2021

What is Privacy? That's the Wrong Question

Woodrow Hartzog
Boston University School of Law

What is Privacy? That's the Wrong Question

Woodrow Hartzog†

Every year on the first day of my course on information privacy law, I ask my students to define the concept of privacy. Usually, I get a few different answers, each of which is built around some singular and definitive conceptualization of privacy. Some notions include: Privacy is "control over personal information." Privacy is "secrecy." Privacy is the "right to be left alone." And so on. Then I gently push back, asking my students about notions of privacy that fall outside their definition. Which definition should the law adopt? All of these definitions seem right, yet somehow not enough. I ask whether it is a good idea to define privacy so broadly that it is synonymous with all personal interference. My goal is for students to appreciate that there are many ways to conceptualize privacy, each of which is underinclusive or overinclusive. I point to the many ways that scholars have explored various components of the important but remarkably vague notion of privacy, happy to leave its definitive boundaries undefined. Scholars and lawmakers are not always so comfortable with such uncertainty; I have made my peace.

Throughout history, privacy has evaded a precise meaning. Initially, lawmakers had no compelling need to give the concept a singular legal definition. The earliest personal information and surveillance rules and frameworks for privacy leveraged specific concepts such as solitude, confidentiality, and substantive due process.[1] But after Samuel Warren and future-Justice Louis Brandeis called for a "right to privacy" in 1890, the concept took on new life as a term of art in legal frameworks.[2] Plaintiffs in tort

† Professor of Law and Computer Science, Northeastern University. I would like to thank Daniel Solove and Ryan Calo for their feedback, Alissa Gutierrez for her research assistance, and Brenna Darling, Kelly Gregg, Kelly McGee, Tyler Wood, and the staff of the *University of Chicago Law Review* for their editing and shepherding this Essay to press.

1 *See* Daniel J. Solove, *A Brief History of Information Privacy Law*, *in* PROSKAUER ON PRIVACY 1-1, 1-4 to 1-10 (Kristen J. Mathews ed., 2006).

2 *Id.* at 1-10 (citing Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890)).

cases were asked to articulate the private nature of facts and actions.[3] Judges confronted with the argument that the state had violated a defendant's Fourth Amendment rights were asked to determine whether the defendant had a "reasonable expectation of privacy" in the activity or space that the state had invaded.[4] State and federal legislators created numerous statutes that sought to protect "private" information from exposure.[5] In short, from the early 1900s to the present day, lawmakers and judges have regularly been compelled to give the term "privacy" a broad and consistent legal meaning. It hasn't gone well.

Daniel Solove, the John Marshall Harlan Research Professor of Law at the George Washington University Law School and perhaps the most prominent and influential privacy scholar of our day, wrote at the turn of the millennium that privacy was "a concept in disarray."[6] In his foundational book *Understanding Privacy*, Solove noted that people have defined privacy in many different ways, including "freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations."[7] In the twentieth century, privacy theorists seemed intent on crafting a definitive, singular meaning for privacy. Alan Westin wrote that "[p]rivacy 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."[8] Charles Fried similarly argued that "[p]rivacy . . . is the *control* we have over information about ourselves."[9] Ernest Van Den Haag wrote that "[p]rivacy *is* the exclusive access of a person (or other legal entity) to a realm of his

---

3 *See id.* at 1-13 to 1-17. *See generally* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960); RESTATEMENT (SECOND) OF TORTS § 652B–E (AM. L. INST. 1977).

4 *See* Solove, *supra* note 1, at 1-22 (citing Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

5 *See id.* at 1-22 to 1-32.

6 DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1 (2008). *See also generally* Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087 (2002) [hereinafter *Conceptualizing Privacy*]; Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2005) [hereinafter *A Taxonomy of Privacy*].

7 *Id.*

8 ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).

9 Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968) (emphasis in original).

own."[10] Some of these theories defined privacy in service of autonomy.[11] Others characterized privacy through its service of intimacy or dignity.[12]

But it turns out that a broad and singular conceptualization of privacy is unhelpful for legal purposes. It guides lawmakers toward vague, overinclusive, and underinclusive rules.[13] It allows industry to appear to serve a limited notion of privacy while leaving people vulnerable when companies and people threaten notions of privacy that fall outside the narrow definition.[14] And it often causes people who discuss privacy in social and political settings to talk past each other because they don't share the same notion of privacy.[15]

The chaos and futility of competing conceptualizations of privacy is why Daniel Solove's research on privacy has been so important and influential for our modern privacy predicament. In an ongoing series of articles and books starting in 2001, Solove worked to reshape the entire narrative around privacy by suggesting that we stop obsessing over what privacy is and start asking what privacy is for.[16] To Solove, there is no singular common

---

[10] Ernest Van Den Haag, *On Privacy*, *in* PRIVACY 149, 149 (J. Roland Pennock & John W. Chapman eds., 1971) (emphasis added).

[11] *See* SOLOVE, *supra* note 6, at 18, 20 (citing Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 423, 426, 433 (1980)).

[12] *See id.* at 29–32, 34–37.

[13] *See Conceptualizing Privacy*, *supra* note 6, at 1089–90, 1146–47; *cf.* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, B.U. L. REV. (forthcoming 2022) [hereinafter *Privacy Harms*] (manuscript at 6, 16) (on file with author); Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 743–44, 756–73 (2018) [hereinafter *Risk and Anxiety*] (describing why courts have struggled to recognize privacy and security breaches as having caused harm). *See generally A Taxonomy of Privacy*, *supra* note 6.

[14] *See* JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 48–57 (2019) (identifying the collection and processing of personal data as resource extraction and management of populations). *See generally* ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER (forthcoming 2021) (arguing that the information industry manipulates discourse, compliance, and design to its favor).

[15] *See* Daniel J. Solove, *'I've Got Nothing to Hide' and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 757 (2007).

[16] Compelling pieces on this question have been written. *See generally, e.g.*, Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904 (2013); DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY (2011) [hereinafter NOTHING TO HIDE]; DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004) [hereinafter THE DIGITAL PERSON]; Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967 (2003). *See also, e.g.*, JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 151 (2012); DANIELLE KEATS CITRON,

denominator of privacy. Scholars seeking it are destined to spin their wheels for eternity. "Privacy is not one thing," Solove wrote, "but a cluster of many distinct yet related things."[17] Taking inspiration from Ludwig Wittgenstein's concept of family resemblances, Solove argued that privacy is best thought of as an umbrella term that brings together a group of concepts that "draw from a common pool of similar characteristics."[18]

Solove's work in privacy has been extraordinarily influential for scholars, policymakers, and practitioners.[19] His works are regularly invoked to counter the argument that privacy is important only to people with "something to hide."[20] Solove's response is that privacy isn't just about hiding things.[21] Solove keenly understands the central role that narratives and stories play in our understanding of privacy. He presciently argued that the modern privacy predicament involving industry's large-scale data processing efforts is more akin to Josef K.'s byzantine bureaucratic nightmare described by Franz Kafka in *The Trial* than the dystopian universal surveillance described by George Orwell in *Nineteen Eighty-Four*.[22] Solove argued that automated systems fueled by personal data don't just power surveillance tools. These tools power systems that make decisions about people's personal lives.

EXPLOITED: INSIDE THE FIGHT FOR INTIMATE PRIVACY (forthcoming 2022); NEIL RICHARDS, WHY PRIVACY MATTERS (forthcoming 2021).

17 SOLOVE, *supra* note 6, at 40.

18 *Id.* at 42 (citing LUDWIG WITTGENSTEIN, PHILOSOPHICAL INVESTIGATIONS (1953)). *But see* M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1139–42 (2011) (acknowledging the wisdom of Solove's approach but arguing that it lacks a limiting principle or rule of recognition).

19 Solove's scholarly impact is remarkable. He is the author of over ten books and textbooks, over fifty scholarly articles, and regularly writes op-eds, magazine articles, and blog posts for the public. His work has won numerous awards and has been translated into multiple languages. He has been cited or discussed in at least 2,700 publications, excerpted in many casebooks, and discussed in many judicial opinions, including those by the U.S. Supreme Court. He was coreporter of the American Law Institute's *Principles of the Law, Data Privacy* from 2013–19 and is cochair of the Privacy Law Scholars Conference, the most important academic privacy law conference in the United States. He is one of the most downloaded law scholars on SSRN, ranking in the top ten among tens of thousands of authors.

20 *See, e.g.*, Mystica M. Alexander & William P. Wiggins, *A Domestic Consequence of the Government Spying on Its Citizens: The Guilty Go Free*, 81 BROOK. L. REV. 627, 668 (2016).

21 *See* NOTHING TO HIDE, *supra* note 16, at 26–29; Solove, *supra* note 15, at 764–72.

22 *See* THE DIGITAL PERSON, *supra* note 16, at 27–55; Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1413–23 (2001).

They control and obscure, leaving people frustrated and vulnerable.[23] Much of Solove's work, such as my collaborations with him regarding the Federal Trade Commission's regulation and enforcement of privacy, aims to make sense of tumultuous areas involving the law of personal information.[24]

Perhaps most importantly, Solove's work provides a structure that frees scholars and lawmakers of the burden of finding one, singular notion of privacy to rule them all. He also helped shepherd in the algorithmic turn in privacy scholarship, which opened the door for discussions of how privacy issues impact marginalized and vulnerable populations.[25] There are many virtues to understanding privacy as a pluralistic, fluid concept. Such an ideal furthers diverse values and is capable of having both intrinsic and utilitarian worth and coexisting with many different policy goals. Under this notion, people in politics, commerce, and society can work to solve complex information problems without constantly relitigating privacy's meaning.

Instead of squabbling over the binary boundaries of privacy, people who understand privacy as more of a vague umbrella term can leave the line-drawing question for another day and get to work identifying problems created by specific conduct, articulating the values implicated by those problems, and crafting solutions to the problems that serve those values.[26] Starting in the late 1990s, Solove,[27] along with other pioneering scholars such as

---

[23] *See* Solove, *supra* note 22, at 1421.

[24] *See generally, e.g.*, Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014); Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230 (2015); Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814 (2011); Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CALIF. L. REV. 877 (2014).

[25] *See generally, e.g.*, SAFIYA UMOJA NOBLE, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM (2018); VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR (2018); DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (2014); SCOTT SKINNER-THOMPSON, PRIVACY AT THE MARGINS (2021).

[26] For example, Neil Richards has proposed a "provisional" definition of privacy as "the degree to which human information is neither known nor used," which allows people to simply get on the same page about what is being discussed then get to the real work of constructing information rules. RICHARDS, *supra* note 16, at 16. *But see* Calo, *supra* note 18, at 1135–42 (defending "the project of" describing the boundaries of privacy harm and contending that Solove's conception of privacy is better characterized as a "broader societal concern").

[27] *See generally, e.g.*, THE DIGITAL PERSON, *supra* note 16; Solove, *supra* note 22.

Anita Allen,[28] Danielle Citron,[29] Julie Cohen,[30] Helen Nissenbaum,[31] Neil Richards,[32] Joel Reidenberg,[33] Paul Schwartz,[34] and others[35]—responded to the late-century ossification of privacy law with new insights for a world gone digital. They arrived not a moment too soon.

The world has never seen anything like the power held and used by modern technology companies. It has never been easier to surveil people and collect, store, search, analyze, and share their personal information. The fair information practices (FIPs), a set of principles developed in response to the risks created by electronic databases, are not enough to meet the moment.[36] Reg-

---

[28] *See generally, e.g.*, Anita L. Allen, *Gender and Privacy in Cyberspace*, 52 STAN. L. REV. 1175 (2000); ANITA L. ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? (2011).

[29] *See generally, e.g.*, CITRON, , *supra* note 25; CITRON, *supra* note 16; Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870 (2019) [hereinafter *Sexual Privacy*]; Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61 (2009) [hereinafter *Cyber Civil Rights*]; Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008) [hereinafter *Technological Due Process*].

[30] *See generally, e.g.*, Cohen, *supra* note 16; Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure*, 75 U. CHI. L. REV. 181 (2008); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000). *See also* COHEN, *supra* note 16, at 107–52.

[31] *See generally, e.g.*, HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010).

[32] *See generally, e.g.*, NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE (2015); RICHARDS, *supra* note 16; Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013) [hereinafter *The Dangers of Surveillance*]; Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149 (2005).

[33] *See generally, e.g.*, Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877 (2003).

[34] *See generally, e.g.*, Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 HARV. L. REV. 2055 (2004); Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815 (2000); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999) [hereinafter *Privacy and Democracy*]; Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1 (1997).

[35] *See generally, e.g.*, PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY (1995); A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461 (2000); Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919 (2005); Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595 (2004); Peter P. Swire, *The Surprising Virtues of the New Financial Privacy Law*, 86 MINN. L. REV. 1263 (2002); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005). *See also* Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1344, 1347–48 (2004).

[36] *See* Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 964–76 (2017) (explaining why the FIPs are inadequate); Woodrow

ulatory manifestations of the FIPs such as the European Union's General Data Protection Regulation (GDPR),[37] Canada's Personal Information Protection and Electronic Documents Act (PIPEDA),[38] and California's Consumer Privacy Act (CCPA)[39] seek transparency and accountability from companies and control for people over their own data. They are the closest thing the world has to a "common language for privacy."[40]

Most of our modern data privacy rules, however, are built to serve individualistic notions of privacy—that is, to respect a person's autonomy and dignity. Few are aimed at disrupting power disparities between people and companies,[41] protecting individuals from harassment[42] and manipulation,[43] or seeking a collective

---

Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1721–37 (2020) (same). The FIPs originated in the 1970s from a series of meetings of the U.S. Department of Health, Education, and Welfare Secretary's Advisory Committee on Automated Personal Data Systems and were made internationally influential by revised adoption and implementation by the Organization for Economic Cooperation and Development. Robert Gellman, Fair Information Practices: A Basic History 1–5, 10–11 (Jan. 26, 2021) (unpublished manuscript) (on file with author); Chris Jay Hoofnagle, *The Origin of Fair Information Practices: Archive of the Meetings of the Secretary's Advisory Committee on Automated Personal Data Systems (SACAPDS)* (2014), https://perma.cc/38RP-NPHC.

37 *See* Council Regulation 2016/679, 2016 O.J. (L 119) 2.

38 S.C. 2000, c 5 (Can.).

39 CAL. CIV. CODE § 1798.100 (West 2021).

40 *See* Paula Bruening, *Fair Information Practice Principles: A Common Language of Privacy in a Diverse Data Environment*, INTEL (Jan. 28, 2016), https://perma.cc/Q4K3-4MK9.

41 *See, e.g.*, Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 135–38 (2007); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 441–47 (2016) (criticizing U.S. privacy law's fixation on harm avoidance and its assumption that people can control their disclosure of information); Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review*, 126 YALE L.J. 1180, 1183–86 (2017) (book review) [hereinafter *Privacy's Trust Gap*] (critiquing the individualistic conception of privacy as insufficiently protective); Neil M. Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. (forthcoming 2022) (manuscript at 8–19, 42–49) (on file with author) [hereinafter *A Duty of Loyalty*] (explaining how companies sort and manipulate data in self-serving ways and that dominant approaches to privacy law overlook these dynamics).

42 *See generally* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET (2007) (arguing that the American system of defamation and privacy torts does not effectively address reputation harms because lawsuits reveal the victim's identity and often target pocketless bloggers); CITRON, *supra* note 25 (arguing that cyber harassment victims may seek redress through three avenues—tort law, criminal law, and civil rights law—but lamenting shortcomings of the first two and underenforcement of the third).

43 *See, e.g.*, WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 34–43 (2018) (explaining how digital design choices

wellbeing for a diverse population in which many people, including women, people of color, members of the LGBTQ+ community, and others, are particularly vulnerable to information systems.[44] If lawmakers were tied to the notion of privacy as control over personal information, they might struggle to diagnose the problem as anything beyond a lack of adherence to fair information practices. Regulators might just engage in extreme FIPs enforcement in the hope that the companies will eventually reach full transparency and that people will have full command over how their data is processed.[45] Companies would go along because the FIPs do little to interfere with business models built around exploiting data.[46]

Transparency, consent, and control solutions won't be enough to get us out of this mess. First, as Solove has noted, the "privacy self-management" approach embodied by notice and choice regimes puts the onus on individuals to protect themselves.[47] But the massive scale and widespread adoption of digital technology have made meaningful informational self-determination impossible. People are simply overwhelmed by the choices presented to them. The result is a threadbare accountability framework that launders risk by foisting it on people who have no practical alternative to clicking the "I Agree" button. Second, consent and control are a poor fit for certain information problems, like manipulation and harassment, that have little to do with how information is processed and more to do with how mediated environments put people at risk.[48] Finally, seeking to give people control over their personal information doesn't account for collective, societal harms from personal information technologies. Privacy

distort users' privacy perceptions); Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1027–31 (2014) (explaining how digital market manipulation creates both subjective and objective harms).

44 *See generally, e.g.*, NOBLE, *supra* note 25; EUBANKS, *supra* note 25; CITRON, *supra* note 25; SKINNER-THOMPSON, *supra* note 25; Ari Ezra Waldman, *Safe Social Spaces*, 96 WASH. U. L. REV. 1537 (2019).

45 *See* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1881–82, 1903 (2013); Woodrow Hartzog, *The Case Against Idealising Control*, 4 EURO. DATA PROT. L. REV. 423, 425–26 (2018); Hartzog, *supra* note 36, at 972–76; Schwartz, *Privacy and Democracy in Cyberspace*, *supra* note 34, at 1632, 1637–39; Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1463, 1487 (2019).

46 *See* COHEN, *supra* note 14, at 41; WALDMAN, *supra* note 14 (manuscript at 16) (on file with author).

47 *See* Solove, *supra* note 45, at 1882–93.

48 *See* SOLOVE, *supra* note 42, at 184–87.

exists for groups and communities, too.[49] Your data can put other people at risk in ways that are hard to predict.[50] We're going to need richer, more diverse notions of privacy to solve these problems.

Thankfully, people have been hard at work converting privacy from a blunt tool into a Swiss Army knife, with each prong in service of a different value or purpose. Scholars have proposed a remarkable array of ways to think and talk about different notions of privacy, including intellectual privacy,[51] sexual privacy,[52] quantitative privacy,[53] and more. They have built out conceptualizations of privacy as obscurity,[54] trust,[55] power,[56] privilege,[57] security,[58] safety,[59] procedural due process,[60] a civil or human right,[61]

---

[49] *See, e.g.*, Evan Selinger & Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 LOYOLA L. REV. 33, 50–51 (2020) (arguing that even if individuals could consent to facial recognition technology, it would lead to "unacceptable harm to our collective autonomy").

[50] *See generally, e.g.*, Salomé Viljoen, *Democratic Data: A Relational Theory for Data Governance*, 131 YALE L.J. (forthcoming 2021) (noting data's use for population-level insights). *See also* Solon Barocas & Karen Levy, *Privacy Dependencies*, 95 WASH. L. REV. 555, 558 (2020).

[51] *See generally, e.g.*, RICHARDS, *supra* note 32.

[52] *See generally, e.g.*, *Sexual Privacy*, *supra* note 29.

[53] *See generally, e.g.*, David C. Gray & Danielle Keats Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013).

[54] *See generally, e.g.*, Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1 (2013); Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 WASH. L. REV. 385 (2013); Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343 (2015); HARTZOG, *supra* note 43.

[55] *See A Duty of Loyalty*, *supra* note 41, at 9–10, 19–23, 29–30 (proposing a duty of loyalty framework based on trust principles); HARTZOG, *supra* note 43, at 97–107. *See generally, e.g.*, Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69 U. MIAMI L. REV. 559 (2015); ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE (2018); Richards & Hartzog, *Taking Trust Seriously*, *supra* note 41; *Privacy's Trust Gap, supra* note 41.

[56] *See generally, e.g.*, Lisa M. Austin, *Enough About Me: Why Privacy Is About Power, Not Consent (or Harm)*, *in* A WORLD WITHOUT PRIVACY: WHAT LAW CAN AND SHOULD DO? 131 (Austin Sarat ed., 2015); CARISSA VÉLIZ, PRIVACY IS POWER: WHY AND HOW YOU SHOULD TAKE BACK CONTROL OF YOUR DATA (2020).

[57] *See generally, e.g.*, Rebecca Wexler, *Privacy as Privilege: The Stored Communications Act and Internet Evidence*, 134 HARV. L. REV. 2721 (2021).

[58] *See generally, e.g.*, Charles D. Raab, *Privacy as a Security Value*, *in* JON BING: EN HYLLEST [A TRIBUTE] 39 (Dag Wiese Schartum, Lee A. Bygrave & Anne Gunn Berge Bekken eds., 2014).

[59] *See generally, e.g.*, A. Michael Froomkin & Zak Colangelo, *Privacy as Safety*, 95 WASH. L. REV. 141 (2020).

[60] *See generally, e.g.*, *Technological Due Process*, *supra* note 29.

[61] *See generally, e.g.*, *Cyber Civil Rights*, *supra* note 29; Alvaro M. Bedoya, *Privacy as Civil Right*, 50 N.M. L. REV. 301 (2020).

and the contextual integrity of information flows.[62] They have argued that privacy protects democracy,[63] "the processes of play and experimentation,"[64] identity,[65] the incomputable self,[66] and significantly more. When lawmakers and judges accept privacy as a concept that contains multitudes, each of these different notions can explicitly be brought to bear on the real needs of people, groups, and institutions rather than deploying an ill-fitting theory in diverse contexts.

Lawmakers have started to embrace privacy as a concept with multiple overlapping dimensions. Legislators and regulators have begun to target problems such as nonconsensual pornography,[67] microtargeting,[68] manipulative user interfaces,[69] and automated decision-making[70] with innovative rules leveraging secondary liability for dangerous and abusive design choices,[71] substantive limits on data collection and use,[72] relational duties of loyalty and care,[73] equitable relief,[74] and criminal penalties[75] in

---

62 *See* NISSENBAUM, *supra* note 31, at 127–28. *See generally* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004).

63 *See* Cohen, *supra* note 16, at 1912–18; *Privacy and Democracy*, *supra* note 34, 1647–66.

64 *See* Cohen, *supra* note 16, at 1906.

65 *See* Mireille Hildebrandt, *Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning*, 20 THEORETICAL INQUIRIES IN L. 83, 87–91 (2019) (arguing for a "relational concept of privacy and the fundamental indeterminacy of human identity that it implies"). *See also generally* Bart van der Sloot, *Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"*, 31 UTRECHT J. INT'L & EUR. L. 25 (2015); Paul M. Schwartz & Karl-Nikolaus Peifer, *Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?*, 98 CALIF. L. REV. 1925 (2010).

66 *See* Hildebrandt, *supra* note 65, at 91–96.

67 *See, e.g.*, *46 States + DC + One Territory Now Have Revenge Porn Laws*, CYBER C.R. INITIATIVE, https://perma.cc/7AV6-VW89.

68 *See, e.g.*, Kate Cox, *Proposed Bill Would Ban Microtargeting of Political Advertisements*, ARS TECHNICA (May 26, 2020), https://perma.cc/GF3N-QUUP.

69 *See, e.g.*, Sean Kellogg, *How US, EU Approach Regulating 'Dark Patterns'*, INT'L ASS'N OF PRIV. PROS. (Dec. 1, 2020), https://perma.cc/6NFQ-BADA.

70 *See, e.g.*, Gissela Moya, *Algorithmic Racial and Gender Bias Is Real. The California State Legislature Must Act*, SACRAMENTO BEE (Jan. 13, 2021), https://www.sacbee.com/opinion/op-ed/article248316280.html.

71 Kellogg, *supra* note 69.

72 *See, e.g.*, Natasha Lomas, *FTC Settlement with Ever Orders Data and AIs Deleted After Facial Recognition Pivot*, TECHCRUNCH (Jan. 12, 2021), https://perma.cc/3VBJ-NXLG.

73 *See, e.g.*, Data Care Act of 2019, S. 2961, 116th Cong. § 3 (2019).

74 *See, e.g.*, Consumer Online Privacy Rights Act, S. 2968, 116th Cong. § 301(c)(2)(D) (2019).

75 *See 46 States*, *supra* note 67.

addition to implementing outright bans on particular technologies.[76]

Judges are also evolving in their thinking about privacy. For years, courts have struggled mightily trying to figure out what it means to have a "reasonable expectation of privacy."[77] Too often, that translates to things not exposed to others. But that has changed a little recently, as in *Carpenter v. United States*,[78] in which a majority of the U.S. Supreme Court conceived of privacy as dependent upon several different factors such as the scope of exposure and the nature of the information.[79]

By getting us past the threshold question of what privacy is, Solove's work provides room for scholars and lawmakers to tackle bigger phenomena, such as how capitalistic incentives cause companies to leverage information in harmful ways,[80] how the design of information technologies matters just as much as data practices,[81] and how marginalized populations are affected first and hardest by privacy-invasive actors.[82] Solove is a pragmatist, and, as such, his work consciously looks at the nature of privacy-related problems.[83] This focus also helps elevate the importance of scholarship aimed at the last legal mile of privacy solutions: how privacy harms are mitigated through legislation, regulation,

---

76 *See* Tom Simonite, *Portland's Face-Recognition Ban Is a New Twist on 'Smart Cities'*, WIRED (Sept. 21, 2020), https://perma.cc/G3J5-U67U.

77 Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring); *see, e.g.*, Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1519–27 (2010); Matthew Tokson & Ari Ezra Waldman, *Social Norms in Fourth Amendment Law*, MICH. L. REV. (forthcoming 2021) (manuscript at 12–16) (on file with author); Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 505–06 (2007); Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 122–23 (2002). *But see* Matthew Tokson, *The Emerging Principles of Fourth Amendment Privacy*, 88 GEO. WASH. L. REV. 1, 27–31 (2020) (arguing that despite the absence of an explicitly articulated framework, the Court consistently applies the same principles in its Fourth Amendment cases).

78 138 S. Ct. 2206 (2018).

79 *See id.* at 2213–20. Justice Neil Gorsuch's dissent even conceptualized privacy in the context of location-revealing data as a kind of bailment, a relational protection rather than one based upon the status of information. *See id.* at 2268–70 (Gorsuch, J., dissenting).

80 *See generally, e.g.*, COHEN, *supra* note 14; Amy Kapczynski, *The Law of Informational Capitalism*, 129 YALE L.J. 1460 (2020) (reviewing SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM; COHEN, *supra* note 14).

81 *See generally* HARTZOG, *supra* note 43.

82 *See generally, e.g.*, SKINNER-THOMPSON, *supra* note 25.

83 *See, e.g.*, Solove, *supra* note 77, at 1514.

and litigation.[84] Solove's own work with Danielle Citron on privacy and data security harms provides a map for judges and lawmakers to better articulate what harms result from bad information practices and which remedies are best to address those harms.[85]

The year is 2021, and privacy is still a concept in disarray. But that's okay. There is now too much data that is collected by too many different entities and used in too many different ways for any singular definition of privacy to be legally useful anyway. Daniel Solove's work on understanding privacy has imposed order upon chaos, shifting our focus away from questions about what privacy is and toward the different problems we want our privacy-based rules to address and the specific values we want them to serve.

---

[84] *See* Ignacio N. Cofone & Adriana Z. Robertson, *Privacy Harms*, 69 HASTINGS L.J. 1039, 1070–89 (2018) (arguing that understanding privacy as a continuum enables improving the third party doctrine); *Risk and Anxiety*, *supra* note 13, at 773, 780–85 (describing the potential for litigation to address harms associated with data breaches); *Privacy Harms*, *supra* note 13, at 50 (proposing a realignment of privacy enforcement and remedies through three specific enforcement rules).

[85] *See generally, e.g.*, *Risk and Anxiety*, *supra* note 13; *Privacy Harms*, *supra* note 13.