FOCUSING PRIVACY LAW

Paul Ohm†

ABSTRACT

If the United States ever enacts an omnibus privacy law akin to the European Union's General Data Protection Regulation, we might declare "mission accomplished." We should not be so quick to celebrate, as this alone would not solve enough of our manifest privacy problems. Given the dysfunctions of our technological, political, economic, and social institutions, any omnibus law this country would enact is likely to be watered down, managerial, and incomplete.

While we continue to pursue an elusive omnibus ideal, we should at the same time focus on enacting new and better focused privacy laws, such as laws that govern narrowly drawn categories of sensitive information or specific uses of information.

Enacting focused privacy laws will harness three great themes in how scholars conceptualize privacy, by centering harms, rights, and context. The great mistake of the omnibus era has been thinking we could write one law to properly account for information's contextual variation. It is better to enact rules and enforcement strategies tailored for each context.

Focused privacy laws also play to the strengths and address the weaknesses of our present-day, complex mix of governance institutions. Narrower laws place the onus on Congress to define rules clearly and in detail, freeing up agencies to prioritize enforcement. This will strengthen privacy protection in the face of attacks on agency authority and resources in recent years. State legislatures can enact focused privacy laws to serve as laboratories of privacy law experimentation, meaning any federal omnibus law should not preempt states from enacting them. Public choice theory suggests that debates over focused laws may inspire less corporate lobbying and other interest group politics that have watered down omnibus proposals.

Finally, focused privacy laws can be used to help us reshape and redesign our broken information economy. Laws that apply special rules for specific uses or categories of information compel firms to reshape their products, services, org charts, and internal operations around values-centric lines. These laws thus give people outside the firm a say in the design of these vital pieces of information infrastructure and can empower those inside the company who focus beyond the bottom line.

DOI: https://doi.org/10.15779/Z389P2W776

† Professor of Law, Georgetown University Law Center. For excellent research assistance, thanks to Andrea Dean and Patrick Yurky. For feedback, thanks to Lindsey Barrett, Kiel Brennan-Marquez, Alan Butler, Danielle Citron, Gautam Hans, Woody Hartzog, Meg Leta Jones, Laura Moy, Jon Penney, Catherine Powell, Neil Richards, Dan Solove, Amelia Vance, and Carly Zubrzycki. Thanks also to participants in the Privacy Law Scholars Conference and students in the Fordham Law "Civil Rights and Civil Liberties in the Digital Age" seminar.

TABLE OF CONTENTS

I. INTRODUCTION

Despite its best efforts, the U.S. Congress cannot seem to pass *omnibus* privacy legislation—meaning a law that would regulate almost all commercial actors and types of information—after more than a decade of false starts.[1] The latest disappointment was the failure of the American Privacy Rights Act (APRA),[2] the support for which fell apart in summer 2024 after a spring season of optimistic prognostication.[3] No doubt, the next Congress will try again, continuing to chase the elusive goal of establishing broad-based data protection for Americans, following the lead of the European Union[4] and countries around the globe,[5] as well as of nineteen states and counting.[6]

---

1. *E.g.*, American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022); Consumer Online Privacy Rights Act, S. 3195, 117th Cong. (2021); Online Privacy Act, H.R. 4978, 116th Cong., 1st Sess. (2020); Data Care Act, S. 3744, 115th Cong. (2018); Commercial Privacy Bill of Rights Act, S. 799, 112th Cong. (2011); *see also* Consumer Privacy Bill of Rights Act of 2015 (administration discussion draft), https:// obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

2. Press Release, U.S. Senate Committee on Commerce, Science, and Transportation, Committee Chairs Cantwell, McMorris Rodgers Unveil Historic Draft Comprehensive Data Privacy Legislation (Apr. 7, 2024), https://www.commerce.senate.gov/2024/4/committee-chairs-cantwell-mcmorris-rodgers-unveil-historic-draft-comprehensive-data-privacy-legislation (describing American Privacy Rights Act or APRA).

3. Dell Cameron, *Surprise! The Latest 'Comprehensive' US Privacy Bill Is Doomed*, WIRED (June 27, 2024), https://www.wired.com/story/apra-privacy-bill-doomed/.

4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) [hereinafter GDPR].

5. *See, e.g.*, Brazil's General Data Protection Law (Lei Geral de Proteção de Dados Pessoais, LGPD), Lei No. 13.709, de 14 de Agosto de 2018, Diário Oficial da União [D.O.U.] de 15.08.2018 (Braz.); Data Protection Act No. (37) (2023) 110:119 O.G., A719–758 (Nigeria) (both heavily inspired by the GDPR); *see also*, *Global Privacy Law and DPA Directory*, INT'L ASS'N OF PRIV. PROS. (last visited Mar. 13, 2025), https://iapp.org/resources/global-privacy-directory/ (listing privacy laws around the world).

6. *See, e.g.*, California Consumer Privacy Act, CAL. CIV. CODE § 1798.105 (2011); Connecticut Data Privacy Act, 2022 Conn. Legis. Serv. Pub. Act No. 22-15 (Senate Bill No. 6) § 3; Colorado Privacy Act, COLO. REV. STAT. § 6-1-1301. For a list of state omnibus privacy laws, see C Kibby, *US State Privacy Legislation Tracker*, INT'L ASS'N OF PRIV. PROS. (last updated

Enacting a federal omnibus privacy protection law would be an important step, but it would not be enough. No omnibus law alone can address the dysfunctional system of surveillance capitalism we have created.[7] The better way to shore up privacy protection is by writing narrower and much more focused privacy laws. This goes against the widely held belief among advocates, policymakers, and scholars that omnibus privacy laws are better.[8]

There are at least three ways to focus a privacy law. A *sectoral* privacy law regulates the information processed by companies in a particular industry sector. The U.S. Congress has been enacting sectoral privacy laws for decades, including laws covering the health care,[9] banking,[10] and education[11] sectors.

Mar. 10, 2025), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/#enacted-laws.

7. SHOSHANNA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 7–8 (2019).

8. Privacy advocacy groups broadly advocate for omnibus—or "comprehensive"—privacy law. *See Hearing on Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy Before the Subcomm. on Innovation, Data & Com., of the H. Comm. on Energy & Com.*, 118th Cong. (Mar. 1, 2023) (statement of Alexandra Reeve Givens, President & CEO, Center for Democracy and Technology) (calling for federal comprehensive privacy law); *Hearing on Safeguarding Americans' Communications: Strengthening Cybersecurity in a Digital Era Before the Subcomm. on Commc'n & Tech., of the H. Comm. On Energy & Com.*, 118th Cong. (Jan. 11, 2024) (statement of Alan Butler, Executive Director, Electronic Privacy Information Center) (calling for federal comprehensive privacy law); *Consumer Privacy in the United States*, PUBLIC KNOWLEDGE (last visited Mar. 13, 2025), https://publicknowledge.org/consumer-privacy-in-the-united-states/ ("We support a comprehensive federal privacy law that allows for states to expand on those baseline protections and ensures a private right of action so that consumers can act when others cannot on their behalf.").

Policymakers from both political parties have similarly argued for the omnibus approach. *See supra* note 1 for bills.

Scholars have also noted the incomplete coverage of the sectoral approach and suggested omnibus privacy laws instead. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 587 (2014) ("The sectoral approach also leaves large areas unregulated, especially at the federal level."); Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 904 (2009); Rory Van Loo, *Privacy Pretexts*, 108 CORNELL L. REV. 1, 57 (2022) (noting that experts in the field of privacy have long proposed omnibus privacy legislation); Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 259 (2011) ("Scholars and advocates have been joined by industry leaders and politicians in support of passage of omnibus legislation requiring the adoption of FIPPs generally").

9. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 262, 110 Stat. 2023 (1996) (applicability provision codified at 42 U.S.C. § 1320d-1) (setting healthcare administration standards for "health plans," "health care clearinghouses," and "health care providers").

10. Gramm-Leach-Bliley Act (GLBA), Pub. L. No. 106-102 (1999) (relevant portions codified at 15 U.S.C. § 6801) (creating obligations for all "financial institutions").

11. Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g (2018) (covering any public or private "educational institution or agency").

Sectoral laws have been rightly criticized for embracing an outdated model of how information flows in the economy, one which fails to account for how categories and uses of information are no longer cabined within industry silos.[12]

To improve on both omnibus and sectoral laws, this Article advocates for two newer approaches to writing focused privacy laws. A *sensitivity-focused* privacy law sets special processing rules for a particular category of information, such as health information,[13] biometric information,[14] or information about children,[15] regardless who processes it.[16] A notable sensitivity-focused privacy law is Illinois's Biometric Information Privacy Act (BIPA) which protects biometric identifiers such as faceprints or fingerprints.[17] A *use-focused* law governs particular uses of information.[18] Colorado's new Artificial Intelligence Act, for example, imposes a duty on developers and deployers of "high risk AI systems" to protect people from algorithmic discrimination.[19]

This Article argues that new sensitivity-focused and use-focused laws will lead to better privacy results than any omnibus alternative. This is a practical

12. *See* Helen Nissenbaum, Katherine Strandburg & Salomé Viljoen, *The Great Regulatory Dodge*, 37 HARV. J.L. & TECH. 1231, 1238–39 (2023); Schwartz, *supra* note 8, at 923.

13. *See* Washington My Health My Data Act, WASH. REV. CODE § 19.373.005 (2023) ("Information related to an individual's health conditions or attempts to obtain health care services is among the most personal and sensitive categories of data collected . . . [this act provides] stronger privacy protections for all Washington consumers' health data.").

14. *See* Illinois Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. 14/5 (2008) ("Biometrics are unlike other unique identifiers . . . The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.").

15. *See* Children's Online Privacy Protection Act (COPPA), 15 U.S.C. § 6502(a) (2018) (regulating the collection and use of personal information from children under 13).

16. Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1133–35 (2015) (defining "sensitive information" and describing laws that focus on sensitive information).

17. BIPA, 740 ILL. COMP. STAT. 14/5 (2008).

18. Daniel J. Solove, *Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data*, 118 NW. U. L. REV. 1081, 1133 (2024) ("[T]he focus should not be on *data*, but instead about harmful or risky *uses of data*.") (emphases in original).

19. Colorado Artificial Intelligence Act, COLO. REV. STAT. §§ 6-1-1702(1), 1702(2). A debate is brewing about whether laws like this one qualify as a privacy law. *Compare* María P. Angel & Ryan Calo, *Distinguishing Privacy Law: A Critique of Privacy as Social Taxonomy*, 124 COLUM. L. REV. 507, 560 (2024) (arguing that "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.'") *with* Daniel J. Solove, *Against Privacy Essentialism* (Geo. Wash. U., Draft Research Paper 2025-19), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4826385 (arguing that "algorithmic manipulation and information-based discrimination . . . are not entirely privacy problems, but they have important privacy dimensions."). That interesting debate is outside the scope of this Article.

and grounded conclusion based not on theoretical ideal laws for an ideal society but instead based on what is needed in the flawed and messy political, technological, economic, and social world we inhabit.[20] Given our starting point, tackling privacy issues one use or sensitive category at a time is far likelier to lead to tailored, meaningful, and lasting privacy protections than continuing to chase an elusive omnibus ideal.[21]

I offer three sets of arguments for why focused privacy laws will lead to better, more meaningful, more tailored privacy laws than the omnibus *status quo*. Call these the *harm reduction, institution selection, and design intervention* arguments, which are elaborated, respectively, in Parts III, IV, and V. These draw on a diverse set of interdisciplinary insights, borrowing from the public choice theory of economics and political science, the values-in-design approach from Science and Technology Studies (STS), and the New Institutional theory of organizational sociology to name only three.

According to the harm reduction argument, offered in Part III, narrow privacy laws advance three great themes in the way we conceptualize information privacy itself, by tailoring legislative protections to harms, rights, and context. Some of the most important, insistent, and thoughtful scholarly writing about privacy of the past two decades has documented the specific and tailored *harms* of different privacy practices, for example, work on protecting intellectual privacy or intimate privacy.[22] Much of this work has placed information privacy in a *civil and human rights* frame.[23] All of this work connects to writing on the *contextual nature of information privacy*.[24]

20. *See* Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1715 (2020) ("[G]iven different systems, value commitments, and political realities, it seems likely that any version of a U.S. GDPR will, in effect, be a GDPR-lite.")

21. *See* ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER (2020); *see also* Schwartz, *supra* note 8, at 928–29.

22. *See generally* NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE (2015); DANIELLE CITRON, THE FIGHT FOR PRIVACY: PROTECTING DIGNITY, IDENTITY, AND LOVE IN THE DIGITAL AGE (2022); *see also* Ohm, *supra* note 16, at 1131 (connecting the category of "sensitive information" to threat models and information harms).

23. *See generally* Alvaro M. Bedoya, *Privacy as Civil Right*, 50 N.M. L. REV. 301, 306 (2020); CITRON, *supra* note 22; RICHARDS, *supra* note 22; Aziz Z. Huq & Rebecca Wexler, *Digital Privacy for Reproductive Choice in the Post-Roe Era*, 98 N.Y.U. L. REV. 555, 576–77 (2023).

24. *See generally* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2009).

The great mistake of the omnibus era has been to think we could write one law to properly account for all this variation.[25] The uniformity of an omnibus law has washed away all of the urgency and specificity of the scholarship on harms, rights, and context. We would do better to channel specific insights, individual issues, and tailored mechanisms each into its own specific privacy law.

Next, Part IV explains how focused privacy laws better harness the capabilities of our governance and political institutions. Omnibus laws delegate the details of decision-making from the legislature to administrative agencies, while focused privacy laws let the legislature exert more fine-grained control over the details, freeing agencies to focus on enforcing the laws. This reallocation of responsibility from agencies to legislatures aligns with three relative strengths and weaknesses of these institutions. First, legislatures are more politically accountable than agencies.[26] Second, agencies charged with privacy protection tend to be notoriously underfunded.[27] Third, the Supreme Court has been diminishing the power of agencies, most notably in a trio of cases from the most recent term.[28]

Narrower privacy laws can also activate state legislatures to be laboratories of privacy democracy. Just as Illinois has led on biometric privacy and Washington State is now leading on health data, with its 2023 My Health My Data Act, other states can experiment with the issues most important to their citizens.[29] To avoid disrupting this experimentation, any federal omnibus privacy law should expressly exempt state sensitivity-focused and use-focused privacy laws from preemption.[30]

---

25. Nissenbaum, Strandburg & Viljoen, *supra* note 12 ("A one-size-fits-all omnibus approach is insufficient, however, to capture privacy's contextual variability, which is keyed not to individual preferences and 'consent' but to disparate social spheres.").

26. *But see* Anya Bernstein & Cristina Rodríguez, *The Accountable Bureaucrat*, 132 YALE L.J. 1600, 1604 (2023) (identifying various mechanisms that increase the accountability of administrators).

27. *See* Justin Sherman, *The Key to Protecting Privacy Is Locked in an Underfunded Government Agency*, SLATE (July 14, 2023), https://slate.com/technology/2023/07/federal-trade-commission-funding-privacy.html (noting that the FTC's "Division of Privacy and Identity Protection has only 40 to 45 employees).

28. *See* Loper Bright Enters. v. Raimondo, 603 U.S. 369 (2024) (overturning Chevron Inc. v. Natural Resources Defense Council, Inc., 467 U. S. 837 (1984)); Corner Post, Inc. v. Bd. of Governors of Fed. Rsrv. Sys., 603 U.S. 799 (2024) (expanding time to challenge agency action); Sec. & Exch. Comm'n v. Jarkesy, 603 U.S. 109 (2024) (narrowing SEC's ability to use administrative law judges).

29. BIPA, 740 ILL. COMP. STAT. 14/5 (2008); Washington My Health My Data Act, WASH. H.B. 1155 (enacted April 27, 2023).

30. *See generally* Schwartz, *supra* note 8, at 904 (arguing against federal preemption of state privacy law).

Public choice theory, and particularly the study of the power of interest groups, adds one last institutional argument in support of focused privacy laws. Every new omnibus privacy law affects every data holder, by definition.[31] This turns the debate over an omnibus privacy law into a broad, whole-of-economy, battle royale: one that sparks an arms race of persuasion and lobbying, with the spoils going to those with the most to invest.[32] Meanwhile, the breadth of these debates can sideline civil society organizations that see neither privacy nor data, writ large, as their causes.

A debate over a focused privacy law improves these political dynamics. Many smaller groups would be activated by narrower debates on the privacy of minority communities, reproductive health privacy, or police surveillance, say, and the narrower debates might similarly encourage more participation by average citizens. Those choosing to participate in the debate are likely to have more expertise about a particular context or category of harm, and they will be negotiating with fewer counterparties.

The third set of arguments, offered in Part V, explain how focused privacy laws can be used as tools to begin to reshape our flawed information economy. Scholarship in New Institutionalism and other areas of organizational sociology explain how laws reshape firms and their products and services.[33] A focused privacy law can take advantage of these dynamics, spurring beneficial changes to technology companies and the apps and platforms they provide. These beneficial effects go beyond the law's direct effects and its limitations on the collection, use, or sharing of particular categories of information. Crafting a focused privacy law gives outsiders a voice in the design of vital infrastructural platforms.[34] These laws might, for example, slash *governance seams*—"socially constructed boundaries, borders, and interfaces" that serve as "loci of transparency, coordination, and oversight"—across a company's

31. *See, e.g.*, Regulation (EU) 2016/679, General Data Protection Regulation, 2016 O.J. (L 119); cor. 2018 O.J. Art. 45 (L 127) Art. 4, at 33 (covering "any information relating to an identified or identifiable natural person"); California Consumer Privacy Act (CCPA), CAL. CIV. CODE § 1798.140 (2024) (covering any "natural person who is a California resident").

32. Ari Waldman, *Civil Society and the Future of Privacy Law* (forthcoming 2024) (on file with author).

33. *See* Mark C. Suchman & Lauren B. Edelman, *Legal Rational Myths: The New Institutionalism and the Law and Society Tradition*, 21 L. & SOC. INQUIRY 903, 922–23 (1996); Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 806–10 (2020); Andrew D. Selbst, *An Institutional View of Algorithmic Impact Assessments*, 35 HARV. J.L. & TECH. 117, 191 (2021).

34. JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM (2019); WALDMAN, *supra* note 21, at 236.

products and services,[35] unlike an omnibus privacy law, which tends to leave such internal considerations out-of-scope and thus untouched.

A focused law might also change the internal organization chart of the firm, giving power and voice to those trained and predisposed to focus on specific harms, civil and human rights, threat models, and obligations, in the way that firms today end up with specialists such as ECPA nerds and HIPAA geeks.[36] Activating this corps of insiders charged with thinking about values imposed from the outside might address some of Ari Waldman's and Julie Cohen's concerns about managerialism.[37]

The Article proceeds in five parts. After briefly explaining the urgent need for new privacy laws, Part II describes recurring problems with our attempts to enact omnibus privacy laws and introduces several narrower alternative strategies. Parts III through V offer arguments in favor of focused privacy laws—respectively, harm reduction, institution selection, and design intervention. Finally, Part VI offers some practical considerations about the focused laws we ought to start enacting.

II. OMNIBUS AND FOCUSED PRIVACY LAWS

Our system of surveillance capitalism has led to concrete harms for individuals, groups, and society. It has contributed to the weakening of democratic, economic, and social systems. We need new privacy laws (along with other kinds of laws) to begin addressing these problems.

For decades, scholars and advocates have argued that we ought to replace outmoded sectoral privacy laws with superior omnibus ones.[38] This dichotomy has neglected a rich set of focused alternatives. To set the table for the arguments in favor of focusing privacy law, we first need to understand what makes each category different, and we need to review the shortcomings of the omnibus and sectoral approaches.

35. Brett Frischmann & Paul Ohm, *Governance Seams*, 37 HARV. J.L. & TECH. 1117 (2023). *See* FREDERICK BROOKS, THE MYTHICAL MAN-MONTH 111 (1975) (describing Conway's Law, which states that the design of a system reflects the communications structure of the organization that created it).

36. *See* Electronic Communications Privacy Act (ECPA), Pub. L. No. 99-508; Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936.

37. *See* WALDMAN, *supra* note 21, at 118; COHEN, *supra* note 34.

38. *See* Schwartz, *supra* note 8, at 904; Van Loo, *supra* note 8, at 57; Bamberger & Mulligan, *supra* note 8, at 306.

A. THE NEED FOR STRONGER PRIVACY LAWS

This Article starts from the proposition that we need to enact stronger and better privacy laws in this country. It builds upon a vast and growing literature that has come to this conclusion.[39] Rather than recite all the underlying arguments that have been made, I will survey them quickly.

Our information economy is built upon systems of pervasive surveillance.[40] Many companies, large and small, extract data from individuals, process that data into insights and inferences, and sell it all to advertisers, data brokers, and other third parties.[41]

Although this system of pervasive corporate surveillance has benefits for individual actors, the government, and (arguably) the economy,[42] it causes real and concrete harm. Harassers, stalkers, and creeps use digital platforms and databases to terrorize victims.[43] Cybercriminals and hostile nation-states steal and stockpile secrets about every person online. Corporate surveillance feeds government surveillance, leading to forms of unwelcome state interference with private life.[44] All of these harms tend to be unevenly distributed, meaning our information ecosystems tend to disproportionately injure vulnerable people including low-income individuals, children, the elderly, and people with disabilities.[45]

Information is power, and corporations and governments alike use the information they amass to control and manipulate people. People are coaxed to buy what they ought not buy, vote against their interests, go where they don't want to go, and do what they don't want to do.[46] Tech addiction and teen body image issues are national crises, fueled by the surveillance business models.[47]

---

39. *See, e.g.*, COHEN, *supra* note 34; RICHARDS, *supra* note 22; WALDMAN, *supra* note 21; CITRON, *supra* note 22; NISSENBAUM, *supra* note 24.

40. ZUBOFF, *supra* note 7.

41. *Id.*

42. Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J.L. & TECH. 1, 5–20 (2011) (extolling the beneficial applications of data in the "Data Commons").

43. CITRON, *supra* note 22.

44. *See* Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 115 (2018) (noting the potential for corporate surveillance to feed government surveillance but identifying incentives that occasionally cause corporations to resist).

45. Michele E. Gilman, *The Class Differential in Privacy Law*, 77 BROOK. L. REV. 1389, 1403–04 (2012).

46. BRETT FRISCHMANN & EVAN SELINGER, RE-ENGINEERING HUMANITY (2018).

47. DR. VIVEK H. MURTHY, U.S. SURGEON GENERAL, SOCIAL MEDIA AND YOUTH MENTAL HEALTH: THE U.S. SURGEON GENERAL'S ADVISORY (2023), https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf (summarizing studies

The system also leads to a host of structural and institutional problems.[48] The panoptic chill of possible surveillance changes what we read and research, which in turn changes what we ask of our political systems, limiting what we can accomplish democratically.[49] The network effects of information and social networks contribute to market concentration, creating massive platforms that shift power and wealth to a small, entrenched elite.[50] This concentration of wealth exacerbates economic inequality and precarity. Wealth protects itself, and the tech giants have rapidly become among the most profligate lobbyists in Washington.[51] Meanwhile, many of the United States trading partners have enacted comprehensive data protection laws that treat privacy as a fundamental right, potentially creating barriers to our ability to share data across our borders.[52]

All of these harms and structural problems are exacerbated by the algorithmic turn in society.[53] Powerful methods of inference convert seemingly benign data into sensitive intelligence about the behavior, movement, and

suggesting crises in tech addiction and body image and finding some connections to social media).

48. *See generally* COHEN, *supra* note 34.

49. RICHARDS, *supra* note 22; Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1912 (2013); *see generally* Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815 (2000).

50. TIM WU, THE CURSE OF BIGNESS (2018); MAURICE E. STUCKE, BREAKING AWAY: HOW TO REGAIN CONTROL OVER OUR DATA, PRIVACY, AND AUTONOMY (2022).

51. *See* Emily Birnbaum, *Tech Giants Broke Their Spending Records on Lobbying Last Year*, BLOOMBERG (Feb. 1, 2023), https://www.bloomberg.com/news/articles/2023-02-01/amazon-apple-microsoft-report-record-lobbying-spending-in-2022 ("In total, the top tech companies spent nearly $70 million on lobbying in 2022, outstripping other industries including pharmaceuticals and oil and gas."); *Ranked Sectors 2023*, OPEN SECRETS, https://www.opensecrets.org/federal-lobbying/ranked-sectors?cycle=2023 (last visited Mar. 13, 2025) (listing Communications/Electronics as third highest in total spending at $580 million spent in 2023, behind only Health and Finance).

52. For example, Article 45 of the GDPR requires a determination by the European Commission of the "adequacy" of the privacy or data protection law of a non-E.U. country before data controllers are permitted to transfer personal data to that country. Regulation (EU) 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) (EU); cor. 2018 O.J. Art. 45 (L 127). Two opinions of the Court of Justice for the European Union have deemed the United States' system of privacy law inadequate, including additional protections added during negotiations to try to establish adequacy. *See* Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. (Schrems II), ECLI:EU:C:2020:559 (July 16, 2020); Case C-362/14, Schrems v. Data Prot. Comm'r (Schrems I), ECLI:EU:C:2015:650, ¶ 216 (Oct. 6, 2015).

53. Ifeoma Ajunwa, *The Paradox of Automation as Anti-Bias Intervention*, 41 CARDOZO L. REV. 1671, 1683 (2020) (describing the algorithmic turn).

predilections of people.[54] Predictive algorithms decide who gets benefits,[55] who gets fired,[56] and who goes to prison.[57]

To be clear, privacy law is not the only area of law that can respond to these problems. We need to shore up other areas of law, including antitrust, consumer protection, labor and worker protection, tax, and many others. We may also need new, tailored legislation to address the problems raised by artificial intelligence.[58] But privacy laws—rules governing what information can be collected and how that information can flow and be used—is a bedrock foundation for any plan. Alas, the privacy and data protection laws we have enacted and considered to date have not been up to the challenge of responding to any of these problems.

B. OMNIBUS PRIVACY LAWS

The conventional wisdom has long held that the best information privacy laws are *omnibus*, meaning they regulate what all companies and governments can do with any information they hold about people.[59] The paradigmatic omnibus law is the European Union's General Data Protection Regulation (GDPR)[60] which covers all "personal information" processed by so-called "data controllers,"[61] and has given rise to imitators around the globe.[62] Omnibus privacy laws are considered to be undeniably superior to *sectoral* laws, laws that focus on particular types of information held by specific individual actors.[63] A quintessential sectoral privacy law is the U.S.'s Health Information Portability and Accountability Act (HIPAA) and its associated Privacy Rule,[64]

54. *See* Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U. L. REV. 357, 379 (2022).

55. VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR (2018); Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1260 (2008).

56. CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY (2016).

57. Julia Angwin, Jeff Larson, Surya Mattu & Lauren Kirchner, *Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

58. *E.g.*, Regulation (EU) 2024/1689 Artificial Intelligence Act 2024 O.J. (European Union AI Act).

59. *See supra* note 8.

60. GDPR, *supra* note 4.

61. *Id.*

62. *See, e.g.*, *supra* note 5.

63. *See supra* note 8.

64. HIPAA, Pub. L. No. 104-191, 110 Stat. 1936 (1996); 45 C.F.R. § 160.103 (2020).

which governs "protected health information" when held by defined "covered entities" and their "business associates."[65]

The mental model of the omnibus strategy is of a rising tide of data protection lifting all boats. It is a totalizing theory ramping up privacy protections across all industries and all kinds of data. It accounts for the variability in risk and harm in different contexts by postponing for later determination by the data controllers themselves of the risk of any particular data practice, perhaps second-guessed by government enforcers charged with spotting, investigating, and remedying the occasional harm that sneaks through.[66] This model seeks to balance potential harms against the beneficial uses to which data can be put, and it defers to companies in the first instance as the best decision-makers for which uses are most important.

Given the strength of the conventional wisdom on this issue, a focus on new omnibus laws has held center stage in jurisdictions around the world for many years. At the federal level in the United States, efforts to enact omnibus privacy or data protection law have been a primary focus for more than a decade. The most recent vehicle was the American Privacy Rights Act, or APRA, and as with all the examples that preceded it, it appears to have no chance of passage.[67] Despite increasing optimism, Congress has not managed to drag an omnibus law over the finish line. While Congress flounders, the states have begun enacting omnibus privacy laws of their own. Most prominently, California has enacted the California Consumer Privacy Act (CCPA), a complex and comprehensive law frequently compared to the GDPR.[68] As of this writing, nineteen states have enacted omnibus privacy laws, and even more are considering following suit.[69] Fearing the compliance burden of this emerging patchwork of privacy law, regulated entities have stepped up efforts to persuade Congress to enact a federal omnibus law, on the condition that it preempt all of these state laws.[70]

65. 45 C.F.R. § 164.502 ("A covered entity or business associate may not use or disclose protected health information").

66. *See* KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE (2015) (describing the role of privacy professionals in firms to determine the implementation of open-textured privacy laws); William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959, 985–988 (2016) (describing a "responsive regulation" approach to privacy law).

67. American Privacy Rights Act of 2024, H.R. 8818, 118th Cong. (2024).

68. CCPA, CAL. CIV. CODE § 1798.140 (2018).

69. Kibby, *supra* note 6.

70. Julia Angwin, *Federal Privacy Law Has Momentum, but There's a Catch*, THE MARKUP (July 30, 2022), https://themarkup.org/newsletter/hello-world/federal-privacy-law-has-momentum-but-theres-a-catch (interviewing Cam Kerry about the ADPPA, stating that "[t]he

C. THE PROBLEMS WITH OMNIBUS PRIVACY LAWS

Omnibus privacy laws provide useful backstops or default rules. We are better off with these laws than without them, and in jurisdictions that have yet to adopt them, it is worth the effort to try to enact them. In the United States, Congress should enact a law like the American Data Privacy and Protection Act (ADPPA), the omnibus bill that failed to pass in 2022,[71] without hesitation. But in the unlikely event it manages to do so, we must understand that omnibus laws provide only a floor of protection that must be supplemented with other laws.[72] In our flawed present politics, omnibus privacy laws flatten all information privacy concerns in ways that have led to several related problems.

To be clear, we should also continue to pursue better omnibus laws, but that means first tearing down and building back up our politics and our institutions.[73] In separate work, I am helping to engage in that effort,[74] but the changes needed will not happen quickly, if they happen at all. In the meantime, we can greatly advance the project of privacy protection by enacting narrower privacy laws.

1. The Underlying "Logic of Omnibus"

The core problem with the omnibus approach is its underlying logic—how it flattens a complex and diverse set of related and unrelated information privacy concerns into a single, unifying set of rules. All information is lumped together in a mostly aggregated mass of "personal data" or "personal information," subject to the same rules.[75] Many problems flow from this flattening.

---

political reality is that the federal preemption is part of the price of getting strong protections.").

71. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

72. *See* Nissenbaum, Strandburg & Viljoen, *supra* note 12, at 1262 ("An omnibus law could act as a gap-filler to sectoral laws. Many recent state privacy laws have this flavor, exempting at least some activities covered by sectoral privacy laws.").

73. *See* JULIE COHEN, *supra* note 34; WALDMAN, *supra* note 21, at 210–231.

74. *Redesigning the Governance Stack Project*, GEO. L. (last visited July 26, 2024), https://www.law.georgetown.edu/tech-institute/initiatives/redesigning-the-governance-stack-project/ ("The Redesigning the Governance Stack Project is working to reinvent the administrative state so that it is equipped to govern the information economy effectively and in a way that centers public values.").

75. Nissenbaum, Strandburg & Viljoen, *supra* note 12, at 1256 ("If sectoral privacy laws facilitate 'dodges,' perhaps we should prefer omnibus privacy regulation. But unless they provide standards for context-sensitive tailoring by judges and agencies, omnibus laws will amount to one-size-fits-all regimes, permitting contextually inappropriate information flows, erecting barriers to contextually appropriate flows, or both.").

An omnibus law's unified approach to regulating all kinds and uses of data is insufficiently sensitive to the great diversity of problems, harms, and solutions in information privacy.[76] Privacy is deeply contextual, so privacy law should attend to contextual problems.[77]

There are practical and institutional problems with treating all data and data uses alike. Doing so delegates the law's implementation, monitoring, and enforcement from Congress to agencies and, all too often, to the supposedly regulated companies themselves. With an omnibus law, since Congress doesn't prescribe the specific categories and uses of information being regulated or the rules for each, it defers to the expertise and experience of the administrative agencies. The agencies in turn have embraced "collaborative governance," further deferring to the regulated companies to interpret the rules in the first instance.[78] Besides, because the agencies have limited visibility into the information-handling practices of these companies, the first instance usually becomes the only instance, and collaborative governance becomes self-governance, or more to the point, no governance.

This ladder of deference and interpretation from Congress to agencies to companies is especially unwise given the challenges faced by agencies today, fueled by judicial and political attacks on the administrative state. Congress has long failed to provide the kind of resources to agencies charged with policing privacy law that other countries allocate.[79] The FTC, in particular, consistently complains about its lack of funding and staff to accomplish its mission.[80]

---

76. More than twenty-five years ago, Spiros Simitis argued that the omnibus approach "cannot deal in a clear and efficient manner with the problems resulting from the use of personal data." Spiros Simitis, *From the General Rules on Data Protection to a Specific Regulation of the Use of Employee Data: Policies and Constraints of the European Union*, 19 COMP. LAB. L. & POL'Y J. 351, 355 (1998).

77. NISSENBAUM, *supra* note 24, at 127–28 (describing the contextual nature of privacy).

78. Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CAL. L. REV. 1529, 1559 (2019) (describing "collaborative governance").

79. Christine Bannan & Raj Gambhir, *Does Data Privacy Need its Own Agency?*, NEW AM. (June 2021), https://www.newamerica.org/oti/reports/does-data-privacy-need-its-own-agency/comparing-the-ftc-and-dpa/ ("Even in Europe, where DPAs have faced funding challenges, each of the European DPAs has funding and personnel levels dramatically higher than the FTC's Division of Privacy and Identity Protection.").

80. *E.g.*, Press Release, *FTC Chair Testifies before House Appropriations Subcommittee*, FED. TRADE COMM'N (May 15, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/05/ftc-chair-testifies-house-appropriations-subcommittee (describing testimony from Chairwoman Khan requesting additional funding); John Hendel, *FTC's Simons Proposes Doubling Tech Task Force if Given Extra Funding*, POLITICOPRO (Sept. 24, 2019), https://subscriber.politicopro.com/article/2019/09/ftcs-simons-proposes-doubling-tech-task-force-if-given-extra-funding-3892549 (describing testimony of Chairman Simons requesting addition funding).

Another distressing problem is that the Supreme Court has been systematically dismantling the administrative state, most recently with a series of rulings at the end of the October 2023 term. In June 2024, the Court overturned four decades of settled precedent by abolishing the *Chevron* deference doctrine,[81] diminished the power of many administrative judges,[82] and opened up the floodgates of litigation against agencies by basically reading the civil statute of limitations from the U.S. Code.[83] It will take years and hundreds of lower court cases to fully grasp the way these cases have disrupted the work of the regulatory state. In the meantime, Congress can respond, in all areas of regulation including privacy, by drafting clearer and more narrowly tailored statutes.

2. Tending Toward Platforms and Managerialism

The collaborative-governance-qua-self-regulatory omnibus approach tends to bolster platform power and surveillance capitalism.[84] Julie Cohen describes the rise of "neoliberal managerialism," for example, as "new frameworks for self-regulation and self-certification."[85] Ari Waldman connects this more directly to the privacy law *status quo*, pointing out the power that privacy laws tend to give to privacy professionals on the ground.[86] Some of these professionals "frame the law in accordance with managerial values like efficiency and reducing corporate risk rather than the substantive goals the law is meant to achieve, like consumer protection or equality."[87]

3. Activating a Problematic Political Economy

Another problem with the omnibus approach stems from interest group politics. Once again, this Article is not focused on ideal political conditions; it is deeply grounded in today's political reality. The legislative debates that have arisen around omnibus privacy law proposals have activated some actors and sidelined others,[88] leading to significant mismatches in resources and influence.

81. Loper Bright Enters. v. Raimondo, 603 U.S. 369 (2024) (overturning Chevron Inc. v. Natural Resources Defense Council, Inc., 467 U. S. 837 (1984)).

82. *Jarkesy*, 603 U.S. at 109 (narrowing the SEC's ability to use administrative law judges).

83. *Corner Post*, 603 U.S. at 799 (expanding time to challenge agency action).

84. ZUBOFF, *supra* note 7, at 7–8 (defining surveillance capitalism as "a bold market venture powered by unilateral claims to others' experience and the knowledge that flows from it . . . Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioral data.").

85. COHEN, *supra* note 34, at 186.

86. WALDMAN, *supra* note 21, at 103.

87. *Id.*

88. *See infra* Part IV.C.

Corporate interest groups have dominated the debates, leading to watered-down and insufficiently protective proposals.

In an information age, few companies can afford to ignore what is at stake when the legislature takes up an omnibus bill, given its broad sweep. Giant platforms and small startups alike care about the outcome. Omnibus laws cross sectors, so telecommunications companies, internet platforms, service sector businesses, and industrial-age manufacturing companies all have a stake in the outcome.

Giant platforms perhaps have the most to lose—or win—from the prohibitions, mandates, exceptions, enforcement mechanisms, and remedies provided in an omnibus law.[89] The internet giants like Google, Meta, Apple, and Microsoft see potential omnibus privacy law as a "bet the company" existential threat.[90] They might also see omnibus privacy laws as helpful barriers to entry blocking new competition, giving the giants both offensive and defensive incentives to participate.[91]

Omnibus laws force a kind of cross-industry reckoning, focusing lobbying efforts on one legislative vehicle, leading inexorably to watered-down provisions.[92] Consider two examples from the past of how the industry successfully beat back attempts to enact omnibus privacy protection. Cam Kerry, one of the architects of the Obama White House Consumer Privacy Bill of Rights, complained how the proposal ultimately "was diluted in an unsuccessful effort to broaden business support, lost civil society support in the process, and so fell flat when it was released publicly."[93] Neil Richards and Woody Hartzog tell a similar but much older story, arguing that industry

89. Hartzog & Richards, *supra* note 20, at 1714–15.

90. *See* Anu Bradford, *The False Choice Between Digital Regulation and Innovation*, 119 NW. U. L. REV 377, 384, 388–390 (2024) (explaining how American tech companies view stringent privacy regulations as a significant threat to their business model, often citing innovation and competitiveness as reasons to oppose such laws).

91. *See id.* at 405–06 (discussing how compliance with stringent regulations like the GDPR imposes significant costs, particularly on small tech companies, which can limit their ability to innovate and compete, thereby potentially entrenching the market power of larger tech firms).

92. Alvaro M. Bedoya, *Why Silicon Valley Lobbyists Love Big, Broad Privacy Bills*, N.Y. TIMES (Apr. 11, 2018), https://www.nytimes.com/2018/04/11/opinion/silicon-valley-lobbyists-privacy.html ("This should make us very skeptical about any calls for a broad, European-style privacy law that would apply across technologies and platforms. We cannot underestimate the tech sector's power in Congress and in state legislatures. If the United States tries to pass broad rules for personal data, that effort may well be co-opted by Silicon Valley, and we'll miss our best shot at meaningful privacy protections.").

93. Cameron F. Kerry, *Will This New Congress be the One to Pass Data Privacy Legislation?*, BROOKINGS (Jan. 7, 2019), https://www.brookings.edu/articles/will-this-new-congress-be-the-one-to-pass-data-privacy-legislation/.

intervention watered down the 1970s enactment of the Privacy Act, a law that focuses only on government uses of personal data and is widely considered toothless.[94]

D. TYPES OF FOCUSED PRIVACY LAWS

Omnibus privacy laws thus suffer from various flaws: they flatten a diverse set of privacy problems into one set of rules, lead to platform power and managerialism, and activate a problematic political economy. The rest of this Article will explain how narrower privacy laws do better on all three scores. There is more than one way to narrow the focus of a privacy law, however, and not all improve on omnibus laws along these three dimensions. This Article focuses on three narrowing approaches: sectoral, sensitivity-focused, and use-focused. These are not rigid categories, and laws sometimes fall into more than one.

The oldest category of focused privacy laws is sectoral, meaning laws that govern the activities of a particular industry sector. Many scholars have long documented myriad problems with the sectoral approach, and this Article will not rehabilitate it.[95] Legislatures should be reluctant to write new sectoral privacy laws.

This leaves two other possibilities, both of which this Article supports: sensitivity-focused and use-focused laws. Sensitivity-focused laws govern categories of information deemed to raise high risks of privacy or other harm. Use-focused laws govern certain high-risk uses of any information, without specifying categories of information. Both approaches avoid the three problems of the omnibus approach, to greater or lesser extent. Consider each of these types of narrow privacy laws in turn, before turning to the arguments in favor of the sensitivity-and use-focused alternatives in Parts III through V.

1. Sectoral Laws are Not the Answer

The wrong way to improve on omnibus privacy law would be to write new sectoral privacy laws, which deserve the criticism they have received.[96] The great weight of scholarly assessment on the value of the omnibus approach has argued that they are far better than sectoral laws.[97]

94. Hartzog & Richards, *supra* note 20, at 1715.
95. *See supra* note 8.
96. *Id.*
97. *Id.*

Many criticize sectoral privacy laws for focusing on increasingly arbitrary distinctions between industry segments.[98] One emblematic target of this critique is HIPAA, which governs sensitive health information but only when held by a "health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse."[99] Laws like HIPAA have not kept up with the information economy's widespread *convergence*.[100] Companies like Apple, Google, Fitbit, and Garmin now sell devices that track a wide range of health-related indicators; startups sell devices to track sleep, temperature, and diet; app developers purport to monitor period cycles or mood; data brokers buy all of this data and more, to be resold to government and corporate analysts; and platforms like Google and Microsoft have dabbled in user-controlled health data clearinghouses.[101] Most of these business models fall outside the HIPAA's scope, meaning the core privacy protection for health information does not cover these important commercial uses.[102]

HIPAA is not the only federal privacy law that has not kept up with convergence. GLBA and other financial privacy laws do not cover new personal finance apps that store sensitive financial information;[103] FERPA's

98. *See* Nissenbaum, Strandburg & Viljoen, *supra* note 12, at 1238–39 (arguing that a "scoping dodge" occurs when laws define their obligations around certain actor types, which can become arbitrary over time due to "social, institutional, and technological upheaval.").

99. 45 C.F.R. § 160.103 (defining "health information").

100. *See* Nissenbaum, Strandburg & Viljoen, *supra* note 12, at 1242 (noting that fertility app companies fall outside of the scope of HIPAA: despite "arguably meet[ing] the definition of health care provider, they generally do not transmit PHI in connection with covered transactions."); Frank Pasquale & Tara Adams Ragone, *Protecting Health Privacy in an Era of Big Data Processing and Cloud Computing*, 17 STAN. TECH. L. REV. 595, 629–637 (2014) (noting that non-healthcare companies like data brokers and social media networks gather health data, and meanwhile "healthcare companies are also developing an interest in cognate data.").

101. *See* Nissenbaum, Strandburg & Viljoen, *supra* note 12, at 1233–34 ("Information companies are flexible business entities; they can morph from providing advertising insights to health insurance profiles to financial services relatively seamlessly.").

102. *Health Information Privacy*, U.S. DEP'T OF HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html (last visited Apr. 26, 2025) (noting that HIPAA Rules "do not protect the privacy of data you've downloaded or entered into mobile apps for your personal use" unless the app is "provided to you by a covered entity or its business associate." Further, this information "may also be sold to a data broker.").

103. *E.g.*, Amanda Lindner, *Exploring Financial Data Protection and Civil Liberties in an Evolved Digital Age*, 28 FORDHAM J. CORP. & FIN. L. 271, 271–280 (2023) (analyzing financial laws, particularly the Gramm-Leach-Bliley Act, and concluding due to loopholes "where FinTechs can share financial data without being subject to laws or regulations," "there is no comprehensive financial privacy law that can protect consumers from a company's collection sharing and selling of consumer data.").

education records privacy rules do not extend to many online learning and edtech businesses.[104]

Many have critiqued these anachronisms. Scholars and advocates have decried the way these loopholes create gaps in the protection afforded by these laws.[105] Sectoral actors have complained about the competitive disadvantages they face against the way giant platforms compete with them without needing to comply with these laws.[106]

Although the great weight of the scholarship condemns the sectoral approach, at least one group of noted scholars has recently argued to rehabilitate it. Helen Nissenbaum, Kathy Strandburg, and Salomé Viljoen have argued in favor of a beefed-up form of sectoral regulation to address the problems with the omnibus approach.[107] They concede that today's sectoral privacy laws tend to be subject to what they call "the great regulatory dodge," such as the problems that convergence have created for HIPAA and GLBA. They advocate for expanded sectoral laws, "drafted functionally to apply to entities and activities that involve the relevant sorts of contextual information flows" rather than based on industry participation alone.[108]

2. Sensitivity-Focused Privacy Laws

A *sensitivity-focused law* is a law that provides collection, use, or sharing rules for specific categories of information.[109] In earlier writing, I reviewed how

104. *See generally* Amy Rhoades, *Big Tech Makes Big Data Out of Your Child: The FERPA Loophole EdTech Exploits to Monetize Student Data,* 9 AM. U. BUS. L. REV. 445 (2020).

105. Nissenbaum, Strandburg & Viljoen, *supra* note 12, at 1235 ("The lacuna in federal regulation is obvious: sectoral statutes miss a large swath of consumer data handled by innumerable companies, small and large."); Nicolas P. Terry, *Protecting Patient Privacy in the Age of Big Data*, 81 UMKC L. REV. 385, 387 (2012) ("[T]he very concept of health sector specific regulation is flawed because health related or medically inflected data frequently circulates outside of the traditionally recognized health care sector.").

106. *See* Erika M. Douglas, *The New Antitrust/Data Privacy Law Interface*, 130 YALE L.J. FORUM 647, 651 (2021) ("Spotty, sector-specific privacy legislation left large swathes of that new online activity unprotected by any data privacy laws.").

107. Nissenbaum, Strandburg & Viljoen, *supra* note 12, at 1261–62.

108. *Id.*

109. *See* Ohm, *Sensitive Information*, *supra* note 16. There is an important hybrid category of privacy rule: the sensitive-within-omnibus category. Every omnibus privacy law provides heightened protections for some sensitive categories of information. Article 9 of the GDPR identifies "special categories" of information for additional protections. GDPR, *supra* note 4. State omnibus laws like the CCPA do the same. CCPA, *supra* note 31.

These smatterings of sensitivity do not rehabilitate omnibus approaches. A few of the arguments presented in favor of focused laws below also provide support for sensitive-within-omnibus provisions. To give one example, sensitive-within-omnibus laws may beneficially reshape the structure of tech companies and the products and services they create.

legislatures had defined these "sensitive information" categories, concluding that they were categories of "information that can be used to enable privacy or security harm when placed in the wrong hands."[110] Since I last reviewed this topic, several new and noteworthy sensitive information laws have been enacted, allowing me to refine the definitions I presented earlier.[111]

Although all sensitive information categories tend to reflect a legislature's or agency's assessment of the risk of harm, they typically fall into one of three overlapping categories: information is considered sensitive if it (1) has been linked to some form of harm (e.g., information about sexual activity used for blackmail or information about race used to unfairly or illegally discriminate); (2) concerns a particular vulnerable or marginalized group (e.g., information about children); or (3) tends to be gathered from a medium[112] or through a relationship protected as confidential (e.g., stored email or student records). Some information falls into more than one of these categories. For example, health information falls into all three, as it can be linked to specific risks of harm (e.g., diagnoses that tend to stigmatize or discriminate), can concern vulnerable populations (e.g., people with certain disabilities), and is often gathered through a confidential relationship (e.g., doctor-patient).

Consider two sensitivity-focused privacy laws enacted in the states. Illinois's Biometric Information Privacy Law (BIPA), enacted in 2008, governs "biometric identifiers," such as fingerprints or face geometry, regardless of who holds them, as well as "biometric information," meaning biometric identifiers "used to identify an individual."[113] The law requires consent in the form of a "written release" before any "private entity may collect, capture, purchase, receive through trade, or otherwise obtain" a biometric identifier or biometric information.[114] It also makes it illegal, without opportunity for opt-

But more of the arguments below militate in favor of focused laws instead. For example, focusing a law on a single sensitive category activates political actors and arguments that might be sidelined during an omnibus debate. This is not true for debates over sensitive-within-omnibus provisions, which are enacted in the all-against-all scorched-earth-warfare setting of an omnibus debate that this Article finds problematic.

110. *Id.* at 1133.

111. Earlier, I offered four factors that seemed to characterize the categories of information that had been deemed sensitive: (1) the connection between the category of information and the harm; (2) a sufficiently high probability of harm; (3) information shared confidentially; and (4) risks that reflected majoritarian concerns. *Id.* at 1161–69.

112. In my earlier treatment, I distinguished sensitive information laws from laws that I called "protected channel" laws. *Id.* at 1136. I have concluded that this distinction added an unnecessary complexity to the analysis and now treat these all as within the category of "sensitive information."

113. Biometric Information Privacy Act (BIPA) of 2008, 740 ILL. COMP. STAT. 14/10 (defining "biometric identifier").

114. *Id.* 14/15(b).

out consent, for any private entity to "sell, lease, trade, or otherwise profit" from a biometric identifier or biometric information.[115]

More recently, the Washington State legislature enacted the "My Health My Data Act (MHMD)," a health data law designed in part to address the sectoral shortcomings of HIPAA.[116] It regulates all uses in the state of "consumer health data," defined as "personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status."[117] It forbids businesses from collecting, sharing, or selling of consumer health data without prior consent, with certain exceptions.[118] The law is connected to the state's consumer protection law, which provides a private right of action.

BIPA and MHMD are neither the first nor the only sensitive information laws in this country, and the federal government has enacted a few. However, the federal examples tend to be narrower in scope or straddle the line between sectoral and sensitive.[119]

3. Use-Focused Privacy Laws

The third type of focused privacy law regulates specific risky or harmful *uses* of information.[120] Like sensitivity-focused laws, these proposals are touted for being narrower and thus more politically viable than omnibus laws.[121] Unlike sensitivity-focused laws, however, these approaches expressly apply to all categories of information.

For example, several recently enacted laws have targeted algorithmic decision-making. These laws target "profiling" or automated decision-making that either has "legal effects" or "similarly significantly affects" the data

115. *Id.* 14/15(c).

116. WASH. REV. CODE §§ 19.373.005–19.373.900 (2023).

117. *Id.* § 19.373.010(8)(a).

118. *Id.* §§ 19.373.030(1)(a), (1)(b), § 19.373.070(1).

119. Video Privacy Protection Act, 18 U.S.C. § 2710; Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6505; Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, Title III, 82 Stat. 211 (1968) (Wiretap Act); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (amending the Wiretap Act).

120. Solove, *supra* note 18, at 1128. A closely related type of privacy law is a purpose-focused law, one that governs the purpose for which data is processed. The key distinction is that a purpose tends to focus on the stated intent of the person doing the processing, while a use focuses more on how data is actually processed. *Id.* at 1128 n.194.

121. *Id.*; Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1902 (2013) ("[T]he focus should be more on downstream uses rather than on the time of the initial collection of data.").

subject.[122] Unlike a sensitivity-focused law, these laws apply to algorithmic decision-making regardless of what kind of data used to support the decision-making. Proponents criticize laws that presuppose that only certain categories of "risky" information—e.g., health or financial information—can be used to harm individuals.

Dan Solove has argued more generally and expressly in favor of use-based laws and against sensitivity-focused laws.[123] He proposes, for example, new laws prohibiting discriminatory uses of data.[124]

E. SCOPE VERSUS SUBSTANCE

Before turning to the arguments in favor of focused privacy laws, it is important to disentangle the scope and substance of a law. Each privacy law defines a scope: the types of data, actors, and actions governed by the law. The scope of a privacy law dictates the law's coverage, leaving anything outside the scope uncovered. The substance of the law is the set of rules, obligations, rights, and procedures that apply to the data, actors, and actions that fall within the law's scope.

For example, HIPAA's scope covers "protected health information" held by "covered entities" and "business associates."[125] A privacy law's scope is often limited by exceptions, such as HIPAA's exemption for deidentified information.[126]

For data falling within HIPAA's scope, the substance permits use for treatment, payment, and health care operations while requiring consent and other procedural hurdles for uses beyond these, such as marketing.[127] The substance of HIPAA gives the Department of Health and Human Services (HHS) the responsibility of monitoring compliance, and it extends investigative powers to HHS to support enforcement.[128]

---

122. *E.g.*, GDPR, Regulation (EU) 2016/679 Art. 22 ("The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.").

123. Solove, *supra* note 18, at 1128.

124. *Id.* at 1133. *See infra* Part VI.B (describing and rebutting Solove's arguments against sensitive information laws).

125. 45 C.F.R. § 160.103 (definitions).

126. *Id.* §§ 164.514(a)–(b).

127. *Id.* § 164.506 (specifying uses and disclosures without the need for individual authorization); §§ 164.501, 164.508(a)(3) (marketing).

128. The substance of HIPAA, as codified in 45 C.F.R. § 160.300-316 (Compliance and Investigations), gives the Department of Health and Human Services (HHS) the responsibility of monitoring compliance. This includes the power to conduct investigations, as stated in 45

It can be helpful to consider scope independently of substance. We can assess the relative pros and cons of a more narrowly scoped law—say one drawn along sectoral, sensitivity, or use lines—versus a more broadly scoped law—say an omnibus law, independent of substantive considerations.[129] Many of the arguments' pros and cons—presented throughout the rest of this Article—apply independent from and prior to considerations about the substance required for each law.[130] For example, we can consider whether a narrowly scoped law helps civil society groups focus their energy, or whether narrowly scoped laws relate to the way scholars conceptualize privacy harm, irrespective of the substance of the law.

Some scholars purport to argue for a particular scope when in fact they seem more concerned about the substance that has been attached to that scope. Dan Solove has launched a broadside critique against sensitivity-focused laws, but he seems primarily motivated by the onerous compliance obligations the GDPR (and laws like it) attach to data deemed sensitive.[131] To be fair, some of his arguments[132] focus on scope, but a key thrust appears to be that sensitive information laws make data processing impossible for too large a category of data.[133] Regardless of the merits of the argument, it is a critique of substance, on the way the GDPR treats sensitive information, not on the scoping decision to treat sensitive information differently from other personal information.

Separating scope from substance is especially useful given the widespread scholarly consensus on the problem with the substantive approaches in almost all privacy laws.[134] Most privacy scholars have turned away from so-called

C.F.R. § 160.306(c). The authority to enforce HIPAA through penalties is derived from 42 U.S.C. § 1320d-5 (General Penalty for Failure to Comply with Requirements and Standards).

129. *See* Ohm, *supra* note 16, at 1129 ("Sensitive information is a showstopper. Otherwise lax regulations become stringent when applied to it. Permissive laws set stricter rules for the sensitive.").

130. *See* Nissenbaum, Strandburg & Viljoen, *supra* note 12, at 1255 ("Our analysis is not a defense of the GLBA's paltry requirements, however, but a lesson about sectoral privacy regulation design.").

131. Solove, *supra* note 18, at 1084 ("If nearly all data is sensitive data, then most organizations are violating the EU's General Data Protection Regulation (GDPR) and many other privacy laws that have heightened protections for sensitive data.").

132. *Infra* Part VI.B.

133. Solove, *supra* note 18, at 1084.

134. *E.g.*, Solove, *Privacy Self-Management and the Consent Dilemma*, *supra* note 121, at 1880, (criticizing the notice-and-choice framework, arguing that it fails to provide meaningful control over personal data: "[p]rivacy self-management does not provide people with meaningful control over their data" due to various cognitive and structural limitations. Solove further contends, "[c]onsent legitimizes nearly any form of collection, use, or disclosure of personal data," which is impractical for individuals to manage across numerous interactions);

notice-and-choice or privacy self-management approaches premised on giving users control over how their information will be stored, used, and shared.[135] These scholars have complained about how notice-and-choice regimes demand too much focus and work by busy and distracted users;[136] how companies take advantage of dark patterns and subtler forms of information presentation to coax users to make choices against their true preferences;[137] and how companies have subverted privacy self-management to manipulate users in order to advance their own interests, for example through managerial control.[138]

Privacy self-management approaches can (and do) exist in omnibus laws as well as in all the focused alternatives.[139] We should not conflate the widespread dissatisfaction over these approaches with anything intrinsic to a focused approach, just as we should not attach them necessarily to the omnibus approach, either.

But the debate about scope cannot be completely disentangled from substantive considerations. The reason to prefer focused laws over omnibus laws is to enact different obligations based on context. In the end, policymakers will need to weigh both scope and substance together. But this Article will keep substantive considerations mostly in the background.

NEIL M. RICHARDS, WHY PRIVACY MATTERS 55–56 (2022) (describes "terrible 'notice-and-choice' rule" as "an elaborate trap"); WALDMAN, *supra* note 21, at 52 (expands on three faulty assumptions that notice-and-choice regimes' legitimacy are based on: "(1) that we can adequately process corporate privacy notices, (2) that our decision-making is rational, and (3) that consent is the same as making a real choice.").

135. Solove, *supra* note 121; RICHARDS, *supra* note 134; WALDMAN *supra* note 134, at 52–57.

136. WALDMAN, *supra* note 21, at 52, 55 ("[I]t would take us nearly 244 hours per year to read the privacy policies of the websites we visit just once. . . . We don't have the cognitive ability to process and understand privacy policies.").

137. WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 208 (2018) ("We can feel so overwhelmed by the thousands of requests for access, permission, and consent to use our data that we say yes just because we are so worn down."); WALDMAN, *supra* note 21, at 56 ("Consent is also easy to manipulate and manufacture. Platforms can use dark patterns to make it seem like accepting cookies, geotracking, or surveillance is the only option.").

138. *See generally* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014); Daniel Susser, Beate Roessler & Helen Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World*, 4 GEO. L. TECH. REV. 1 (2019).

139. *E.g.*, GDPR, Regulation (EU) 2016/679 Art. 6 (omnibus law allowing processing once "the data subject has given consent to the processing"); GLBA, 15 U.S.C. § 6802 (sectoral law with opt-out provision).

III. HARM REDUCTION: RECOGNIZING HARM, RIGHTS, AND CONTEXT

The arguments in favor of focused privacy laws fall into three categories. This Part focuses on the first, the way focused privacy laws correspond to our well-developed notions of harm, rights, and context. They thus build on some of the most important scholarly writing about *why* we ought to protect privacy.

A. ACCOUNTING FOR HARM

One reason to enact new and bolster preexisting use-and sensitivity-focused laws is to focus privacy law on preventing and remediating harm and the risk of harm. Use-focused laws regulate uses known to raise risks of harm. Categories of sensitive information amount to predictions of how information can be used to harm individuals, groups, and society.[140]

Omnibus laws tend not to draw lines along harm and tend instead to defer harm to second-and third-order protections and considerations, such as the managerial choices of regulated companies or the priorities of enforcement officials.[141]

From the birth of information privacy law as a field through two-plus decades of development, some of the best reasoned, most sharply analyzed, and most practically implementable scholarly writing has focused on privacy harms that arise in narrow contexts, affecting certain kinds of individuals engaged in specific activities.

Danielle Citron has identified a family of information privacy harms under the label of *intimate privacy*.[142] These harms stem from individuals and companies misusing information about sex, sexuality, and relationships. Blackmailers and extortionists ranging from individual actors to sophisticated crime rings use images and information to target people, including children.[143] Domestic abusers install communications-monitoring and location-tracking stalkerware on the cell phones of their partners.[144] Platforms use intimate data to manipulate the vulnerable, for example recommending content on social media sites that fuel anxiety and depression.[145]

140. Ohm, *Sensitive Information*, *supra* note 16, at 1132–1133.

141. WALDMAN, *supra* note 21, at 118.

142. CITRON, *supra* note 22, at xii (2022) ("Intimate privacy involves the social norms (attitudes, expectations, and behaviors) that set and fortify the boundaries around our intimate lives. It concerns 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.").

143. *Id.* at 31.

144. *Id.* at 34.

145. *Id.* at 22.

The harms these victims experience are well-established, concrete, and significant. These actions cause "significant emotional distress" and shatter self-esteem.[146] "Victims' lives are plagued with worry and pain."[147] "A majority of victims suffer serious physical, emotional, and psychological trauma, resulting in chronic conditions like depression and PTSD."[148] "Minors . . . are particularly vulnerable to depression and suicide."[149] "Victims stop expressing themselves and withdraw from community activities."[150]

More broadly, Citron and Dan Solove have laid out a typology of privacy harms.[151] They identify seven specific types: "(1) physical harms; (2) economic harms; (3) reputational harms; (4) psychological harms; (5) autonomy harms; (6) discrimination harms; and (7) relationship harms." Many of the harms they identify often occur when sensitive information is misused.[152] Information about physical location can be used to inflict physical harm, such as in the tragic case of Rebecca Schaefer, an actress murdered by a stalker who used DMV records to learn her home address.[153] Doxing is one example of the disclosure of physical location that has tragically led to many injuries and deaths.[154] Psychological harm such as emotional distress is often the result of the improper disclosure of location as well.[155]

Economic injury often results in the form of identity theft, which entails the abuse of information like account numbers and passwords, which are considered sensitive information under many statutes.[156] Actionable discrimination harm results from the improper use of information that reveals a person's protected class characteristics, such as race, ethnicity, sex, gender, or disability.[157] Discrimination harms also result when decisions are made based on information, such as reproductive health information that disproportionately impact protected groups.

In earlier writing, I coined the phrase "database of ruin" to describe the way modern data practices tend to "join the data from all of the databases in

146. *Id.* at 41.
147. *Id.* at 41.
148. *Id.* at 42.
149. *Id.*
150. *Id.*
151. Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 830 (2022).
152. *Id.* The point of their analysis is to help courts more often recognize privacy harms, for example in Article III standing. *Id.* at 831.
153. *Id.* at 832.
154. *Id.* at 834.
155. *Id.* at 841–42.
156. *Id.* at 835.
157. *Id.* at 855.

the world together into one, giant, database-in-the-sky, an irresistible target for the malevolent."[158] The database of ruin makes every one of us susceptible to "blackmail, discrimination, harassment, or financial or identity theft."[159] A use-focused law could target these specific harms. Many of the data points that could be used to these ends would be protected under various definitions of sensitive information.[160]

B. ACCOUNTING FOR RIGHTS

Focused privacy laws are also better than omnibus privacy laws for protecting civil and human rights. A significant amount of writing in information privacy has focused on how certain data practices impinge on civil and human rights. As with the writing on harm, many rights-based discussions focus on specific categories and uses of information. Sensitivity-focused and use-focused laws can be tailored to those concerns.

In 2020, Alvaro Bedoya, now an FTC Commissioner, argued that privacy should be properly understood as a civil right.[161] He forcefully argued through stories from Plymouth Rock to J. Edgar Hoover to Donald Trump's Immigration and Customs Enforcement that there is a "color of surveillance."[162] Importantly he pointed out that the minority and marginalized targets of this surveillance were often not "helpless victims"; instead, they were often "watched precisely because they [were] fighting back," citing the government's surveillance of figures such as Cesar Chavez and Martin Luther King Jr.[163] Some of his examples focused on the tracking of sensitive information, such as: location tracking using automated license plate readers, facial recognition systems powered by DMV records,[164] the monitoring of the intimate details of relationships of Mormons in the nineteenth century,[165] and the wiretapping of King in the twentieth.[166]

Commissioner Bedoya is not the only privacy scholar focused on the connection between information privacy and civil rights. Neil Richards focuses on the impact on speech and thought that results from surveillance into what people read or the media people consume. Richards advocates for what he

158. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1748 (2010).
159. *Id.*
160. *Id.* (pointing to facts about "past conduct, health, or family shame").
161. Alvaro M. Bedoya, *Privacy as Civil Right*, 50 N.M. L. REV. 301, 306 (2020).
162. *Id.*
163. *Id.* at 309–311.
164. *Id.* at 317.
165. *Id.* at 308.
166. *Id.* at 311.

calls *intellectual privacy*, a "zone of protection that guards our ability to make up our minds freely."[167] Failure to protect intellectual privacy risks profound chilling effects, harming not only to the person who refrains from speaking or reading but also those around them or society generally with the ideas not transmitted.[168]

Citron's writing on intimate privacy and sexual privacy documents, in chilling detail, how women and other marginalized people are disproportionately targeted in online spaces. Anonymous assailants subject them to harassment, doxing, and threats.[169] Invasions of intimate privacy "reinforce destructive bigoted and gendered stereotypes."[170] These invasions often have economic consequences, such as when employers refuse to interview applicants due to damaging search results of their names, or when victims of nonconsensual intimate image sharing lose their jobs.[171]

Along these lines, Scott Skinner-Thompson has argued for a constitutional right of information privacy specifically to prevent the government from abusing two categories of sensitive information: intimate information and political thought.[172] Intimate information would include "primarily sexual, medical, and mental health information."[173] Political thought would be carved along similar lines to Richards's category of intellectual privacy.[174]

After the Supreme Court reversed *Roe v. Wade*[175] and stripped people of the right to make important reproductive health care decisions, some scholars have focused on how the lack of information privacy can subject doctors and patients to criminal investigation and prosecution.[176] This continues a history of troubling pregnancy surveillance, such as the invasive monitoring tied to public funding for prenatal care.[177]

---

167. RICHARDS, *supra* note 22; Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 419 (2008).

168. Richards, *Intellectual Privacy*, *supra* note 167, at 419 ("Intellectual exploration must be private . . ., and also unwatched, lest the surveillance of others chill the development of new thoughts in the direction of the bland and the mainstream."); *see also* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1425 (2000).

169. Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 68–81 (2009).

170. CITRON, *supra* note 22, at 43.

171. *Id.* at 44.

172. Scott Skinner-Thompson, *Outing Privacy*, 110 NW. U. L. REV. 159, 175 (2015).

173. *Id.* at 205.

174. *Id.* at 212.

175. Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228 (2022), overruling Roe v. Wade, 410 U.S. 113, 154 (1973), and Planned Parenthood v. Casey, 505 U.S. 833, 834 (1992).

176. Huq & Wexler, *supra* note 23, at 576–77.

177. CITRON, *supra* note 22, at 61.

Scholars and advocates have argued that police use of facial recognition technology allows standardless mass surveillance at a distance, which chills speech and association. These technologies also tend to make life-altering mistakes, often disproportionately affecting black people.[178]

C. ACCOUNTING FOR CONTEXT

Beyond privacy harm and civil rights violations, focused laws also better account for contextual variation. Philosopher Helen Nissenbaum's influential theory known as "contextual integrity" conceptualizes privacy as the "appropriate flow of information," meaning flow that comports with norms in a given context.[179] In her theory, contexts are "distinct social domains . . . such as commerce, education, finance, healthcare, civic life, family, and friends."[180]

Contextual integrity has been deeply influential.[181] Researchers have used the "CI" framework to analyze a vast array of privacy problems.[182] Advocates cite CI to support new legislation and to advise courts on how to interpret existing law. Privacy laws around the world bear the imprint of CI in the way they emphasize context.[183]

In more recent writing, Nissenbaum and her co-authors have used context to critique omnibus privacy legislation.[184] Similar to the approach taken in this Article, those scholars seem critical not of ideal omnibus legislation, but instead by the way "simplistic" omnibus laws enacted today rely on problematic notice-and-choice frameworks.[185]

---

178. Clare Garvie, Alvaro M. Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO. L. CTR. PRIV. & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org/ [https://perma.cc/3K32-2YE6].

179. NISSENBAUM, *supra* note 24, at 140–47.

180. Nissenbaum, Strandburg & Viljoen, *supra* note 12, at 1236.

181. Jordan M. Blanke, *Top Ten Reasons to Be Optimistic About Privacy*, 55 IDAHO L. REV. 281, 284 (2019) ("[*Privacy as Contextual Integrity*] has been arguably the most influential article ever written about privacy in terms of shaping the direction of privacy research and its literature.").

182. *See* Sebastian Benthall, Seda Gürses & Helen Nissenbaum, *Contextual Integrity Through the Lens of Computer Science*, 2 FOUNDS. & TRENDS PRIV. & SEC. 1, 1 (2017) (surveying uses in Computer Science of contextual integrity).

183. Alexis C. Madrigal, *The Philosopher Whose Fingerprints Are All Over the FTC's New Approach to Privacy*, THE ATLANTIC (March 29, 2012), https://www.theatlantic.com/technology/archive/2012/03/the-philosopher-whose-fingerprints-are-all-over-the-ftcs-new-approach-to-privacy/254365/.

184. Nissenbaum, Strandburg & Viljoen, *supra* note 12, at 1238.

185. *Id.* ("While omnibus laws attempt to import flexibility through notice and consent, that approach is unworkable in the modern world where it is impossible for individual data subjects to meaningfully assess the choices they are presented with.").

However, in arguing against "simplistic" omnibus privacy laws, Nissenbaum and her collaborators say little about sensitivity-or use-focused alternatives.[186] Instead, they recommend incorporating contextual integrity into the way we write sectoral and omnibus laws.[187] Sectoral laws like HIPAA could be amended to account for convergence issues, and to avoid what they call the dual problems of the "scoping dodge" (the way direct-to-consumer health apps aren't covered) and the "exceptions dodge." (The way many laws exempt "public" data from their coverage, notwithstanding many privacy-in-public concerns.)[188] Likewise, they suggest amending omnibus laws to "incorporate a general [contextual integrity] standard to be fleshed out by judges and agencies."[189]

Although Nissenbaum herself has not fully endorsed sensitivity-focused nor use-focused alternatives, I believe that CI supports these approaches because they attend specifically to some of the five factors at the heart of CI: the data subject, data sender, data recipient, information type (topic, attribute), and transmission principle.[190] Sensitivity-focused laws center on the "information type" factor. Use-focused laws emphasize the "transmission principle," which she defines as "the conditions, or constraints, under which data about subjects flows from senders to recipients."[191]

D. TAILORED SOLUTIONS FOR TAILORED HARMS

One reason to tailor legislative solutions to specific harms, rights, and contexts is to put legislators and regulators in close consultation with experts focused on that particular slice of information and its corresponding regulatory environment.[192]

For example, nonconsensual intimate image laws must grapple with the history of blaming victims that we have grappled with already in our legal history. Putting women "on trial" for engaging in sex on camera is a tried (and tired) strategy, and focused laws might take that into consideration by

186. *Id.* at 1261–64.
187. *Id.* at 1264.
188. *Id.* at 1256.
189. *Id.* at 1262.
190. *Id.* at 1237.
191. *Id.* I suspect Nissenbaum might be critical of focused privacy laws because "information type" or "transmission principle" is only one of five "parameters" used in the theory of contextual integrity. She might argue that any law premised on a single parameter will miss the subtlety and contextual variation that is at the heart of the theory.
192. *Id.* at 1248 ("Ultimately, while regulators will benefit from the insights of privacy experts, the experts most critical to this endeavor are those who grasp the data flows enabled by fertility app use and can envision how those data flows affect people, healthcare systems, and societies.").

permitting pseudonymous lawsuits or modifying rules of evidence. Similar protections may not be necessary or appropriate to protect other categories of sensitive information, say precise geolocation information, where the problem of victim shaming is not always present.

Another example of the need to focus laws relates to enforcement. For some sensitive categories, the harms in any violation tend to be varied and individualized, perhaps suggesting the importance of individual private rights of action. Laws protecting information revealing sexual orientation are an example.

In contrast, some sensitive categories and specific harmful uses tend to produce diffuse but similar harms felt by many victims. Laws protecting information about children are one example. Laws about information about children might be best enforced by the FTC and State Attorneys General, who can marshal centralized resources and powerful investigative tools to go after large-scale technology platforms. For this reason, individual private rights of action might be less necessary or even potentially counterproductive.

E. AS APPLIED TO USE-FOCUSED AND SENSITIVITY-FOCUSED LAWS

Although this Article provides support for both use-focused and sensitivity-focused laws as improvements to the omnibus status quo, the arguments support each of the two categories in somewhat different ways and to varying extents. Parts III through V of this Article will each conclude by elaborating on some of these differences.

In general, both use-focused and sensitivity-focused laws attend to harm, rights, and context. A use-focused law targeting algorithmic discrimination, for example, protects the civil rights of people in protected classes, recognizing the way important decisions increasingly get made with the assistance of algorithms. A sensitivity-focused law protecting reproductive health information helps protect the rights and safety of pregnant people and their doctors.

The key distinction is a tradeoff between precision and flexibility. The categorical approach taken by sensitivity-focused laws makes them precise tools for focusing on specific harms, rights, or contexts. They identify the precise categories of sensitive information that have led to past harms or violations of civil rights. Laws protecting health information, for example, acknowledge the way medical records tend to be connected closely to a range of health information harms the laws are meant to address.

In contrast, use-focused laws are more flexible because they apply to uses regardless of the underlying categories of information. This approach might be a better way to protect a right or context or to protect against a harm. For

example, a use-focused law might prohibit the use of any information for discriminatory purposes in employment or advertising, regardless of the kind of information used.

The tradeoff between precision and flexibility is common in law, as exemplified by the old debate over rules and standards.[193] This distinction will matter more for some of the other arguments in later Parts. When harms, rights, and context are the focus, both sensitivity-focused and use-focused approaches should be used.

IV. INSTITUTION SELECTION: CHANNELING POWER AND POLITICS

The second set of arguments for enacting narrow privacy laws focuses on power, politics, and the comparative strengths and weaknesses of various government institutions. Narrower laws give Congress more fine-grained control over the priorities and content of privacy protection. This approach prioritizes a part of government that is more politically accountable than agencies. It also responds to the unfortunate twin realities of the chronic underfunding of agencies by Congress and the Supreme Court's recent and systematic stripping of agency power.

States also have an important role to play in enacting focused privacy laws. States can prioritize different categories of sensitive information or different uses of data to reflect their individual histories, politics, institutions, and priorities. States can also serve as Brandeisian laboratories of privacy law innovation by experimenting with different narrowing approaches. To avoid impeding this innovation, no federal omnibus law should preempt narrowly drawn state privacy laws, even if federal politics demand the preemption of omnibus state privacy laws.[194]

Finally, public choice theory suggests that narrower privacy laws—at both the state and federal levels—narrow the political stakes, increasing the odds of success and helping avoid watered down protections. Huge platforms tend to see debates over omnibus privacy laws as existential, bet-the-company moments and spend their lobbying budgets accordingly. They may feel less threatened by a much narrower debate exclusively over, for example, reproductive health information or precise geolocation information.

193. *See, e.g.*, Pierre J. Schlag, *Rules and Standards*, 33 UCLA L. REV. 379, 383 (1985).

194. *See* Schwartz, *supra* note 8, at 946 ("A federal omnibus information privacy law with strong preemption provisions would be an unfortunate development. It would limit further experimentation in federal and state sectoral laws. Such a law also would be difficult to amend, and would, therefore, become outdated as technological changes undermine such a statute's regulatory assumptions.").

A. SELECTING INSTITUTIONS

Omnibus laws and their narrower alternatives differ in how they allocate power and responsibility between legislatures and agencies. The broad coverage of omnibus laws relieves the legislature of dealing with the finer details of implementation. The GDPR covers "personal data," and the CCPA similarly governs "personal information." These sweeping definitions amount to a legislative delegation to agencies of the power and obligation to flesh out the details.

In contrast, focused privacy laws require the legislature to delve more deeply and specifically into the details. Defining the scope of a narrow privacy law—the categories of sensitive information or the specific uses that are covered—reserves a finer-grained role within the legislature, giving less discretion to the agency.

Considering only institutional competence, we would likely not prefer legislative control to administrative expertise when it comes to something as complex and fast-moving as the information economy. At the same time, the concern with complexity can be overstated—Congress and state legislatures write detailed laws governing many complex topics, some arguably much more complex than the digital economy—from nuclear energy to environmental protection to the tax code to trade policy.

One reason to shift some power from agencies to Congress (and state legislatures) is simple political accountability. Congress is more politically accountable than the administrative agencies. Those who argue in favor of new privacy regulations might find ways to marshal and highlight public alarm about a new privacy problem to urge Congress to act. At the same time, those opposed to new privacy protections will marshal industry lobbyists to argue against burdensome new restrictions. Congress has more of an incentive, and more expertise, in gauging these political signals than more insular agency heads.

There are also practical reasons to want to shift some of the work of protecting privacy away from agencies. First, agencies tend to be underfunded.[195] Asking the FTC to take on a sweeping new omnibus privacy law would be asking an under-resourced agency to do more. In contrast, giving the FTC new, well-defined enforcement powers over a narrow class of information practices might strike the balance of empowering without overburdening the FTC.

Shifting responsibility from agencies to Congress also responds to the Supreme Court's recent and systematic dismantling of the administrative state,

195. Sherman, *supra* note 27.

especially at the end of the October 2023 term. In June 2024, the Court upset 40 years of precedent by abolishing the *Chevron* preemption doctrine, stripped some agencies of the right to bring their claims to an administrative judge, and opened up the floodgates on spurious challenges by basically reading the civil statute of limitations out of the U.S. code.[196] It will take years and hundreds of lower court cases to better understand the way these cases have disrupted the work of the regulatory state. In the meantime, Congress should begin writing new laws clarifying the role that agencies play in this new landscape. Writing narrower laws is one approach they ought to consider when they do.

B. ACTIVATING THE LABORATORIES OF PRIVACY LAW

In a time of dysfunction in the federal government, we increasingly look to the states to address the big problems of our day. This is certainly true for privacy legislation, as the states have enacted dozens of both omnibus and focused privacy laws in recent years.[197]

Illinois's BIPA is the single-best example of a focused privacy law with meaningful privacy impact in this country. After sitting quietly on the books for several years, it suddenly became a powerful force after the Illinois Supreme Court issued a series of opinions clarifying the broad private right of action the law provided.[198] Now, an active plaintiffs' bar routinely files lawsuits against major technology companies experimenting with facial recognition and other biometric technologies.[199] Giant tech platforms and startups alike have had to shape their products and services to comply with the Illinois law.[200]

196. *See* cases cited *supra* note 28.

197. Kibby, *supra* note 6 (tracking state privacy legislation).

198. Erin Heller, Note, *Analyzing the Legal Landscape of BIPA Preemption*, 2024 U. ILL. L. REV. 645, 648 (2024); *see also* Cothron v. White Castle Sys., Inc., 216 N.E.3d 918, 924 (Ill. 2023) (holding that each scan of a biometric identifier is a separate BIPA violation); Tims v. Black Horse Carriers, Inc., 216 N.E.3d 845, 853 (Ill. 2023) (applying a five-year statute of limitations to BIPA, rejecting a defense argument for only one year); Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1206 (Ill. 2019) (requiring only a statutory violation—not a separate proof of actual harm—to sustain a BIPA award).

199. *See* Heller, *supra* note 198, at 648 (describing the opening of "floodgates" of litigation in 2019).

200. *See* Adi Robertson, *Clearview AI Agrees to Permanent Ban on Selling Facial Recognition to Private Companies*, THE VERGE (May 9, 2022), https://www.theverge.com/2022/5/9/23063952/clearview-ai-aclu-settlement-illinois-bipa-injunction-private-companies; Torsten Kracht, Lisa Sotto & Bennett Sooy, *Facebook Pivots from Facial Recognition System Following Biometric Privacy Suit*, REUTERS (Jan. 26, 2022), https://www.reuters.com/legal/legalindustry/facebook-pivots-facial-recognition-system-following-biometric-privacy-suit-2022-01-26/.

Whether BIPA represents the source of vexation litigation or meaningful privacy protection is somewhat in the eye of the beholder.[201] I fall in the latter camp—I believe BIPA has been a powerful and positive force of privacy protection, perhaps the most significant focused law currently on the books in the United States. But even for those who disagree, the point stands that state legislatures can be major players in privacy law by enacting new focused laws.

As with omnibus privacy laws, states will pay close attention to what their peer states do with privacy law to both keep up with and stay one step ahead, thanks to a spirit of interstate collaboration mixed with a healthy sense of competition.

Narrow state privacy laws also fare better under two constitutional principles that have been used to assail other types of laws: the dormant commerce clause and Article III standing. There is a looming battle over whether state-level omnibus privacy laws violate the dormant commerce clause.[202] Narrow laws focused on categories of sensitive information or specific uses or purposes might fare better under dormant commerce clause analysis than sweeping omnibus laws.

Federal privacy enforcement has been hampered by the Supreme Court's jurisprudence on Article III standing, which has raised new barriers for private rights of action specifically in privacy cases.[203] State courts, however, are not restricted by the case or controversy requirements of Article III, and many do not have comparable restrictions on private rights of action.[204]

Finally, the specter of possible federal preemption looms. One reason many in Congress have been motivated to consider omnibus privacy laws like ADPPA and APRA is due to increasing industry dissatisfaction with the

201. *Compare a Bad Match: Illinois and the Biometric Information Privacy Act*, 2021 INST. FOR LEGAL REFORM 2 ("The Illinois Biometric Information Privacy Act is a prime example of a misdirected law that has led to more litigation abuse than consumer protection.") *with Biometric Information Privacy Act (BIPA)*, ACLU Illinois (last visited March 3, 2025), https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa ("At this critical moment, it is important for state decision makers to continue protecting BIPA under mounting attacks.").

202. *See* Jack Goldsmith & Eugene Volokh, *State Regulation of Online Behavior: The Dormant Commerce Clause and Geolocation*, 101 TEX. L. REV. 1083, 1087 (2023) (analyzing dormant commerce clause challenges to social media regulation and other laws).

203. *See* TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2201 (2021) (holding that mere statutory violations, without concrete harm—such as undisclosed misleading credit reports—cannot establish standing); Spokeo, Inc. v. Robins, 578 U.S. 330, 341 (2016) (clarifying that a "bare procedural violation" cannot suffice without showing a concrete and particularized injury); Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 (2013) (rejecting standing based on speculative injuries and requiring harm to be "certainly impending").

204. Wyatt Sassman, *A Survey of Constitutional Standing in State Courts*, 8 KY. J. EQUINE, AGRIC., & NAT. RESS. L. 349, 353 (2015).

growing patchwork of state omnibus laws. Both proposals featured sweeping state preemption, which is industry's must-have feature for any new federal omnibus privacy law. Although civil society groups have been willing to stomach preemption in exchange for a strong federal privacy law, state government representatives, especially those from California, fundamentally oppose preemption and have been a major roadblock to these laws.[205]

Those who insist on preemption in an omnibus privacy law may not ask for preemption for narrower laws.[206] As explained in the next subpart, companies have less at stake with a narrow law, which may focus on information categories or uses that are not especially important to a given company.[207]

Thus, if Congress insists on some form of federal preemption, it should take care not to stand in the way of narrower state privacy laws. Any federal preemption for state privacy laws should expressly exempt "privacy laws that focus on specific uses or categories of information."

C. NARROWED POLITICS: THE PUBLIC CHOICE ANALYSIS

Public choice theory has been described as "the application of the economist's methods to the political scientist's subject."[208] According to the theory, lawmakers are not entirely driven (or maybe not at all) by their principles, but instead respond to personal incentives—notably the desire to get reelected—in deciding what laws to enact.[209] One strand of public choice focuses on interest groups, political actors who come together to try to sway legislators toward a particular outcome that advances the group's interests as a means to overcome difficult collective action problems.[210]

---

205. Cameron Kerry, Commentary, *Will California be the Death of National Privacy Legislation?*, BROOKINGS (Nov. 18, 2022), https://www.brookings.edu/articles/will-california-be-the-death-of-national-privacy-legislation/.

206. For example, APRA carved out exceptions to its broad preemption provision for some focused privacy state laws. American Privacy Rights Act of 2024, H.R. 8818, 118th Cong., § 20 (2024) (providing exceptions for preemption to, among others, "laws that protect the privacy of health information, healthcare information, medical information, medical records, HIV status, or HIV testing" and "laws that address banking records, financial records, tax records, social security numbers, credit cards, identity theft, credit reporting and investigations, credit repair, credit clinics, or check-cashing services").

207. *Infra* Part IV.C.

208. DANIEL A. FARBER & PHILIP P. FRICKEY, LAW AND PUBLIC CHOICE: A CRITICAL INTRODUCTION 1 (1991).

209. Derek E. Bambauer, *Everything You Want: The Paradox of Customized Intellectual Property Regimes*, 39 BERKELEY TECH. L.J. 205, 220–21 (2024).

210. Aaron Burstein, Will Thomas DeVries & Peter S. Menell, *Foreword: The Rise of Internet Interest Group Politics*, 19 BERKELEY TECH. L.J. 1, 7 (2004).

Public choice theory has spurred different methodological approaches to describing the incentives and actions of interest groups. Owing to its origins in economics, some public choice scholars model the game theoretic choices of interest groups and legislators.[211] More frequently, scholars use a less formal approach, recounting examples of interest group politics in a particular field from the past to reveal underlying incentives and forecast future behaviors. This latter method is how we will investigate how interest groups respond to omnibus and narrower privacy proposals.

Older works have chronicled the development of prior privacy legislation at the federal and state levels.[212] Much of this work focused on the inordinate control wielded by private interests that seek to weaken privacy legislation because they benefit from the unimpeded flow of information.[213]

The debate over an omnibus law invites all industry interest groups to take part. No company or sector can afford to ignore the opportunity to influence the shape or prospects of an omnibus bill. All companies, large and small, will be governed by an omnibus law, and all companies have much to lose from onerous compliance costs or threats to their business models.

The evidence supports this theory.[214] The tech industry—and especially the giant platforms—invest heavily whenever omnibus privacy legislation is considered.[215] Not only do the companies lobby individually, but every tech giant also participates in multiple trade associations that similarly participate in the debates over omnibus privacy laws.[216]

In contrast, the debate over a focused law might attract less corporate lobbying.[217] Companies that rely heavily on the specific use or category of

211. *See* Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041, 2055 (2000).

212. PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY (1995).

213. *Id.* at xii ("[T]he interests opposed to privacy protections were better organized and had greater resources and were therefore successful at delaying and weakening legislation.").

214. Jake Snow, *Big Tech Is Trying to Burn Privacy to the Ground-And They're Using Big Tobacco's Strategy to Do It*, TECH POLICY PRESS (Oct. 9, 2024), https://www.techpolicy.press/big-tech-is-trying-to-burn-privacy-to-the-ground-and-theyre-using-big-tobaccos-strategy-to-do-it/.

215. *See* Alfred Ng, *Privacy Bill Triggers Lobbying Surge by Data Brokers*, POLITICO (Aug. 28, 2022), https://www.politico.com/news/2022/08/28/privacy-bill-triggers-lobbying-surge-by-data-brokers-00052958.

216. *See* Sam Sabin, *In Early Days of Democrats' Antitrust Agenda, Big Tech's Trade Associations Could Play an Outsized Role*, MORNING CONSULT (Mar. 25, 2021), https://pro.morningconsult.com/articles/big-tech-antitrust-lobbying-trade-associations.

217. *See* Nissenbaum, Strandburg & Viljoen, *supra* note 12, at 1260 ("Omnibus privacy laws also have to cover so much (and invite lobbying from so many sectors), that they may end up with watered-down, lowest-common-denominator provisions.").

sensitive information under consideration may rationally invest the most, while other companies might spend their lobbying funds on other issues.

Public choice theory also examines the role of civil society groups in the legislative process.[218] Civil society groups have long been a major force in moving legislatures to enact privacy laws.[219] Recently, several scholars have noted that civil society groups that focus on technology policy have assumed an even more central role as they have grown in size, expertise, resources, and influence in DC and state capitols.[220] This commentary finds much to both praise and criticize in civil society's privacy law track record. Many flattering portraits have emerged chronicling the success of civil society groups led by Alastair Mactaggart in enacting the CCPA in California, which in turn inspired other laws in other states.[221] At the same time, in some of the postmortems dissecting why the ADPPA failed in the last Congress, a few scholars have placed blame on the priorities and strategies of civil society.[222]

My theory is that the omnibus framing distorts who among the civil society organizations can and will dedicate their scarce resources towards trying to shape legislation. By activating every corporate actor, especially the giant platforms, omnibus privacy laws raise the price tag of civil society participation. None but the most well-funded stand a chance to match industry's lobbying scale.[223] Civil society responds by building coalitions.[224] This response has several negative repercussions. First, coalitions tend to be

218. *See id.*

219. REGAN, *supra* note 212.

220. Ari Waldman, Compromised Advocates: Civil Society and the Future of Privacy Law (unpublished manuscript on file with author); Brenda Dvoskin, *Representation Without Elections: Civil Society Participation as a Remedy for the Democratic Deficits of Online Speech Governance*, 67 VILL. L. REV. 447, 501 (2022).

221. Nicholas Confessore, *The Unlikely Activists Who Took on Silicon Valley—and Won*, N.Y. TIMES MAG. (Aug. 14, 2018), https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html.

222. Ari Waldman, *Civil Society and the Crisis of Privacy Law*, 74 EMORY L.J. (forthcoming 2025) (on file with author) (explaining the central role of nonprofit advocates' in drafting the America Data Privacy Protection Act, and quoting an advocate in saying that nonprofit advocates play a "unique" role in advocating for policy positions due to their perceived status as experts); Laura Moy, *The Mysterious Case of Missing Laws: Solving the U.S. Privacy Puzzle* (forthcoming) (on file with author).

223. Mariano-Florentino Cuéllar & Aziz Z. Huq, *Privacy's Political Economy and the State of Machine Learning: An Essay in Honor of Stephen J. Schulhofer*, 76 N.Y.U. ANN. SURV. AM. L. 317, 340 (2021) (discussing the lobbying activities of Google and Facebook).

224. *E.g.*, Eric Null & Samir Jain, CDT Joins 45+ Orgs in Letter Urging Congress to Protect Americans' Privacy and Bring American Data Privacy and Protection Act to Vote, CTR. DEMOCRACY & TECH. (Aug. 25, 2022), https://cdt.org/insights/cdt-joins-45-orgs-in-letter-urging-congress-to-protect-americans-privacy-and-bring-american-data-privacy-and-protection-act-to-vote-adppa/.

led by large and well-funded organizations who often (with notable exceptions) achieve their scale and influence by accepting corporate funding. This gives less of a voice to civil society groups that refuse such entanglements. Second, a coalition will adopt a single strategy, embracing a set of substantive and strategic approaches that all members of the coalition can agree to. Adopting a single strategy leaves out idiosyncratic approaches held only by a few members. This might, for example, cause groups to abandon radical positions to try to appease more centrist or moderate views in the name of broadening the coalition's big tent approach.

All of these dynamics might deter some civil society groups from participating in debates over omnibus privacy legislation. Groups that do not place privacy or data at the center of their missions might sit out. Many groups focused on civil rights or specifically on particular marginalized populations might do little else than sign coalition letters organized by a privacy organization. Similarly, groups that prioritize radical change over centrist politics and iterative improvements might find no space for their views in broad-based privacy coalitions.

In contrast, debates over narrower proposals might activate additional groups that may not see themselves as primarily focused or even particularly interested in information privacy law. There are many examples of narrow proposals that have seen the significant involvement of particular advocacy groups. COPPA rulemakings attract participation from children's rights organizations.[225] The broadband privacy rulemaking in the FCC saw contributions from groups such as Public Knowledge and Free Press, which are better known for their focus on intellectual property and telecommunications policy.[226] Proposals to address algorithmic discrimination in policing and housing have attracted civil rights groups without a long track record for focusing on information privacy law.[227]

225. *E.g.*, *Children's Advocates Urge the Federal Trade Commission to Enact 21st Century Privacy Protections for Children*, CTR. FOR DIGIT. DEMOCRACY (Mar. 12, 2024), https://democraticmedia.org/publishings/children-s-advocates-urge-the-federal-trade-commission-to-enact-21st-century-privacy-protections-for-children.

226. *About Us*, PUBLIC KNOWLEDGE (last visited Mar. 3, 2025) ("Public Knowledge works at the intersection of copyright, telecommunications, and internet law, at a time when these fields are converging."), https://publicknowledge.org/about-us/; *About*, FREE PRESS (last visited Mar. 3, 2025) ("Free Press closely watches as the decisions shaping the media landscape are made and sounds the alarm when people's rights to connect and communicate are in danger."), https://www.freepress.net/about.

227. *E.g.*, *Reflections on Civil Rights and Our AI Future*, THE LEADERSHIP CONFERENCE ON CIVIL AND HUMAN RIGHTS (Apr. 18, 2023), https://civilrights.org/blog/reflections-on-civil-rights-and-our-ai-future/; *Resolution: Ensuring Representation and Eliminating Bias in Artificial*

This echoes now-Commissioner Bedoya's argument in 2018 against pursuing omnibus privacy reform in Congress. Instead, he argued:

> Let's make this a debate about people and pass laws to address the threats they actually face. Let's talk about the people who are still stalked every year through their smartphones. Or how retailers secretly use face recognition to spot shoplifters, even though the technology misfires more often when trying to identify African-Americans and women. Let's make this a debate about how Facebook tracked people to determine if they had an "affinity" for African-Americans, Hispanics and Asians, and then let advertisers block those people from seeing real estate ads.[228]

Commissioner Bedoya's comments also speak to the possibility of engaging the public directly. Debates over omnibus laws tend to be elite affairs between experts. A focused law on, say, reproductive health information or children's privacy may speak more directly to nonexpert citizens and their representatives. This participation can help ground and legitimate privacy discourse.

The same political dynamics and forces that make sensitivity-focused laws easier to enact will also make them easier to amend. Omnibus laws get enacted only as grand compromises between all interested industries through negotiation and horse trading. Once these deals are struck, amending that law will again require everybody affected to agree. This is likely to be extremely difficult to do, leading to ossification and making it harder to respond to technological and social change.[229] As a result, many important online privacy laws were enacted decades ago, long before the rise of smartphones, social media, the internet of things, or generative AI.[230]

Privacy laws drawn along sensitivities and uses may also be more attentive to the needs and interests of specific communities. Consider the way the Supreme Court's decision in *Dobbs* to overrule *Roe v. Wade*'s constitutional

Intelligence, NAACP (last visited Mar. 3, 2025), https://naacp.org/resources/ensuring-representation-and-eliminating-bias-artificial-intelligence.

228. Bedoya, *supra* note 92.

229. "The risk of ossification following enactment of a federal omnibus privacy law is also great. Such an omnibus law, like the NLRA, would be difficult to amend—industry, privacy advocates, and other parties may be able to muster enough congressional support to block any significant changes to it." Schwartz, *supra* note 8, at 928.

230. *E.g.*, *Modernizing the Electronic Communications Privacy Act* (ECPA), ACLU (last visited July 1, 2024), https://www.aclu.org/issues/privacy-technology/internet-privacy/modernizing-electronic-communications-privacy-act-ecpa.

guarantee of access to abortion has spurred attention to the data that can be used to conduct surveillance to support new abortion restrictions.[231]

D. AS APPLIED TO USE-FOCUSED AND SENSITIVITY-FOCUSED LAWS

Both use-focused and sensitivity-focused laws will advance the three institutional arguments offered above: the division of responsibility between legislatures and agencies, privacy federalism, and public choice. Again, there are slight differences in the suitability of the two approaches for each of these.

As stated earlier, sensitivity-focused laws give a bit more prescriptive control to the legislature than use-focused laws.[232] In contrast, from an institutional selection point of view, a use-focused law has some similarity to an omnibus law: it applies to all categories of information that might be subject to the specified use, giving companies the opportunity in the first instance to decide what information is covered. If a legislature is trying to avoid over-deferring to the interpretative choices of companies and agencies, it might prefer the sensitivity-focused route.

Moreover, if the concern is the Supreme Court's stripping of agency deference in *Loper Bright*,[233] sensitivity-focused laws will probably tend to be more detailed, less ambiguous, and thus more prescriptive statutory instructions for agencies, which may make them less resistant to constitutional attack.

Viewed through a pro-federalism lens, either approach seems as good as the other. State legislatures are well positioned to write either kind of law and state agencies are well positioned to enforce either kind of law. In fact, to best serve the laboratories of democracy, different states ought to experiment with writing both kinds of law. Their experience would give us concrete evidence about the relative strengths and weaknesses of the two approaches.

Finally, either approach can give rise to the public choice benefits of narrowed politics. Google may choose to spend less of its formidable lobbying budget opposing new privacy protections for reproductive health information or algorithmic decision-making than it would for a bet-the-company omnibus proposal. What will likely matter most in a company's response to a focused law is how closely the regulated category of information or use implicates the

231. Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228 (2022). *See* Huq & Wexler, *supra* note 23; Suzanne Bernstein, *The Role of Digital Privacy in Ensuring Access to Abortion and Reproductive Health Care in Post-Dobbs America*, ELEC. PRIV. INFO. CTR. (June 13, 2024), https://epic.org/the-role-of-digital-privacy-in-ensuring-access-to-abortion-and-reproductive-health-care-in-post-dobbs-america/.

232. *Supra* Part V.E.

233. Loper Bright Enters. v. Raimondo, 603 U.S. 369 (2024).

core business model of each company. A use-focused law targeting digital advertising, say, might inspire fierce lobbying from companies that rely heavily on this source of revenue.

V. DESIGN INTERVENTION: RESHAPING THE INFORMATION ECONOMY

My third and final set of arguments advance the idea that our current privacy approaches assign too much unquestioned authority to private actors to design critical platform infrastructure. Focused laws should be seen as tools for reshaping these societally crucial platforms to increase harm prevention, accountability, and transparency. Laws can literally inscribe boundary lines on the organizational and data structures of private corporations and other important institutions such as standards bodies and government agencies. These tools are a way to distribute power and decision-making authority across a broad set of actors both inside and outside of regulated companies.

A. EMPOWERING AND DISEMPOWERING PRIVACY PROFESSIONALS

The idea that law can alter the very shape of companies, markets, products, and services is an old one, although not enough of this literature has been incorporated into privacy law scholarship. One rich vein is New Institutionalism, an interdisciplinary approach grounded in organizational sociology that attempts to illuminate the way social "institutions provide the frames that guide human action."[234] For example, one concept from New Institutionalism that has been imported repeatedly into legal scholarship is organizational "isomorphism," the observation that diverse organizations often end up bearing many structural similarities.[235]

In privacy law scholarship, New Institutionalism has most richly been applied in a series of important qualitative sociological studies of privacy professionals working inside companies.[236] Writing a decade ago, Ken Bamberger and Deirdre Mulligan argued that privacy law was best understood "on the ground."[237] Contradicting the conventional wisdom that the United States, in particular, had enacted weak privacy law "on the books," Bamberger and Mulligan found that companies in the United States tended to employ corporate Chief Privacy Officers and other privacy-focused executives and

234. Dan L. Burk, *On the Sociology of Patenting*, 101 MINN. L. REV. 421, 432 (2016).

235. *See* Paul J. DiMaggio & Walter W. Powell, The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields, 48 AM. SOC. REV. 147, 147 (1983).

236. *See*, *e.g.*, BAMBERGER & MULLIGAN, *supra* note 66; WALDMAN, *supra* note 21.

237. *Id.*

managers who had built rich and meaningful programs for privacy protection within their companies.[238]

The Bamberger and Mulligan studies are landmarks, and this Part builds on their novel insights and important qualitative data. Still, the idea that we should trust corporations guided by wise privacy officers to strike the right balance between corporate goals and the values and rights of the rest of us seemed implausible to me when Bamberger and Mulligan first wrote. We now have a decade of examples suggesting that the story they told is incomplete at best. Successive waves of developments since then, from Cambridge Analytica;[239] to market concentration (Facebook acquired Instagram in 2012 and WhatsApp in 2014);[240] to the damning revelations of whistleblower Frances Haugen;[241] to the disastrous turn Elon Musk has had owning and running Twitter (now X),[242] suggest that relying on companies to protect user privacy seems naïve in 2025 at best.

Ari Waldman later provided an important corrective to Bamberger and Mulligan's work. He extended their qualitative data to include interviews with additional privacy professionals and, crucially, ordinary staff in addition to executives.[243] He concluded that Bamberger and Mulligan had been overly optimistic about the ability employees possessed to protect user privacy in the face of constant pressure from corporate leadership to maximize revenue, growth, and shareholder value in ways that are at odds with some forms of privacy protections for users.[244] In particular, he described a tendency toward

238. *Id.*

239. Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, GUARDIAN (Mar. 17, 2018), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

240. Mark Glick, Catherine Ruetschlin & Darren Bush, *Big Tech's Buying Spree and the Failed Ideology of Competition Law*, 72 HASTINGS L.J. 465, 486–505 (2021).

241. In 2021, a whistleblower revealed internal Facebook documents to multiple press outlets. The first story published was by the Wall Street Journal. Jeff Horwitz, *Facebook Says Its Rules Apply to All. Company Documents Reveal a Secret Elite That's Exempt.*, WALL ST. J. (Sept. 13, 2021), https://www.wsj.com/articles/facebook-files-xcheck-zuckerberg-elite-rules-11631541353 (first in series). A month later, the whistleblower was revealed to be a former Facebook product manager named Frances Haugen. Ryan Mac, *Who Is Frances Haugen, the Facebook Whistle-Blower?*, N.Y. TIMES (Oct. 5, 2021), https://www.nytimes.com/2021/10/05/technology/who-is-frances-haugen.html.

242. KATE CONGER & RYAN MAC, CHARACTER LIMIT: HOW ELON MUSK DESTROYED TWITTER (2024).

243. *See* WALDMAN, *supra* note 21, at 4–5.

244. *Id.* at 118.

"managerialism," meaning activities that sacrifice privacy protection in favor of revenue generation.[245]

Regardless of their differences, Waldman, Bamberger and Mulligan all recognize that law is a powerful force for empowering—or stymieing—the work of privacy professionals. Once again, this builds on the literature on isomorphism, the tendency for companies to come up with similar structures.[246] This literature describes "coercive isomorphism," which occurs when external rules trigger similar responses from regulated companies, leading them to make similar changes to their practices and organizational structures.[247]

B. HOW OMNIBUS AND FOCUSED PRIVACY LAWS RESHAPE DIFFERENTLY

Although Bamberger and Mulligan looked beyond "privacy on the books," they identified some characteristics of U.S. privacy law that helped bring about the kind of privacy practices that exist in the United States.[248] As we flip the script and see many of those "successful" practices in 2012 as failures in 2024, we now can review some of them as cautionary tales. I argue that any new omnibus federal privacy law we are likely to enact would possess many of these features and thus would do nothing to reverse the managerial tendencies that Waldman identifies.

Bamberger and Mulligan connected the power of CPOs to the open-textured and non-prescriptive privacy laws in the United States.[249] They applauded "ambiguity with accountability," which is provided by open-textured and productively ambiguous laws.[250] Some of the CPOs they interviewed focused specifically on the famously open-ended and sweeping FTC Act as a key example of productive ambiguity, which gave them the ammunition they needed to argue for the value of privacy without saddling them with detailed prescriptive rules.[251]

Perhaps this analysis had it exactly backwards. Waldman's conclusion about the tendency of corporate privacy professionals to lose internal debates suggests that their efforts may have been hampered rather than helped by the United States' open-textured privacy laws.[252] Bamberger and Mulligan may

245. *Id.*
246. DiMaggio & Powell, *supra* note 235, at 147.
247. *Id.*
248. BAMBERGER & MULLIGAN, *supra* note 66, at 68–73.
249. *Id.* at 224.
250. *Id.*
251. *Id.* at 226.
252. WALDMAN, *supra* note 21, at 87–90.

have mistaken flexibility for power. Broad and ambiguous laws give CPOs voice but not direction. Waldman chronicles several strategies companies use to stifle pro-privacy arguments.[253] In the face of these, privacy professionals need to be able to point to concrete, specific, and credible threats of legal sanction to push back against other corporate goals.[254] In other words, privacy professionals may need a law that says, "take these specific actions or suffer the consequences" to empower these workers, rather than an omnibus law that announces merely that "privacy is very important."[255]

C. RESHAPING CORPORATIONS AND THEIR PRODUCTS AND SERVICES

I argue that narrow privacy laws will empower privacy professionals within firms while providing more specific guidance and a narrower remit for what these professionals are meant to do to protect privacy. One goal for these laws is to provide a source of beneficial friction.[256] With the right type of laws, privacy professionals can be made gatekeepers and sources of bureaucratic friction. A firm that wants to process the kind of personal data or the kind of specific use governed by the law will encounter the cost of dealing with that expert, that part of the bureaucracy, or that point of friction. That friction might be a roadblock or a speed bump, depending on the content of the law, the power given to the expert, and how the expert chooses to wield it. Still, the friction will nevertheless begin to manifest, even if it does so in accordance with the specific shape of the institution around it.

What ought these narrower laws empower these privacy professionals to do? Given the manifest dysfunctions of the information economy,[257] we should use focused privacy laws to begin to reshape these companies and the platforms, services, and products they provide. Since one of the motivating goals of focusing privacy law is to attend to context,[258] there are necessary limits to what we can generally say about how to reshape companies. The reshaping work that can and should be accomplished will depend on context. The necessary reshaping work of, say, a precise geolocation privacy law will differ from that needed in an algorithmic discrimination law. Fully illuminating

253. *Id.* at 145–48.

254. *Id.* at 237–45.

255. *Id.* at 76–78.

256. *See* Paul Ohm & Jonathan Frankle, *Desirable Inefficiency*, 70 FLA. L. REV. 777 (2018); Brett M. Frischmann & Susan Benesch, *Friction-In-Design Regulation as 21st Century Time, Place, and Manner Restriction*, 25 YALE J.L. & TECH. 376 (2023); Ayelet Gordon-Tapiero, Paul Ohm & Ashwin Ramaswami, *Fact and Friction: A Case Study in the Fight Against False News*, 57 U.C. DAVIS L. REV. 171 (2023).

257. *Supra* Part I.

258. *Supra* Part III.C.

these mechanisms is an important new research agenda to be developed in later work.

Speaking generally for now, privacy laws can reshape the deals and relationships between firms, the internal structure of firms, and the design of the products and services they produce. Specifically, privacy law can divide and separate, slashing borders or boundaries between companies, departments, workers, products, and services. In other work with Brett Frischmann, I have explored the role of *governance seams*.[259] Governance seams are "socially constructed boundaries, borders, and interfaces" that harness what we call "friction-in-design."[260] This is beneficial friction, not the hated friction that is the bane of most economic and design discourse. Friction gives time for human-scale decision-making and governance seams provide a locus of space for governance activities such as monitoring and control.[261]

For example, a sensitivity-focused or use-focused privacy law might give privacy professionals the power they need to slash a governance seam across the org chart, designating one company lawyer the authority on issues around a category of information or use. A precise geolocation privacy law might lead to a gatekeeper who must approve all product team requests to access a user's physical movements. They might sequester the work of a specific team, the only team empowered to access such data.

Privacy law may lead to reshaping products and services as well as org charts and deals. Many scholars from various disciplines have investigated connections between design and values. Leading the way, Science and Technology Studies (STS) scholars have long interrogated how the design of technological artifacts advance or impede particular human values.[262] Legal scholars have built on this STS foundation to explain how law and legal institutions can play a key role in encouraging value-sensitive design.[263] Woody Hartzog has encouraged legislators and regulators to nudge technology companies to design online services that better respect user privacy.[264] Privacy

259. Frischmann & Ohm, *supra* note 35.

260. *Id.* at 1118.

261. *Id.*; *see also* works cited *supra* note 256.

262. Langdon Winner, *Do Artifacts Have Politics?*, 109 DAEDALUS 121, 122–23, (Winter 1980); *see also*, *e.g.*, Mary Flanagan, Daniel C. Howe & Helen Nissenbaum, *Embodying Values in Technology: Theory and Practice*, *in* INFORMATION TECHNOLOGY AND MORAL PHILOSOPHY 322 (Jeroen van den Hoven & John Weckert eds., 2008); BATYA FRIEDMAN & DAVID G. HENDRY, VALUE SENSITIVE DESIGN: SHAPING TECHNOLOGY WITH MORAL IMAGINATION (2019).

263. HARTZOG, *supra* note 137; WALDMAN, *supra* note 21.

264. HARTZOG, *supra* note 137.

laws have long incorporated the goal of "privacy-by-design."[265] Scholars in computer science[266] and business[267] have similarly studied the connections between design and values.

Focused laws may carve governance seams in the very design of digital systems. Sensitive information regulation might literally cause a company to split a database into two halves, the half that has not been deemed sensitive, and the sensitive half. Some organizations may leave data fields deemed relatively nonsensitive in databases that are broadly accessible within the firm, while limiting access to the tables that contain, for example, health diagnoses, sexual orientation, or precise geolocation information.

I am not arguing that any law that reshapes a company is necessarily a good thing nor that every governance seam or point of friction is beneficial. But I do argue that focused privacy laws will tend to lead to beneficial targeted friction because the governance seams that they draw would not be selected arbitrarily. As Part III explained, categories of sensitive information and use are selected due to their connection to harms and violations of civil rights, so the lines they inscribe can do important protective and value-laden work. For example, laws on protecting precise geolocation information can be designed to privilege the freedom of movement and association, laws that prohibit nonconsensual releases of intimate imagery can advance sexual liberty and intimacy, and laws that limit the amount of information gathered from children can protect children.

D. EXPANDING WHO GETS TO PARTICIPATE

The identity and experience of these empowered internal gatekeepers may matter as much as the work they do to reshape their organizations. For example, a listing for a job to superintend the handling of race or ethnicity information might attract applicants with prior work experience or coursework focused on race and ethnicity. Similarly, special handling rules around sexual

265. ANN CAVOUKIAN, PRIVACY BY DESIGN IN LAW, POLICY AND PRACTICE: A WHITE PAPER FOR REGULATORS, DECISION-MAKERS AND POLICY-MAKERS 26 (2011); ANN CAVOUKIAN, PRIVACY BY DESIGN: THE 7 FOUNDATIONAL PRINCIPLES: IMPLEMENTATION AND MAPPING OF FAIR INFORMATION PRACTICES 1, 4 (2009), https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf.

266. Computer scientists have coined a rule called "Conway's Law," that suggests that the design of a system reflects the communications structure of the organization that created it. Melvin E. Conway, *How Do Committees Invent?*, DATAMATION MAGAZINE (April 1968), https://www.melconway.com/Home/Committees_Paper.html.

267. Wafa Ben Khaled & Jean-Pascal Gond, *How Do External Regulations Shape the Design of Ethical Tools in Organisations? An Open Polity and Sociology of Compliance Perspective*, 73 HUM. RELS. 653, 658–59 (2019) (suggesting regulations that mandate ethical behavior led to the creation of "ethical tools" within those organizations).

orientation might privilege those who have focused on sexual orientation. This might literally mean a more diverse workforce on the theory that people who specialize in issues surrounding a particular identity group are more likely to be a member of that group. More broadly, it might privilege prior experience or training that otherwise would be seen as neutral or unhelpful in large tech companies.

I contend that a root cause of our dysfunctional system of surveillance capitalism is that too much power is held by too few. Not only does a narrow class of global society—mostly men in their 20s and 30s living in a few zip codes in Northern California and around Seattle—control a major percentage of economic activity, but they also shape platforms that dictate the conditions of core civic life: from speech to education to work to play to family to community to opportunity. Focused privacy laws can thus help break the monopoly on design currently being held by too few people working for too few companies.

E. AS APPLIED TO USE-FOCUSED AND SENSITIVITY-FOCUSED LAWS

Perhaps more than with the harm reduction and institution selection arguments, the design intervention argument plays out differently for use-focused and sensitivity-focused privacy laws. Once again, this results from the relatively better precision of sensitivity-focused laws and the concomitantly relative increased flexibility of use-focused ones. Both types of laws will reshape the activities and org charts of companies, but because sensitivity-focused laws tend to draw brighter lines than use-focused laws, the former will give the legislature more precise platform reshaping control than the latter.

Consider biometric privacy laws like BIPA.[268] There are two ways to define the target of a biometric privacy law: it might protect all biometric identifiers,[269] a sensitivity-focused approach, or it might regulate the act of using information to identify a person, a use-focused approach.[270]

The sensitivity-focused approach lets the legislature play a more detailed and prescriptive role in design interventions. It forces companies to find, label, and specially handle a category of information: faceprints and other biometric information.[271] It leads more directly to specific governance seams in databases and org charts.

268. Illinois Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. 14/5 (2008).

269. *Id.* at 14/10 (defining "biometric identifier," a sensitivity-focused term).

270. *Id.* (defining "biometric information," a use-focused term).

271. *Id.* at 14/15 (setting forth BIPA requirements for "a private entity in possession of biometric identifiers or biometric information").

The use-focused approach defers more to company prerogatives in its reshaping activities. A company that collects faceprint information for some reason other than identification would feel less of the legislature's prescriptive design intervention than from the sensitivity-focused law. For example, companies have criticized BIPA because it constrains their ability to use faceprints for non-identifying purposes.[272]

If the goal of the legislature is to prescribe specific governance seams[273]—particularized cleavages in a database or org chart—a sensitivity-focused law is a more precise and controllable tool.

VI. CRAFTING EFFECTIVE FOCUSED PRIVACY LAWS

The central goal of this Article is to articulate the *why* for encouraging legislatures to enact focused privacy laws. We need to shift attention and energy away from omnibus proposals in favor of new sensitivity-focused and use-focused laws. This final, brief Part suggests some practical *how* and *what* considerations as we undertake this work.

A. FOCUS ON USE OR SENSITIVITY?

Most of the arguments support either use-focused or sensitivity-focused privacy laws. Either of these would be an improvement on the omnibus status quo, and both should be on the agenda for future federal and state lawmaking. But as we have encountered throughout, there are some differences in the two approaches.

1. What If Everything Is Sensitive?

Some have raised an argument against sensitivity-focused privacy laws: the problem of inference.[274] They have argued that because machine learning techniques excel at inferring sensitive fact X from nonsensitive fact Y, then any attempt to regulate X is difficult, overprotective and underprotective, or

272. One (somewhat trivial) example is the ability for photo editing and video conferencing apps to offer face filters that turn people into cartoons and animations. Christina Lamoureux, *AI Avatar App Is the Latest Target of BIPA Class Action Litigation*, NAT'L L. REV. (Mar. 1, 2023), https://natlawreview.com/article/ai-avatar-app-latest-target-bipa-class-action-litigation (describing BIPA lawsuit against Lensa).

273. *See supra* Part V.C.

274. In addition to Dan Solove, whose arguments will be addressed presently, others who have made this argument include Müge Fazlioglu, *Beyond the 'Nature' of Data: Obstacles to Protecting Sensitive Information in the European Union and the United States*, 46 FORDHAM URB. L.J. 271, 296 (2019); George R. Milne, George Pettinico, Fatima M. Hajjat & Ereni Markos, *Information Sensitivity Typology: Mapping the Degree and Type of Risk Consumers Perceive in Personal Data Sharing*, 51 J. CONSUMER AFFS. 133, 134–36 (2017).

even arbitrary and fundamentally incoherent.[275] These arguments oversell the strength of inference, fail to recognize ways to draft these laws to account for inference, and in general fall prey to a dangerous style of AI-related rhetoric.

It is undeniably true that, thanks to the power of machine learning inference, a data controller may be able to infer something sensitive about a data subject—say their sexual orientation, religion, or health diagnosis—from something seemingly unrelated and nonsensitive—say their consumer purchase history or the shape of their social network.[276] This power poses a challenge to the concept of sensitive information as a stable category.[277] If a law applies special rules to information based on sensitivity, its coverage will change over time.[278] Because the power of inference tends to grow and not shrink, it means that sensitivity-focused privacy laws will expand over time.[279] With every technological advance, a law will cover more data and may cover more companies and more commercial activity. For companies regulated by a sensitivity-focused law, tracking the law's coverage will require tracking the state-of-the-art of inferential capability, a complex undertaking that place expensive burdens on all companies and a disproportionate burden on smaller and less well-resourced companies.

Following this line of thinking, Dan Solove has offered a full-throated argument against laws that draw distinctions based on sensitive information.[280] Solove argues that the idea of sensitive information lacks coherence because machine learning techniques can help a data analyst infer sensitive information from seemingly nonsensitive information.[281]

In offering this critique, Solove contrasts sensitive information from the category of "personal data," something he and many others have written about in earlier work.[282] This comparison undermines his argument. Personal data has also proven to be a slippery and ever-expanding category due to the very same power of inference, yet Solove fails to account for how this similarity undermines his expansionist fears about sensitive information. If all information is (or soon will be) sensitive information because of advances in

275. Solove, *supra* note 18, at 1099.
276. Solow-Niederman, *supra* note 54, at 378.
277. Solove, *supra* note 18, at 1111–15.
278. *Id.* at 1109.
279. *Id.*
280. *Id.* at 1099.
281. *Id.*
282. Solove, *supra* note 18, at 1086 (citing 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, 1828–36 (2011)).

the power of inference, then all information will also be personal information through the very same mechanism.

Solove's earlier work (with Paul Schwartz) attempted to save personal data from the critique about its expansive nature by focusing attention on the *identifiability* of data.[283] Some data does not alone identify an individual, but it may be intentionally combined with other data to infer identity. Legislatures around the world have followed this lead, crafting new laws that cover both identified and identifiable data.[284] These definitions turn on the intent and actions of the data controller. This means that the scope of these laws increases over time. It also means that regulated entities can control the coverage of these laws, for example by declining to combine data sets that would together reveal identity or by stripping certain readily identifiable information out of data sets.

Solove does not explain why this exact same approach cannot work for categories of sensitive information. Some sensitive information—a database containing sex assigned at birth, health diagnoses, or race, to name a few—would be intrinsically sensitive and therefore covered. Other information that might, in combination with other information, be used to infer sensitive information about an individual is not covered in the first instance. But, just as with personal data, we might consider such information as "revealing" sensitive information rather than intrinsically sensitive information, setting up the same gradation of coverage as we have with personal data.[285] This is how several sensitive provisions within omnibus laws would address this problem.

Just as with personal data, we should not consider information to be sensitive information due solely to a theoretical possibility of the drawing of an inference. If a law is crafted according to these principles, we can adequately address the concerns about the difficulty companies will face in tracking the

283. Solove & Schwartz, *supra* note 282, at 1828.

284. *E.g.*, GDPR, *supra* note 4, art. 4(1) ("'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly").

285. *See, e.g.*, GDPR, *supra* note 4, art. 9(1); Case C-184/20, OT v. Vyriausioji tarnybinės etikos komisija, ECLI:EU:C:2022:601, ¶ 119 (Aug. 1, 2022) ("[A]lthough the personal data the publication of which is mandatory pursuant to [a challenged provision of Lithuanian law] on the reconciliation of interests are not, inherently, sensitive data for the purpose of Directive 95/46 and the GDPR, the referring court takes the view that it is possible to deduce from the name-specific data relating to the spouse, cohabitee or partner of the declarant certain information concerning the sex life or sexual orientation of the declarant and his or her spouse, cohabitee or partner."); Colorado Privacy Act, COLO. REV. STAT. § 6-1-1303(24) ("Sensitive Data" means "personal data *revealing*" a list of sensitive information categories) (emphasis added); Colorado Privacy Act Rules, 4 CCR-904-3 Rule 2.02 ("'Revealing" as referred to in C.R.S. § 6-1-1303(24)(a) includes Sensitive Data Inferences.").

growing power of inference. Just as companies are already obligated to know when information they might deem nonidentifying has become identifying, so too can they track new advances in sensitivity. If this seems too daunting, we can task institutions with tracking these advances. A regulator can promulgate lists of inferential sensitivity. Standards bodies, civil society groups, and academics can release reports with tables summarizing these advances.

B. WHERE TO START

A good start would be to enact a new federal law limiting the collection, distribution, and use of precise geolocation, such as cell site information and GPS information collected by smartphones.

Following Citron, we should also enact a law protecting "intimate data."[286] She defines this quite broadly as "data about our bodies, health, sex, gender, sexual orientation, close relationships, online searches, reading habits, and private communications."[287] This definition may prove too broad for a sensitivity-focused privacy law, and we might carve off the final three categories under a separate law protecting "intellectual privacy."[288]

Another law long overdue, at least at the federal level, is a law focused on the special problem of facial recognition. We can look to the laboratory of states laws that have already enacted different types of facial recognition laws, ranging from outright bans for some purposes to risk-based regulation.[289]

Congress has already been pursuing a focused law to protect the privacy and mental health of children, inspired by a set of revelations about how Meta has ignored internal research suggesting that its services were harming young users. In summer 2024, the Senate advanced two such laws, the Kids Online Safety Act[290] and the Children's Online Privacy Protection Act 2.0.[291]

A fourth law would respond to concerns in the wake of *Dobbs* that sensitive information would be used to track people seeking abortions and their doctors and other medical professionals and caregivers.[292] Faced with a credible threat from state law enforcement agencies and plaintiffs' groups to target people

286. CITRON, *supra* note 22, at 156.

287. *Id.*

288. *See* RICHARDS, *supra* note 22, at 160 (calling for new regulations to protect "information about intellectual activity").

289. Jake Laperruque, *Status of State Laws on Facial Recognition Surveillance: Continued Progress and Smart Innovations*, TECH POLICY PRESS (Jan. 6, 2025), https://www.techpolicy.press/status-of-state-laws-on-facial-recognition-surveillance-continued-progress-and-smart-innovations/.

290. Kids Online Safety Act, S. 1409, 118th Cong. (2024).

291. Children and Teens' Online Privacy Protection Act, S. 1418, 118th Cong. (2024).

292. *See* Huq & Wexler, *supra* note 23, at 576–77.

who have sought, obtained, and helped others obtain medical care, we should implement protections for the information that might aid such efforts.[293]

Finally, we also need to rehabilitate our sectoral privacy laws. Congress should be working on a new HIPAA that applies to all holders of health information, a new FERPA that covers education services and providers that don't fall within the old statute's narrower definitions, and a financial privacy law that covers any company that holds financial information, not just banks.

C. WHAT THIS MEANS FOR OMNIBUS PRIVACY LAWS

As we focus on narrower privacy laws, we should redirect some of our energy away from enacting omnibus privacy laws. Because focused privacy laws, by definition, do not cover every use and piece of personal data, we should continue to strive to enact an omnibus privacy law that provides universal ground rules, but we should overlay it with focused laws providing more meaningful protections. We can enact these laws in any order: omnibus before focused or vice versa.

Once we understand that an omnibus privacy law will be one piece in an ensemble of protection, it might take the pressure off an omnibus law to try to do everything. Omnibus privacy laws should provide baseline Fair Information Practice Principles, such as providing users with rights of access, rectification, and data portability.[294] But focused privacy laws can provide more fine-grained protections for certain contexts. This might relieve some of the interest group opposition to omnibus efforts.

Congress might even consider sensitivity-focused laws to be experiments, pilot tests, or information gathering tools for a future omnibus law. New privacy laws focused on narrower categories of information can be used to develop key definitions or to experiment with novel compliance or enforcement mechanisms.

VII. CONCLUSION: IN DEFENSE OF PATCHWORKS

The turn to focused privacy laws turns a commonly deployed epithet against sectoral privacy laws into praise: they create patchworks. Patchworks bespeak arbitrariness, incoherence, and unnecessary complexity. Calling something a patchwork, at least when it comes to law or regulation, is to criticize its lack of a unifying, totalizing vision.

---

293. *Id.*

294. Robert Gellman, *Fair Information Practices: A Basic History* 1, 1–6 (Apr. 9, 2024), https://bobgellman.com/rg-docs/rg-FIPshistory.pdf (providing a history of the FIPPS).

We can rehabilitate the metaphor, because patchworks also sometimes describe beautiful, kaleidoscopic works of art. What matters is the skill of the patchwork designer and the care with which the patchwork is stitched together. In inferior hands, patchworks might be rough-hewn, ugly, and chaotic. When designed by artisans, they can be well thought-out and beautiful.

Patchworks—in both the regulatory and artistic senses—can also be the work of many hands. A patchwork quilt might be assembled by communities coming together, stitching something beautiful out of scraps. They can reflect federalism, with contributions from federal, state, and local government and governance; they can stitch together the contributions of many countries in a cohesive international regulatory regime.

The patchwork of privacy law becomes a patchworked information ecosystem.[295] The silk square of health information sits apart from the linen square of education records, both separated by lines of stitching from the wide expanse of flannel information held by an advertiser. Let us engage in a quilting bee of privacy law and blanket us all in the warmth and security of improved privacy protection.

295. *See* Solove, *supra* note 18, at 1083 ("Personal data is akin to a grand tapestry, with different types of data interwoven to a degree that makes it impossible to separate out the strands.").