

As Yoshino has noted, this can be seen in the case of the military's "Don't Ask, Don't Tell" policy:

> [W]hile the invisibility of gays may free them from certain kinds of superficial judgment, it entraps them in others. . . . [T]he superficial judgments about gays that justify the [Don't Ask, Don't Tell] policy—that they destroy unit cohesion, that they trench on the privacy of heterosexual servicemembers, and that they create debilitating sexual tension—survive precisely because the coerced invisibility of gays prevents them from being challenged.[228]

Relatedly, cisgender men and women have sometimes weaponized their own right to privacy in order to curtail LGBTQI+ equality. Hazeldean, for example, has shown how the privacy of women and girls has been wrongly used as a pretext to attack antidiscrimination protections for LGBTQI+ people, such as allowing transgender individuals to enter facilities that correspond to their gender identity.[229]

In sum, there are myriad situations in which privacy does not always further equality or protect people against discrimination.[230] On the contrary, privacy can operate against marginalized populations by not only obscuring the real rights and values at stake but also reinforcing and even legitimizing oppressive and discriminatory practices. A taxonomic approach that simply embraces equality as part of the privacy family renders these types of tensions harder to recognize and resolve.

Though the privacy umbrella has helped move the field forward, it has also obfuscated from public awareness the internal tensions among the values privacy implicates without offering solutions.[231]

2. *Conflicts Between Privacy and Algorithmic Accountability.* — As with equality, privacy can also conflict with the values that algorithmic account-

---

228. Yoshino, supra note 224, at 545.

229. See Hazeldean, supra note 224, at 1722 ("A desire for privacy in the bathroom is legitimate, but policies that allow transgender people to use bathrooms that accord with their gender identity do not undermine privacy.").

230. See also Lior Jacob Strahilevitz, Privacy Versus Antidiscrimination, 75 U. Chi. L. Rev. 363, 378–80 (2008) (arguing that the protection of private information regarding criminal history status will rarely, if ever, be the most appropriate tool for reintegrating people with felony convictions into the workplace).

231. Analogously, in *Seeking Refuge Under the Umbrella: Inclusion, Exclusion, and Organizing Within the Category Transgender*, anthropologist Megan Davidson argued that, although the umbrella term "transgender" has been a useful tool for mobilizing activism, its use often elides "ideological differences, internal contestations, and deep ambiguities about inclusion, exclusion, and the processes of creating social change" among activists in public consciousness, without contributing to solving them. Megan Davidson, Seeking Refuge Under the Umbrella: Inclusion, Exclusion, and Organizing Within the Category *Transgender*, 4 Sexuality Rsch. & Soc. Pol'y: J. Nat'l Sexuality Res. Ctr. 60, 78 (2007). In a similar fashion, although the taxonomic approach to privacy has provided refuge to a myriad of values, its use also elides critical conflicts among them.

ability and technological due process pursue, such as explainability, transparency, and accuracy. The eventual integration of procedural justice into the privacy family could obscure and downplay those conflicts.

One need look no further than technology firms' strategic, recurrent invocations of privacy to forestall accountability. In 2021, for example, Meta[232] shut down the accounts of NYU researchers who were running the free, open-source browser extension Ad Observer to look into misinformation on the company's platform.[233] Meta invoked its consumers' privacy in preventing researchers' access to data—though it was voluntarily provided by users and being used only to evidence the extent of misinformation on Facebook. Such "privacywashing"[234] practices demonstrate that privacy does not always further the other values it is expected to.

A decade or more of scholarship on algorithmic accountability also provides plenty of examples of cases in which an effort to protect desirable values such as accountability, explainability, or transparency in the context of algorithms may work against privacy. For instance, Professors Roger Allan Ford and W. Nicholson Price II have examined the conflict that can exist between the twin goals of privacy and accountability when it comes to the use of big-data techniques for healthcare applications: "[I]ndependent researchers need access to this [health] information to verify black-box algorithms, ensuring they are accurate and unbiased, but risking further privacy losses."[235]

Professors Finale Doshi-Velez and Mason Kortz have highlighted a comparable tension between privacy and explainability. According to the authors, "[U]nlike human decision-makers, AI systems can delete information to optimize their data storage and protect privacy."[236] Yet if we want these systems to generate ex post human-like explanations, the authors explain, we will necessarily need them to automatically store information regarding their decisions.[237]

---

232. Previously known as Facebook.

233. Laura Edelson & Damon McCoy, Opinion, We Research Misinformation on Facebook. It Just Disabled Our Accounts., N.Y. Times (Aug. 10, 2021), https://www.nytimes.com/2021/08/10/opinion/facebook-misinformation.html (on file with the *Columbia Law Review*).

234. Rory Mir & Cory Doctorow, Facebook's Attack on Research Is Everyone's Problem, Elec. Frontier Found. (Aug. 12, 2021), https://www.eff.org/deeplinks/2021/08/facebooks-attack-research-everyones-problem [https://perma.cc/7AA3-UHSX] (arguing that Facebook's strategy of presenting its actions against NYU disinformation researchers as a defense of user privacy is "a dangerous practice that muddies the waters about where real privacy threats come from").

235. Ford & Price, supra note 25, at 42.

236. Doshi-Velez & Kortz, supra note 25, at 10.

237. See id. ("AI systems do not automatically store information about their decisions. . . . However, an AI system designed this way would not be able to generate *ex post* explanations the way a human can.").

A similar situation occurs in the case of transparency. Claims to open the "black box" of algorithms require, among other things, extensive information disclosure. Despite these disclosures' multiple advantages, several authors have repeatedly stressed that "an excessive disclosure of information about the internal logic of a system could infringe on the rights of others, either by revealing protected trade secrets or by violating the privacy of individuals whose data is contained in the training dataset."[238]

Finally, scholars have also argued that privacy runs in tension with the accuracy of automated decisionmaking systems, though some have contested this claim.[239] In Professors Jane Bambauer and Tal Zarsky's view, implementing individual privacy rights, such as the right to opt out or the right to be forgotten, might enable gaming of AI systems and "hamper the firm's ability to use countergaming measures like complexity or constantly changing predictive models."[240] Thus, although they enhance subjects' autonomy and control over their data, these privacy-based measures can be detrimental for the accuracy of the data collected and the data-driven decisions made.

These examples are not uncommon. They demonstrate how privacy does not always align itself with the values algorithmic accountability encompasses. Yet the taxonomic approach fails to acknowledge, let alone resolve, this reality, instead offering an ambiguous criterion of inclusion—social recognition—that may eventually allow algorithmic accountability to find its way into the privacy family.

3. *The Disregarded Tensions Between Privacy and Freedom of Expression.* — Privacy advances freedom of expression by protecting society against another privacy harm: the "chilling effect."[241] Likewise, scholars have described protecting intellectual privacy as essential

238. Sandra Wachter, Brent Mittelstadt & Chris Russell, Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR, 31 Harv. J.L. & Tech. 841, 882–83 (2018) (noting that an excessive disclosure of information about operating systems could violate trade secrets or privacy rights); see also Margot E. Kaminski, Binary Governance: Lessons From the GDPR's Approach to Algorithmic Accountability, 92 S. Cal. L. Rev. 1529, 1580 (2019) ("[E]stablishing accountability in a collaborative governance regime can raise individual privacy concerns.").

239. Notably, the existence of this tension has been disputed by Professors Ignacio Cofone and Katherine Strandburg. See Ignacio N. Cofone & Katherine J. Strandburg, Strategic Games and Algorithmic Secrecy, 64 McGill L.J. 623, 650 (2019) ("Disclosure of information about secret automated decision-making algorithms will increase the threat of gaming by obfuscation or altered input only in a narrow range of circumstances.").

240. Jane Bambauer & Tal Zarsky, The Algorithm Game, 94 Notre Dame L. Rev. 1, 35 (2018).

241. See Citron & Solove, Privacy Harms, supra note 79, at 854 (defining "chilling effect" as a "harm caused by inhibiting people from engaging in certain civil liberties, such as free speech, political participation, religious activity, free association, freedom of belief, and freedom to explore ideas").

to the First Amendment values of free thought and expression.[242] In that sense, self-expression is usually recognized as a value furthered by privacy.

Yet privacy can also be in tension with First Amendment freedom of expression. Despite some precarity,[243] the historical dominance that free expression interests have had over privacy interests (sometimes referred to as "the Supreme Court's maximalist approach to First Amendment law"[244]) is now well-known.[245] "When information is true and obtained lawfully," Professor Fred Cate has noted, "the Supreme Court has repeatedly held that the State may not restrict its publication without showing a very closely tailored, compelling governmental interest."[246]

It is no secret either that many of the most relevant privacy reforms face strong First Amendment obstacles. Despite heavy contestation,[247] multiple scholars have argued that the First Amendment restricts the government's ability to rely on means such as the privacy tort of "disclosure,"

---

242. See Richards, Rethinking Civil Liberties, supra note 60, at 3–5 (showing how free speech and privacy complement each other in the digital age); Richards, Intellectual Privacy, supra note 60, at 394 ("Because the core of the First Amendment is the freedom of thought, if we care about speech, we must care about intellectual privacy."); Paul M. Schwartz, Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence, 52 Stan. L. Rev. 1559, 1572 (2000) [hereinafter Schwartz, Free Speech vs. Information Privacy] (arguing that "information privacy law is an integral part of the mission of free speech and not its enemy").

243. See Amy Gajda, The First Amendment Bubble: How Privacy and Paparazzi Threaten a Free Press 3 (2015) (describing the "First Amendment bubble, in which constitutional protection for press and news media continually expands to the breaking point, jeopardizing future protection not only at the margins but also for the core").

244. Jane Bambauer, Is Data Speech?, 66 Stan. L. Rev. 57, 117 (2014) (arguing that data must receive First Amendment protection).

245. See, e.g., N.Y. Times Co. v. Sullivan, 376 U.S. 254, 279–80 (1964) ("The constitutional guarantees [of the First and Fourteenth Amendments] require, we think, a federal rule that prohibits a public official from recovering damages for a defamatory falsehood relating to his official conduct unless he proves that the statement was made with 'actual malice' . . . ."); see also Peter B. Edelman, Free Press v. Privacy: Haunted by the Ghost of Justice Black, 68 Tex. L. Rev. 1195, 1198 (1990) ("If the right to publish private information collides with an individual's right not to have that information published, the Court consistently subordinates the privacy interest to the free speech concerns. Its rationale for doing so is quite mysterious.").

246. Fred H. Cate, Principles of Internet Privacy, 32 Conn. L. Rev. 877, 887 (2000) [hereinafter Cate, Principles of Internet Privacy].

247. See Neil M. Richards, Reconciling Data Privacy and the First Amendment, 52 UCLA L. Rev. 1149, 1166 (2005) [hereinafter Richards, Reconciling] (criticizing scholars who have "improperly conflated information flows—such as the sale of a database—with the 'freedom of speech' protected by the First Amendment"); Schwartz, Free Speech vs. Information Privacy, supra note 242, at 1559 (disputing Volokh's idea that "the government's safeguarding of information privacy endangers a wide range of speech unrelated to personal data").

criminal laws prohibiting the publication of the names of rape victims, or privacy laws limiting the sale of personal data.[248]

Some scholars have gone so far as to claim that the First Amendment's protections apply not only to disseminating data but to collecting it as well.[249] For Professor Jane Bambauer, the right to freedom of speech carries an implicit right to knowledge creation through data acquisition.[250] In practice, this could result in data protection laws having to withstand judicial scrutiny under the First Amendment.[251] As Bambauer has written, "[C]ourts will need to scrutinize whether a privacy law is actually tailored to specific, weighty interests in seclusion or confidentiality. A well-tailored regulation will create limitations on particular disclosures and misuses of information, rather than creating global bans on data collection and distribution."[252] Bambauer's arguments are contested within the privacy literature.[253] But the view that free speech may protect data collection also appears in the context of civil accountability. As Professor Margot Kaminski has explored, the prevailing view among federal appellate courts holds that the First Amendment also includes a right to record.[254] Therefore, filming the police, at least in public, constitutes a constitutionally protected activity.[255]

---

248. See, e.g., Cate, Principles of Internet Privacy, supra note 246, at 887 (requiring that restrictions on publication of truthful and lawfully obtained information must demonstrate "a very closely tailored, compelling governmental interest"); Singleton, supra note 23, at 97 ("The courts should think twice before sacrificing the mature law of free speech to the less coherent concerns about privacy."); Rodney A. Smolla, Privacy and the First Amendment Right to Gather News, 67 Geo. Wash. L. Rev. 1097, 1138 (1999) ("As matters stand today, strong First Amendment doctrines stand in the way of many of the most meaningful privacy reforms."); Volokh, supra note 23, at 1051 ("While privacy protection secured by contract is constitutionally sound, broader information privacy rules are not easily defensible under existing free speech law.").

249. See, e.g., Bambauer, supra note 244, at 63 ("[F]or all practical purposes, and in every context relevant to the current debates in information law, data is speech. Privacy regulations are rarely incidental burdens to knowledge. Instead, they are deliberately designed to disrupt knowledge creation."); Froomkin, supra note 36, at 1508 ("The First Amendment protects the freedom of speech and of the press, but does not explicitly mention the right to gather information. However, both the Supreme Court and appellate courts have interpreted the First Amendment to encompass a right to gather information.").

250. See Bambauer, supra note 244, at 60 ("This Article contends that the freedom of speech carries an implicit right to create knowledge. When the government deliberately interferes with an individual's effort to learn something new, that suppression of disfavored knowledge is presumptively illegitimate and must withstand judicial scrutiny.").

251. See id.

252. Id. at 114.

253. See, e.g., Richards, Rethinking Civil Liberties, supra note 60, at 89–90 (warning that the adoption of the "data is speech" position will turn into "digital *Lochner*").

254. See Margot E. Kaminski, Privacy and the Right to Record, 97 B.U. L. Rev. 167, 168 (2017) ("Recent cases, however, have recognized a First Amendment 'right to record.'").

255. See id. at 181 ("[R]ecording police activity should be squarely protected by the First Amendment, both because the recording serves a government oversight function and because it can inform future policy choices.").

This conflict is well-known and highly discussed, but the taxonomic approach to privacy provides little insight into the longstanding tensions between privacy and freedom of expression. By allowing self-expression to be adopted into the capacious privacy family, it not only fails to address those conflicts but also obscures them.[256]

4. *Emerging Conflicts Within Privacy and Among Privacy Problems.* — So far, all-embracing or umbrella approaches to privacy appear to beget conflicts *within* privacy—that is, among privacy-associated values. When the value of equality, which underpins the feminist and queer-studies criticisms of privacy, itself becomes part of the privacy family, discrimination is an issue that privacy both expands and exacerbates as well as a value it protects.[257] For example, privacy disempowers marginalized populations by rendering their oppression less visible. Yet at the same time, privacy also empowers them to resist unequal treatments that result from the misuse of their information. Because these are now all dimensions of the same concept of privacy, privacy ends up both promoting and undermining itself.[258] How can privacy be balanced against privacy?

The expansive nature of the privacy umbrella allows for more direct conflicts as well—namely, conflicts that appear to be *among* privacy problems. As privacy problems multiply, so does the range of conflicts between them. Labeling everything as "privacy" diminishes scholars' capacity, not to mention the capacity of lawmakers and courts, to balance information harms, one against the next. It seems defensible, for example, for a commentator or polity to decide that antidiscrimination represents a higher value than information privacy in many contexts. But if every information harm involves privacy, then it is clear neither analytically nor pragmatically how privacy may yield to discrimination.

As new privacy problems are welcomed into the umbrella, it becomes evident how mitigating these problems implicates other, well-known privacy problems. This is what Pozen has referred to as "*dimensional tradeoffs*," whereby "[t]argeting one privacy risk creates a new, countervailing risk."[259] For example, the police must invade a stalking

256. There are some exceptions. See Richards, Reconciling, supra note 247, at 1150–52 (arguing for greater reconciliation between data privacy and the First Amendment and claiming that many data privacy rules "are fully justifiable under well-established First Amendment theory, either because they do not regulate 'speech' protected by the First Amendment, or because they are legitimate speech regulations under existing doctrine").

257. Analogously, many social or political movements embody a tension between inclusivity and focus. See, e.g., Davidson, supra note 231, at 63–65 (exploring this tension in the context of activists' discourse about inclusion under the "transgender umbrella" circa 2007). Thank you to Kendra Albert for this analogy.

258. Something similar happens with freedom of expression. Privacy has long been thought to further free speech. Yet different types of privacy invasions (e.g., personal data collection, data recording of the police or farming operations) are considered part of free speech. Free speech has thus turned out to be both a value that privacy furthers and a privacy problem.

259. Pozen, supra note 20, at 230.

suspect's privacy to investigate the suspect's surveillance of a victim. Developers of artificial intelligence must give third parties access to training databases with personal information to try to resolve or mitigate algorithmic bias or unfairness in their systems. Stalking is a privacy problem, but so is surveillance. Bias is a privacy problem, but so is access.

The taxonomic approach is silent—even agnostic—as to these emerging conflicts. As Pozen has accurately warned since 2016, "[t]he danger of this approach is that *it increases the likelihood of intraprivacy conflicts* (by recognizing more claims as privacy claims) *while simultaneously depriving us of resources to resolve them* (by refusing to supply a hierarchy of privacy principles)."[260] Like a strong wind, this danger will eventually cause the worn-out privacy umbrella to flip inside out.

## III. BEYOND SOCIAL TAXONOMY: A PRIVACY RESEARCH AGENDA

Here is the argument thus far. For over a century, privacy scholars sought to define privacy by reference to a unitary concept—often involving control over or access to the self. Dissatisfaction with this quixotic project led to the embrace of an attractive alternative: the social-taxonomic approach. This approach, however, eschews analytic efforts at definition, instead emphasizing privacy problems and pitching a big tent encompassing *any* problem that the right people or institutions have come to recognize as implicating privacy. This pluralist, pragmatic approach opened the door to a shift in emphasis from defining to doing, as well as the broadening of privacy to encompass information-based harms such as discrimination and algorithmic manipulation. Yet the approach is beginning to wear thin, particularly when it comes to determining what constitutes a privacy problem. Social recognition provides no answers for critical questions about the legitimacy and authority of voices in the field. And addressing conflicts between values under the umbrella or among privacy problems without a framework that distinguishes among them turns out to be a problem of its own.

The final Part of this Essay briefly sketches the contours of a post-taxonomic approach to privacy. The time has come to take a deeper look at the reasons why a given problem merits study under a privacy framework. If everything that touches information is a privacy problem just because people say so, what are privacy scholars experts in? This Essay does not advocate a return to the search for a specific and unitary definition of privacy.[261] Nor does it deny the importance of furnishing policymakers and jurists, who are often reticent to intervene on behalf of

260. Id. at 243.

261. For one of the latest essentialist efforts of this type, see Bellin, supra note 20, at 471 (pushing back on privacy pluralists and proposing a baseline definition of privacy to anchor legal discourse).

privacy victims, with a concrete set of privacy harms.[262] But it does reject the viability of relying solely on social recognition to define privacy problems.

A post-taxonomic approach to privacy grapples with an admittedly difficult question: Exactly what work is the concept of privacy doing? This question permits anyone—irrespective of their role in society or how many voices agree with them at the moment—to press the case that a given problem is worthy of study from a privacy standpoint. The criteria for what makes the problem a privacy problem, however, should be something other than social recognition or a vague resemblance. Building on other privacy scholars' work, this Essay takes the view that privacy problems sit somewhere at the intersection of observation and power. In that sense, to qualify as a privacy problem, we think, a given phenomenon must involve: (1) an observation that (2) exposes individuals to unbalanced information relationships and (3) that renders them vulnerable[263] and/or powerless.[264]

---

262. See Citron & Solove, Privacy Harms, supra note 79, at 799 (providing a typology to "clear away the fog so that privacy harms can be better understood and appropriately addressed").

263. Various scholars, including one of us, have theorized extensively about the relationship between vulnerability and privacy/data protection. See, e.g., Ryan Calo, Privacy, Vulnerability, and Affordance, 66 DePaul L. Rev. 591, 602 (2017) (arguing that privacy plays a complex role as both a shield and a sword for vulnerability and proposing to conceptualize it as an affordance); Gianclaudio Malgieri & Jędrzej Niklas, Vulnerable Data Subjects, Comput. L. & Sec. Rev., July 2020, at 1, 6 (foregrounding the role and potentiality of the notion of "vulnerable data subjects" in the data protection field and proposing the adoption of a layered approach to vulnerability in European law); Nora McDonald & Andrea Forte, The Politics of Privacy Theories: Moving From Norms to Vulnerabilities, CHI '20: Proc. of the 2020 CHI Conf. on Hum. Factors in Computing Sys., Ass'n for Computing Mach., Apr, 30, 2020, at 1, 8 (proposing to augment existing privacy frameworks by integrating intersectional and queer-Marxist theories that allow researchers to look at what creates the privacy shortfalls of vulnerable populations).

264. Several privacy law scholars have for years foregrounded the role of power in information relationships. See, e.g., Julie E. Cohen, Examined Lives: Informational Privacy and the Subject as Object, 52 Stan. L. Rev. 1373, 1408 (2000) ("The data processing paradigm conceals a power relationship, and that relationship, in turn, is a crucial determinant of the truth that data processing constructs."); Neil M. Richards, The Information Privacy Law Project, 94 Geo. L.J. 1087, 1094 (2006) [hereinafter Richards, Information Privacy Law Project] ("I am in basic agreement with these scholars that a greater attention to both the architectures of information flow and the power asymmetries involved in information relationships is warranted."); Neil Richards & Woodrow Hartzog, A Relational Turn for Data Protection?, 6 Eur. Data Prot. L. Rev. 492, 492–93 (2020) [hereinafter Richards & Hartzog, A Relational Turn] ("Data is dangerous in the hands of these companies not just because it is personal to us, but because in their hands it becomes power that can be wielded to control people and institutions. It exposes us in ways that risk more than just identification or denial of control." (footnote omitted)); Solove, Conceptualizing Privacy, supra note 14, at 1142 ("Privacy is an issue of power; it is not simply the general expectations of society, but the product of a vision of the larger social structure."); Solove, Limitations of Privacy Rights, supra note 181, at 979 ("Privacy is about power. Rights can't empower individuals enough to equalize the power imbalance between individuals and the organizations that collect and use their data." (footnote omitted)); Daniel J. Solove, Privacy and Power: Computer

An essentialist definition is not the only path forward. Recent scholarship has embraced a *functional* account of privacy that defines the field in terms of the specific set of problems privacy exists to address.[265] Rather than define privacy per se, socially or otherwise, this approach interrogates what privacy is "for." As early as 1968, Professor Charles Fried argued that privacy is the necessary atmosphere for "respect, love, friendship and trust."[266] As explained by Fried, "Privacy is not merely a good technique for furthering these fundamental relations; rather without privacy they are simply inconceivable. They require a context of privacy or the possibility of privacy for their existence."[267] In 1980, Gavison proposed "the promotion of liberty, autonomy, selfhood, and human relations, and furthering the existence of a free society" as the set of functions that privacy has in our lives.[268]

Cohen has also delved into the purpose of privacy. In her canonical 2013 article *What Privacy Is For*, Cohen contended that privacy is distinct because it preserves "breathing room" for the critical, emergent, and relational subjectivity needed for liberal democracy and innovation to thrive and "engage in socially situated processes of boundary management."[269] Similarly, in his recent book *Why Privacy Matters*, Richards claimed that privacy furthers identity, freedom, and protection, which he described as "human values that make our lives better, both as individuals and as members of society."[270] The functional approach highlights what is unique and valuable about privacy without trying to define the term in the abstract.

An explicit set of criteria for privacy or privacy problems permits immediate discussion of a phenomenon, whether or not the right people or institutions talk a certain way, so long as the proponent can convincingly

---

Databases and Metaphors for Information Privacy, 53 Stan. L. Rev. 1393, 1399 (2001) ("Databases alter the way the bureaucratic process makes decisions and judgments affecting our lives; and they exacerbate and transform existing imbalances in power within our relationships with bureaucratic institutions."); Ari Ezra Waldman, Privacy, Practice, and Performance, 110 Calif. L. Rev. 1221, 1227 (2022) ("[T]he goal is to perform privacy law in emancipatory ways—namely, to address the ways in which data-extractive capitalism creates vulnerabilities, power asymmetries, and subordination.").

265. See infra notes 266–270.

266. See Fried, supra note 11, at 477.

267. Id.

268. See Gavison, Privacy and the Limits of Law, supra note 12, at 423.

269. See Cohen, What Privacy Is For, supra note 31, at 1909–12 (internal quotation marks omitted) (quoting Julie E. Cohen, Configuring the Networked Self: Law, Code and the Play of Everyday Practice 149 (2020)).

270. See Richards, Why Privacy Matters, supra note 92, at 5–6. Notably, Solove himself has taken a functional approach to privacy, stating that privacy should be "valued as a means for achieving certain other ends that are valuable." Solove, Conceptualizing Privacy, supra note 14, at 1145. Unlike Fried, Gavison, Cohen, and Richards, however, who are clear about the values that privacy serves, Solove avoids committing to a specific value. Instead, he contends that the values that privacy promotes vary in different contexts. See id. at 1145–46.

ground the problem in privacy. The word "explicit" is key in this endeavor. Qualitative researchers have furnished the term "reflexivity" to describe the tool or method by which "the researcher engages in an explicit, self-aware meta-analysis of the research process."[271] As a practice, reflexivity not only cultivates self-awareness about the normative presuppositions underlying the researcher's knowledge claims and their "inescapable linkage to researcher positionality"[272] but also invites the researcher to make those assumptions visible.[273] According to Professor Roni Berger, "Reflexivity is demonstrated by use of first-person language and provision of a detailed and transparent report of decisions and their rationale."[274] As in the social sciences, we believe that privacy scholarship would highly benefit from scholars' reflexive accounts of their assumptions and rationale for bringing privacy into a given conversation about information-based problems.

For an information-based problem to be of interest to privacy law and scholarship, it need not involve *only* privacy. Few do. The problem of unaccountable algorithms or information capitalism is hardly limited to government or corporate love of data. But privacy discourse should arguably focus on the aspects of the problem our methods and literature illuminate. Tackling the enormous issue of online misinformation, for example, represents privacy scholarship to the extent the inquiry centers around core privacy concerns such as intrusion or (now) data-driven manipulation. We may simply have wiser things to say about the way

---

271. Linda Finlay, "Outing" the Researcher: The Provenance, Process, and Practice of Reflexivity, 12 Qual. Health Rsch. 531, 531 (2002). Reflexivity is just one of the possible methods used by qualitative researchers to acknowledge, self-evaluate, and respond to their "positionality," or "the multiple, unique experiences that situate each of us." David Takacs, How Does Your Positionality Bias Your Epistemology?, 19 Thought & Action 27, 33 (2003). In that sense, reflexivity can be considered as a strategy for "situating knowledges." See Gillian Rose, Situating Knowledges: Positionality, Reflexivities and Other Tactics, 21 Progress Hum. Geography 305, 306 (1997) ("Reflexivity in general is being advocated by these writers as a strategy for situating knowledges: that is, as a means of avoiding the false neutrality and universality of so much academic knowledge.").

272. See Louise Folkes, Moving Beyond 'Shopping List' Positionality: Using Kitchen Table Reflexivity and In/Visible Tools to Develop Reflexive Qualitative Research, 23 Qual. Rsch. 1301, 1302 (2023) (citing Jennifer Mason, Qualitative Researching (2d ed. 2002); Anne E Pezalla, Jonathan Pettigrew & Michelle Miller-Day, Researching the Researcher-as-Instrument: An Exercise in Interviewer Self-Reflexivity, 12 Qual. Rsch. 165 (2012); Jeff Rose, Dynamic Embodied Positionalities: The Politics of Class and Nature Through a Critical Ethnography of Homelessness, 23 Ethnography 451 (2020)).

273. See Dongxiao Qin, Positionality, *in* The Wiley Blackwell Encyclopedia of Gender and Sexuality Studies 2 (Nancy A. Naples ed. 2016) ("The reflexivity of researcher's positionality seeks to clarify the personal experiences that have shaped this research inquiry and to make transparent the reflexivity that informs the analyses and theorizing process.").

274. Roni Berger, Now I See It, Now I Don't: Researcher's Position and Reflexivity in Qualitative Research, 15 Qual. Rsch. 219, 222 (2015).

Cambridge Analytica enables the targeting of political messages[275] than we do about the prevalence or impact of Russian disinformation bots.

The question of what work privacy is doing helps disentangle privacy harms from other information-based harms, each of which may merit its own treatment. We take this to be Mulligan and Dwork's insight about algorithmic fairness when they say that "it's not privacy and it's not fair."[276] Mulligan and Dwork understand that lumping questions of fairness into discussions of surveillance can potentially dilute both.[277]

And we take it to be Schwartz's point when he discusses the limited utility of the concept of privacy in the context of government use and abuse of databases.[278] Today, there are entire conferences about algorithmic fairness and accountability.[279] There are special volumes in law reviews dedicated to the role of data-driven decisionmaking in administrative law.[280] Privacy scholars participate in this discourse as privacy scholars only when they say something about privacy itself—for example, the role of observation and power. Otherwise, they are participating as scholars of due process or other aspects of constitutional or administrative law.

Focusing on the precise work privacy is doing within contemporary information problems could also help explain why some invocations of privacy should be given credence, while others—for example, corporations hoping to avoid transparency or lawmakers trying to enforce rigid gender norms—should be entirely discounted. At most, the social-taxonomic approach can sort such claims into this or that category of privacy problem. But they are not truly privacy problems, no matter how many people or institutions say so. They are not even problems so much as cynical rhetorical strategies aimed at another objective.[281]

---

275. See Jeremy B. Merrill & Olivia Goldhill, These Are the Political Ads Cambridge Analytica Designed for You, Quartz (Jan. 10, 2020), https://qz.com/1782348/cambridge-analytica-used-these-5-political-ads-to-target-voters [https://perma.cc/BL2B-734W] (describing Cambridge Analytica's advertising tactics, which used data (including stolen Facebook data) to target voters based on their personality traits).

276. Dwork & Mulligan, supra note 31, at 35 (cleaned up).

277. See id. at 37 ("Exposing the datasets and algorithms of big data analysis to scrutiny—transparency solutions—may improve individual comprehension, but given the independent (sometimes intended) complexity of algorithms, it is unreasonable to expect transparency alone to root out bias.").

278. Schwartz, Data Processing, supra note 31, at 1347.

279. See, e.g., ACM Conference on Fairness, Accountability, and Transparency (ACM FAccT), https://facctconference.org [https://perma.cc/2C6F-U9HZ] (last updated Oct. 17, 2023).

280. See, e.g., Volume 71, Number 6 (March 2022): Fifty-Second Annual Administrative Law Issue: Automating the Administrative State, Duke L.J., https://scholarship.law.duke.edu/dlj/vol71/iss6/ [https://perma.cc/8HX6-9F6A] (last visited Feb. 6, 2024).

281. As Pozen has perceptively pointed out, "it is important to remain on guard against false tradeoffs, exaggerated countervailing risks, and overly reductive logic in debates over privacy reform." Pozen, supra note 20, at 245.

Understanding why that is involves understanding what privacy is about.

This foregrounding of the role of the concept of privacy—foreshadowed by leading and emerging privacy theorists[282]—could begin to furnish a roadmap for analyzing tensions among and between privacy problems and the values that underpin them. In fact, it could contribute to the development of normative frameworks—long called for by Pozen in privacy theory—for when policymakers must make hard choices and weigh various privacy interests.[283]

It can be true that algorithmic hiring constitutes a privacy problem because it reduces people to data and pulls information from surprising or nonconsenting sources. It can also be true that algorithmic hiring poses a discrimination problem because the data the systems draw from to form their models are biased against historically marginalized people. And it can be true that addressing bias involves sifting through personal data in ways that implicate privacy.[284] But unless we articulate what sort of value privacy is, it is not clear how that value can be weighed against another, perhaps better-articulated value, such as antidiscrimination.

Finally, clearly identifying privacy's role within contemporary information problems may give American privacy scholarship the opportunity to engage in contemporary global discussions about how to best govern data in the digital age. One of those discussions addresses the distinction between the concepts of privacy and data protection. European scholars have mostly dominated this conversation after the Right to Data Protection was listed as a fundamental right in Article 8 of the Charter of Fundamental Rights of the European Union.[285] Authors have debated whether data protection is a simple facet of

---

282. See Cohen, What Privacy Is For, supra note 31, at 1911 (arguing that privacy is not a legal protection for the liberal self but, rather, a fundamental tool for protecting the boundary management practices needed for self-determination); Richards, Why Privacy Matters, supra note 92, at 5–6 (arguing that privacy can promote and safeguard identity, freedom, and protection); Viljoen, supra note 31, at 578 (highlighting the limits of privacy law's focus on individual selfhood).

283. See Pozen, supra note 20, at 243 ("The development of normative frameworks for evaluating privacy-privacy tradeoffs is an increasingly urgent task for the privacy field.").

284. We understand that bias is systemic, that algorithmically sorting people may be inherently oppressive, and that the evidence is that completely de-biasing models does not seem to be possible as a factual matter. See Zeerak Waseem, Smarika Lulz, Joachim Bingel & Isabelle Augenstein, Disembodied Machine Learning: On the Illusion of Objectivity in NLP 2 (Jan. 28, 2021) (unpublished manuscript), https://openreview.net/pdf?id=fkAxTMzy3fs [https://perma.cc/6WTZ-K4YT] (explaining that "[b]y contextualising bias in these terms, we seek to shift the discourse away from bias and its elimination towards subjective positionality"). We use this context only as an example.

285. See infra notes 298–300.

privacy,[286] a different but interdependent right,[287] or an autonomous one with its own added value.[288] In the United States, Professors Margot Kaminski and Meg Leta Jones recently examined the distinctions between privacy law and data protection law[289] as well as the differences between the U.S. and E.U. approaches to data privacy.[290] Similar analyses have also been done in the past by Cate;[291] Professors Paul Schwartz and Karl-

286. See, e.g., Antoinette Rouvroy & Yves Poullet, The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy, *in* Reinventing Data Protection? 45, 61–62 (Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne & Sjaak Nouwt eds., 2009) (exploring how the data protection facet followed the "seclusion" and "noninterference" facets of privacy).

287. See, e.g., Hielke Hijmans, The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU, at 66 (2016) ("[P]rivacy and data protection are different concepts. The right to privacy represents a normative value, whereas the right to data protection represents a legal structure aimed at allowing individuals to claim that their data should be fairly and lawfully processed."); Paul De Hert & Serge Gutwirth, Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power, *in* Privacy and the Criminal Law 61, 62–63 (Erik Claes, Antony Duff & Serge Gutwirth eds., 2006) (describing privacy as a "tool of opacity" and data protection and criminal procedure as "tools of transparency" while emphasizing the importance of "ascertaining the differences in scope, rationale and logic" between these tools and the rights they protect (internal quotation marks omitted)); Norberto Nuno Gomes de Andrade, Data Protection, Privacy, and Identity: Distinguishing Concepts and Articulating Rights *in* Privacy and Identity Management for Life 90, 96 (Simone Fischer-Hübner, Penny Duquenoy, Marit Hansen, Ronald Leenes & Ge Zhang eds., 2011) ("[A] crucial distinction can be made between data protection, on the one hand, and privacy and identity on the other. Data protection is procedural, while privacy and identity are substantive rights.").

288. See, e.g., Orla Lynskey, The Foundations of EU Data Protection Law 90 (2015) (explaining that data protection may be viewed as "an independent right which serves a multitude of functions including, but not limited to, the protection of privacy" and arguing that "data protection offers individuals enhanced control over their personal data"); Lorenzo Dalla Corte, A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection, *in* Data Protection and Privacy: Data Protection and Democracy 27, 29 (Dara Hallinan, Ronald Leenes, Serge Gutwirth & Paul De Hert eds., 2020) ("[D]ata protection is evolving away from privacy into something entirely distinct, albeit still connected to it."); Orla Lynskey, Deconstructing Data Protection: The 'Added Value' of a Right to Data Protection in the EU Legal Order, 63 Int'l & Comp. L. Q. 569, 573 (2014) ("[D]ata protection offers individuals more rights over more types of information than the right to privacy."); Maria Tzanou, Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a Not So New Right, 3 Int'l Data Priv. L. 88, 88 (2013) ("The two rights seem to share a parent–child relationship. Data protection appeared as an offspring of privacy and the two rights still seem inextricably tied up together with a birth cord. However—as does any child—data protection is trying to mark its own way in life.").

289. Meg Leta Jones & Margot E. Kaminski, An American's Guide to the GDPR, 98 Denv. L. Rev. 93, 97–101 (2020) (noting that "[d]ata protection arguably has a different scope than privacy").

290. Id. at 106–11 (discussing several ways in which the U.S. approaches to information or data privacy differ from European-style data protection).

291. See Fred H. Cate, The Changing Face of Privacy Protections in the European Union and the United States, 33 Ind. L. Rev. 173, 179 (1999) (acknowledging the differences between the American and the European contexts that would impede the extension of the E.U. data protection directive to the United States).

Nikolaus Peifer;[292] and Professors Chris Jay Hoofnagle, Bart van der Sloot, and Frederik Zuiderveen Borgesius.[293] There has yet to be, however, a substantial discussion of the advantages, drawbacks, and feasibility of adopting a data protection approach in the American context nowadays. Richards once argued that given that privacy "is itself a troublesome concept, whose vagueness eludes definition and whose historical and conceptual baggage complicates and limits efforts to distill it to a particular essence," it would be more convenient to "provide a better conceptual home for the problems of personal data than the troublesome metaphors of 'privacy': data protection [law] and confidentiality [law]."[294] This discussion is worth continuing today.

Meanwhile, global discussions are moving beyond data protection entirely in favor of broader discussions of information governance and harm mitigation. In 2019, for example, Canada started a larger-scale overhaul of its data privacy landscape with the announcement of its digital charter.[295] Consequently, on June 16, 2022, it introduced the Digital Charter Implementation Act (Bill C-27), which amends the country's data

---

292. See Paul M. Schwartz & Karl-Nikolaus Peifer, Transatlantic Data Privacy Law, 106 Geo. L.J. 115, 121–38 (2017) (analyzing the respective legal identities constructed around data privacy in the European Union and the United States).

293. See generally Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, The European Union General Data Protection Regulation: What It Is and What It Means, 28 Info. & Commc'ns Tech. L. 65 (2019) (highlighting how the EU's GDPR differs from U.S. privacy law).

294. Richards, Information Privacy Law Project, supra note 264, at 1088, 1134–35. With both Solove and Hartzog, Richards has taken the law of confidentiality seriously. See Woodrow Hartzog & Neil Richards, Legislating Data Loyalty, 97 Notre Dame L. Rev. Reflection 356, 358 (2022), https://ndlawreview.org/wp-content/uploads/2022/07/Hartzog-and-Richards_97-Notre-Dame-L.-Rev.-Reflection-356-C.pdf [https://perma.cc/F9UZ-Z8FL] (proposing a legislative model for applying the duty of loyalty to privacy law); Woodrow Hartzog & Neil Richards, The Surprising Virtues of Data Loyalty, 71 Emory L.J. 985, 992 (2022) (arguing that "clarifying the duty of loyalty is, in fact, the single most important factor enabling its potential as a key cog in a meaningful data privacy framework"); Neil Richards & Woodrow Hartzog, A Duty of Loyalty, supra note 99, at 967 (proposing that a duty of loyalty be applied to American privacy law); Richards & Hartzog, A Relational Turn, supra note 264, at 494 (noting that scholars are increasingly turning to confidentiality and relationships-based models of trust to ground privacy law); Neil Richards & Woodrow Hartzog, Taking Trust Seriously in Privacy Law, 19 Stan. Tech. L. Rev. 431, 459–62 (2016) (conceptualizing confidentiality as a form of discretion that should shape privacy law); Neil M. Richards & Daniel J. Solove, Privacy's Other Path: Recovering the Law of Confidentiality, 96 Geo. L.J. 123, 133–45 (2007) (tracing the history of confidentiality as a protected aspect of law before the birth of the right to privacy); Neil Richards & Woodrow Hartzog, Privacy's Trust Gap: A Review, 126 Yale L.J. 1180, 1188 (2017) (book review) (arguing that privacy rights can be revitalized using a foundation of trust through concepts like confidentiality). Nevertheless, with regards to data protection law, it appears like there's been a lot of water over the dam since.

295. See Canada's Digital Charter in Action: A Plan by Canadians, for Canadians, Minister's Message, Gov't of Can. (May 21, 2019), https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter/canadas-digital-and-data-strategy [https://perma.cc/USW2-UTR3] (last updated Oct. 23, 2019).

privacy statute at the federal level, establishes a tribunal specializing in privacy and data protection and, more importantly, purports to enact the Artificial Intelligence and Data Act.[296] The latter act "aims to protect individuals against a range of serious risks associated with the use of artificial intelligence systems, including risks of physical or psychological harm or biased output with adverse impacts on individuals."[297]

Similarly, since 2020, the European Union has adopted a comprehensive approach to data, which seeks to increase the use and demand of data as well as promote the adoption of artificial intelligence.[298] The European Union has been in the process of approving various legislative acts that, complementing its data protection regime, look to (1) establish an appropriate regulatory framework regarding data governance, access, and reuse;[299] and (2) address the multiple types of risks associated with the use of artificial intelligence.[300] With a better understanding of privacy's role, and therefore its limits, American privacy scholars will be in a better position to evaluate, and even consider, these broader approaches to data governance.

Ultimately, privacy is not the only value at play in a complex digital ecosystem. For privacy scholarship to remain relevant, the field needs to move beyond the comfortable habit of labeling whatever information-based harm the right people are talking about as a "privacy problem." This worked for a time and got the field out of an analytic tailspin. That time

---

296. See Bill C-27: An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to Other Acts, Charter Statement, Gov't of Can. (Nov. 4, 2022), https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c27_1.html [https://perma.cc/PT3A-EX2Z] [hereinafter Bill C-27 Charter Statement] (last updated Nov. 10, 2022); Lisa R Lifshitz, Roland Hung & Cameron McMaster, Proposed Canadian Privacy Bill Introduces Fines and New Requirements for Private Organizations, ABA (July 6, 2022), https://www.americanbar.org/groups/business_law/resources/-business-law-today/2022-july/proposed-canadian-privacy-bill/ (on file with the *Columbia Law Review*) (describing the introduction and effects of Bill C-27).

297. Bill C-27 Charter Statement, supra note 296.

298. See Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data, at 1, COM (2020) 66 final (Feb. 19, 2020); European Commission, White Paper on Artificial Intelligence—A European Approach to Excellence and Trust, at 25–26, COM (2020) 65 final (Feb. 19, 2020); European Commission Press Release IP/20/273, Shaping Europe's Digital Future: Commission Presents Strategies for Data and Artificial Intelligence (Feb. 19, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273 [https://perma.cc/UMN4-448U] (last updated Feb. 26, 2020).

299. See, e.g., Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act), at 1, COM (2020) 767 final (Nov. 25, 2020); Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act), at 3, COM (2022) 68 final (Feb. 23, 2022).

300. See Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, at 3, COM (2021) 206 final (Apr. 21, 2021).

has passed. Privacy scholars cannot avoid the questions of just what it is we are studying and what it is that privacy law should look to address. This does not necessitate a unitary definition. But it does require a deeper discussion of the set of questions—and problems—that are unique to privacy scholarship and the law it influences.

## CONCLUSION

Social taxonomy offered an attractive way out of the elusive search for the definition of privacy. In its place, the social-taxonomic approach welcomed under a common tent the many problems that people and institutions have associated with privacy since the turn of the twentieth century. The tent now shelters more problems—such as information-based discrimination and manipulation—than those widely recognized at the dawn of the social-taxonomic approach. And scholars have branched out from defining privacy to understanding and even addressing the consequences of its absence. Today, the conversation is less about what privacy is than what privacy is for.

This Essay has nevertheless argued that social taxonomy fails to provide a useful framework for determining what constitutes a privacy problem and, as a consequence, has begun to disserve the community. Not everyone or everything is staying safe and dry under the tent. The criterion of social recognition raises difficult questions about *whose* attention matters. Until recently, these questions have been elided in mainstream privacy law discourse. Social recognition also obscures tensions between privacy and other values and exacerbates the issue of privacy–privacy tradeoffs, offering no coherent framework by which to reconcile new and old conflicts between family members.

The way forward involves confronting the defects in social taxonomy without revisiting the quixotic search for a single, perfect definition of privacy. Under a functional approach, for instance, the field can say—and has said—what work privacy is doing without having to agree on its essential nature. Privacy scholarship and law take place against a complex backdrop of societal values and information-based harms. Though it is not an easy task, the field should return its focus to the precise work privacy is doing. Some of privacy scholarship's leading lights are already heading in this direction. We join these voices in calling for a deeper and more explicit understanding of the specific value of privacy in this complicated digital world.

What is the *role* of privacy in a complex information environment? What is it that privacy scholarship and law should look to address in this context? What is the set of *questions* that are unique to our field? What types of *problems* are our *methods* and *literature* best suited to tackle? Privacy scholars will hopefully begin to address these types of questions before studying

an issue under a privacy framework, aiming to participate in ongoing, global discussions about information governance and harm mitigation.

The field of privacy, especially information privacy, has benefited from the freedom to expand and shift emphasis. The social taxonomy did indeed expand the tent and provide shelter from the storm. Having achieved a level of stability and strength, however, the field should consider owning up to the flaws of social recognition and the many, growing conflicts between the loose family members huddled under the same tent. It is still raining out there, but the wear and tear of the tent is beginning to show.