UC DAVIS LAW REVIEW ONLINE

VOL. 55 AUGUST 2021

# The New Privacy Law

*Ari Ezra Waldman*[*]

*We are in a second wave of privacy law. The first wave was characterized by privacy policies, self-regulation, and notice and choice. But in the last three years, eleven proposals for comprehensive privacy legislation have been introduced in the United States Congress and forty have been introduced in the states. From the perspective of practice, almost all of these proposals are roughly the same: They guarantee individual rights to data and rely on internal corporate compliance for ongoing monitoring. This second wave of privacy law is undoubtedly different from the first, but how? This essay provides a taxonomy to understand changes in U.S. privacy law, distinguishing between two "waves" along three metrics: their practices, theories of governance, and underlying ideologies. A first wave was characterized by privacy policies, self-regulation, and limited regulatory*

 Professor of Law & Computer Science and Faculty Director, Center for Law, Information, and Creativity, Northeastern University. Ph.D., Columbia University; J.D., Harvard Law School; A.B., *magna cum laude*, Harvard College. Affiliate Scholar, Yale Law School Information Society Project. This essay benefited from comments from participants at several workshops, including ones hosted by Cornell Tech's Digital Life Initiative, New York University's Privacy Research Group, Northeastern University's Humanities Center, the University of Colorado School of Law, and Columbia University School of Law and Columbia University Department of Computer Science. Special thanks to Steve Bellovin, Michael Byrne, Danielle Keats Citron, Julie Cohen, Madiha Z. Choski, Woodrow Hartzog, Julie Holley, Margot Kaminski, Tomer Kenneth, Nathaniel Lubin, Helen Nissenbaum, Frank Pasquale, Katherine Strandburg, Daniel Solove, Thomas Streinz, Tyler Valeska, and Salome Vijoen. Daniel Davies provided essential research assistance. Any waves of errors are my own.

*enforcement. Its practices were focused on notice, its governance was self-regulatory, and its ideology was* laissez faire. *A second wave almost uniformly relies on rights and internal corporate compliance structures to manage data collection, processing, and use. Its practices are focused on compliance, its governance is managerial, and its underlying ideology is neoliberal. This taxonomy offers privacy law scholars a new way to understand and critique the current state of the field. The essay concludes with four research questions for scholars to pursue.*

TABLE OF CONTENTS

## INTRODUCTION

We are in the middle of privacy law's second wave.[1] Since 2018, eleven proposals for comprehensive privacy legislation have been introduced in Congress.[2] During that same time, two ballot initiatives and forty privacy bills have been introduced in twenty-eight states.[3] These proposals come in the wake of the General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act

[1] The "waves" terminology is borrowed from feminist theory. *See, e.g.*, Aya Gruber, *Neofeminism*, 50 HOUS. L. REV. 1325, 1331-45, 1372-90 (2013) (analyzing second wave "orthodoxies" and providing a third wave critique); Martha Minow, *Introduction: Finding Our Paradoxes, Affirming Our Beyond*, 24 HARV. C.R.-C.L. L. REV. 1, 1-3 (1989) (describing three "stage[s]" of feminism).

[2] *See* Consumer Data Privacy and Security Act of 2021 (CDPSA), S. 1494, 117th Cong. (2021); Data Care Act of 2021, S. 919, 117th Cong. (2021); Information Transparency & Personal Data Control Act of 2021, H.R. 1816, 117th Cong. (2021); Data Accountability and Transparency Act of 2020 (DATA), S. ___, 116th Cong. (2020) (distributed as discussion draft); Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act (SAFE DATA Act), S. 4626, 116th Cong. (2020); American Data Dissemination Act of 2019, S. 142, 116th Cong. (2019); Consumer Online Privacy Rights Act (COPRA), S. 2968, 116th Cong. (2019); Data Care Act of 2019, S. 2961, 116th Cong. (2019); Mind Your Own Business Act of 2019 (MYOBA), S. 2637, 116th Cong. (2019); Online Privacy Act of 2019, H.R. 4978, 116th Cong. (2019); Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019).

[3] *See* California Consumer Privacy Act of 2018 (CCPA), CAL. CIV. CODE § 1798.100-1798.199.100 (2021); California Privacy Rights Act of 2020 (codified as amended at CAL. CIV. CODE § 1798.100-1798.199.100); NEV. REV. STAT. § 603A.010-603A.360 (2021); H.R. 216, 2021 Leg., Reg. Sess. (Ala. 2021); S. 190, 73d Gen. Assemb., 1st Reg. Sess. (Colo. 2021); S. 893, 2021 Gen. Assemb., Jan. Sess. (Conn. 2021); H. 3910, 102d Gen. Assemb., 1st Reg. Sess. (Ill. 2021); S. 46, 192d Gen. Ct., Reg. Sess. (Mass. 2021); S. 567, 2021 Leg., 244th Reg. Sess. (N.Y. 2021); A. 6042, 2021 Leg., 244th Sess. (N.Y. 2021); S. 6701, 2021 Leg., 244th Reg. Sess. (N.Y. 2021); S. 569, 2021 Gen. Assemb., 2021 Sess. (N.C. 2021); H.R. 1126, 205th Gen. Assemb., 2021 Sess. (Pa. 2021); H.R. 3741, 87th Leg., Reg. Sess. (Tex. 2021); S. 1392, 2021 Gen. Assemb., 1st Spec. Sess. (Va. 2021); S. 5062, 67th Leg., Reg. Sess. (Wash. 2021); S. 1614, 54th Leg., 2d Reg. Sess. (Ariz. 2020); H.R. 2729, 54th Leg., 2d Reg. Sess. (Ariz. 2020); H.R. 963, 2020 Leg., 122d Reg. Sess. (Fla. 2020); S. 2330, 101st Gen. Assemb., 1st Reg. Sess. (Ill. 2020); H. 5603, 101st Gen. Assemb., 2d Reg. Sess. (Ill. 2020); H. 784, 2020 Gen. Assemb., 441st Sess. (Md. 2020); H. 1656, 2020 Gen. Assemb., 441st Sess. (Md. 2020); H.R. 3936, 91st Leg., 2d Reg. Sess. (Minn. 2020); L. 746, 106th Leg., 2d Reg. Sess. (Neb. 2020); H.R. 1236, 2020 Gen. Ct., 166th Sess. (N.H. 2020); A. 3255, 219th Leg., 1st Ann. Sess. (N.J. 2020); H.D. 473, 2020 Gen. Assemb., Reg. Sess. (Va. 2020); S. 418, 30th Leg., Reg. Sess. (Haw. 2019); S. 2263, 101st Gen. Assemb., 1st Reg. Sess. (Ill. 2019); S. 946, 129th Leg., 1st Reg. Sess. (Me. 2019); H.R. 1253, 2019 Leg., 2019 Reg. Sess. (Miss. 2019); S. 176, 54th Leg., 1st Sess. (N.M. 2019); S. 224, 2019 Leg., 242d Sess. (N.Y. 2019); S. 5642, 2019 Leg., 242d Sess. (N.Y. 2019); H.R. 1049, 203d Gen. Assemb., 2019 Sess. (Pa. 2019); S. 234, 2019 Gen. Assemb., Jan. Sess. (R.I. 2019); H.R. 4390, 86th Leg., Reg. Sess. (Tex. 2019); H.R. 4518, 86th Leg., Reg. Sess. (Tex. 2019); A. 2188, 219th Leg., 1st Ann. Sess. (N.J. 2018); S. 2834, 218th Leg., 1st Ann. Sess. (N.J. 2018).

("CCPA"), with more proposals likely on the way.[4] Remarkably, almost all of them look similar: they combine a series of individual rights with internal compliance structures in which industry is its own privacy governor.

To date, privacy law in the U.S. has been a combination of sector-specific federal statutes, Federal Trade Commission ("FTC") consent decrees, and a default transparency requirement known as notice-and-consent.[5] Among other practices, industry wrote and posted privacy policies, individuals were expected to read them, and regulators enforced the promises companies made themselves.[6] This is the regime of click-to-agree, opt-out consents, and long legalese privacy notices.[7] Governance was self-regulatory and classically liberal.[8] That was privacy law's first wave. Relative to the first, some scholars argue that new proposals reflect a "paradigm shift."[9]

Undoubtedly, the second wave is different from the first. It requires more than just notice and a button to click "Agree." It imposes more obligations on industry than the responsibility to write, post, and adhere to a privacy policy that no one reads. It adds practices like completing privacy impact assessments ("PIAs"), hiring chief privacy officers ("CPOs") and staffs, conducting audits, writing and adhering to industry codes of conduct, self-certifying compliance, keeping records and paper trails, automating compliance, and developing internal processes for adjudicating customer rights. But those differences,

[4] CCPA § 1798.100; Regulation 2016/679, of the European Parliament and of the Council of 27 Apr. 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, 2016 O.J. (L 119) 1 [hereinafter GDPR].

[5] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 600-06, 628-30 (2011).

[6] Various state laws required specific notices. *See, e.g.*, California Online Privacy Protection Act (CalOPPA), CAL. BUS. & PROF. CODE § 22575 (2021) (requiring any commercial websites or online services collecting information on California residents to "conspicuously" display a privacy policy with specific details); Delaware Online Privacy and Protection Act, DEL. CODE ANN. tit. 6, § 1205(c) (2021) (stating similar requirements as CalOPPA).

[7] *See* Joel R. Reidenberg, N. Cameron Russell, Alexander J. Callen, Sophia Qasir & Thomas B. Norton, *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 I/S: J. L. & POL'Y FOR INFO. SOC'Y 485, 490-96 (2015) (summarizing broad critiques of the notice-and-consent framework).

[8] *See* David Singh Grewal & Jedediah Purdy, *Introduction: Law and Neoliberalism*, 77 L. & CONTEMP. PROBS. 1, 1, 10, 13 (2014) (distinguishing between classical liberalism and neoliberalism).

[9] Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1737 (2021).

though notable, neither materially shift privacy law's political economy nor meaningfully limit the information economy's data-extractive business model. Different, yes; substantive, no.

Privacy law is at a crossroads. The second wave is arguably reifying mistakes that have contributed to ubiquitous commodification and corporate surveillance. But scholars still have the chance to advise lawmakers to chart a new path. Now is the time to understand where we have been, where we are, and where we need to go if we want to safeguard any semblance of privacy in the information age.

Part I of this essay offers a taxonomy to understand the evolution of privacy law. It is meant as a jumping off point for scholars, a way to frame and understand developments in privacy law in order to enhance future research and debates on privacy law and policy. The essay makes the descriptive argument that U.S. privacy law's two waves can be distinguished on three metrics — their practices, theory of governance, and underlying ideology. Where the first wave focused on notice, was largely self-regulatory, and reflected a *laissez faire* approach to the information economy, the second wave relies on compliance, managerializes privacy, and mirrors neoliberal forces common throughout U.S. law today. This taxonomy is reflected in Figure 1. Part II teases out three generative research questions and normative policy arguments based on this taxonomy.

Figure 1. First and Second Wave Privacy Law

| | 1st Wave | 2nd Wave |
|---|---|---|
| Practices | **Notice** | **Compliance** |
| Governance | **Self-Regulatory** | **Managerial** |
| Ideology | **Classical Liberalism** | **Neoliberal** |

## I. FROM FIRST TO SECOND WAVE PRIVACY LAW

Privacy law is transitioning from a first wave focused on notice to a second wave focused on internal procedures. Governance mechanisms are evolving from self-regulation to managerialized compliance. And the underlying ideology of privacy law is shifting from *laissez faire* to neoliberalism. The following sections develop that descriptive taxonomy.

### *A. Compliance and Internal Structures*

First wave privacy law required companies to draft and post privacy policies.[10] Federal sector-specific statutes and state laws like the California Online Privacy Protection Act required "conspicuous" notices with certain categories of information.[11] In this regime, privacy law was primarily a self-regulatory sphere, with industry making its own data use policies and individuals navigating their privacy preferences platform by platform.[12]

Second wave privacy law relies on internal organizational structures. The FTC's 2011 consent decree with Google offered the first hints of this shift in the U.S.[13] As part of a settlement for misleading Google Buzz customers, the FTC ordered Google to create an internal privacy program,[14] beginning a compliance-based approach in which regulators rely on internal corporate structures to implement the law in practice.[15] Google had to hire a chief privacy officer and staff, situate staff inside organizational hierarchies, complete risk analyses for new products, and develop privacy trainings.[16] The company also had to conduct biennial assessments of that program.[17]

New proposals would create sixteen different internal corporate programs, offices, and practices for privacy governance. Companies must develop a "process" for responding to user opt-out requests,[18]

---

[10] Solove & Hartzog, *supra* note 5, at 592.

[11] CalOPPA § 22575; *e.g.*, Children's Online Privacy Protection Act, 15 U.S.C. §§ 6502(b)(1)(A)-(B) (requiring websites geared toward children to disclose what data they collect, how it will be used, whether it will be shared, and how to delete it or opt out of data collection); Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6803(a)(1)-(2); 16 C.F.R. §§ 313.6(a)(3), (6) (2021) (imposing similar requirements to the Children's Online Privacy Protection Act on certain financial institutions).

[12] Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2235 (2015).

[13] Google, Inc., No. C-4336, at *4 (F.T.C. Oct. 13, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf [https://perma.cc/7FJE-KWV9] (requiring a company to create a "comprehensive privacy program" for the first time).

[14] *Id.*

[15] Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CAL. L. REV. 1529, 1565 (2019).

[16] Solove & Hartzog, *supra* note 5, at 617-18.

[17] Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 793 (2016); Solove & Hartzog, *supra* note 5, at 618.

[18] *E.g.*, CCPA, CAL. CIV. CODE § 1798.135(a)(1) (2021); MYOBA, S. 2637, 116th Cong. §§ 6(a)(6), 7(b)(1)(D)(i)-(ii), 7(b)(1)(F) (2019) (requiring consumer consent, consumer access, and correction by the covered entity if a consumer's personal information is inaccurate); H.R. 216, 2021 Leg., Reg. Sess. §§ 9(a)(1)-(2) (Ala. 2021);

train their employees on privacy issues,[19] keep records on data collected,[20] and complete PIAs when developing new products.[21] They have to develop "organizational" measures, like comprehensive privacy programs, to ensure compliance and conduct regular audits — both of processors and vendors and of the privacy programs themselves.[22] A proposal in Minnesota would require an internal appeals process and four other laws discuss independent tests and annual impact assessments of automated processing or facial recognition.[23] The Mind

H. 3910, 102d Gen. Assemb., 1st Reg. Sess. § 40(a)(1)-(2) (Ill. 2021); S. 46, 192d Gen. Ct., Reg. Sess. § 3(c)(1) (Mass. 2021); S. 569, 2021 Gen. Assemb., 2021 Sess. § 75-72(b)-(c) (N.C. 2021); S. 6701, 2021 Leg., 244th Reg. Sess. § 1102(9) (N.Y. 2021); S. 5062, 67th Leg., Reg. Sess. §§ 103(2)-(5) (Wash. 2021); S. 1614, 54th Leg., 2d Reg. Sess. § 18-701(L)(1)-(4) (Ariz. 2020); S. 2330, 101st Gen. Assemb., 1st Reg. Sess. § 30(a) (Ill. 2020); H. 5603, 101st Gen. Assemb., 2d Reg. Sess. § 40(a)(1)-(2) (Ill. 2020); H. 784, 2020 Gen. Assemb., 441st Sess. § 14-4204 (Md. 2020); H. 1656, 2020 Gen. Assemb., 441st Sess. § 14-4204 (Md. 2020); H.R. 3936, 91st Leg., 2d Reg. Sess § 325O.05 subdiv. 2 (Minn. 2020); A. 3255, 219th Leg., 1st Ann. Sess. § 8 (N.J. 2020); S. 418, 30th Leg., Reg. Sess. § 487J-H (Haw. 2019); H. 1253, 2019 Leg., 2019 Reg. Sess. § 9(a)-(b) (Miss. 2019).

[19] *E.g.*, CCPA § 1798.135(a)(3); CDPSA, S. 1494, 117th Cong. § 6(c)(2)(A) (2021); COPRA, S. 2968, 116th Cong. § 107(b)(4) (2019); Ariz. S. 1614 § 18-701(L)(5); Ill. H. 5603 § 40(a)(6); Md. H. 784 § 14-4204(E); Md. H. 1656 § 14-4204(E); Haw. S. 418 § 487J-H(6); S. 176, 54th Leg., 1st Sess. § 6 (N.M. 2019).

[20] *E.g.*, MYOBA § 6(a)(2)(A); Online Privacy Act of 2019, H.R. 4978, 116th Cong. § 202(b) (2019); Haw. S. 418 § 487J-H (requiring lists of identifying information collected).

[21] *E.g.*, CDPSA § 6(b)(3); SAFE DATA Act, S. 4626, 116th Cong. § 107(a)(1), (b) (2020); MYOBA § 7(b)(G)-(H); S. 190, 73d Gen. Assemb., 1st Reg. Sess. § 6-1-1309 (Colo. 2021); S. 893, 2021 Gen. Assemb., Jan. Sess. § 7(a) (Conn. 2021); N.C. S. 569 § 75-74; N.Y. S. 6701 § 1103(b); Wash. S. 5062 § 109; Ill. S. 2330 § 35(l); Minn. H.R. 3936 § 325O.08; H.D. 473, 2020 Gen. Assemb., Reg. Sess. § 59.1-576 (Va. 2020); S. 2263, 101st Gen. Assemb., 1st Reg. Sess. § 30 (Ill. 2019); H.R. 4390, 86th Leg., Reg. Sess. § 541.058 (Tex. 2019) (establishing an accountability program to assess risk); *see also* Kaminski, *supra* note 15, at 1603-05 (noting that PIAs are internal documents meant to help balance risks and benefits and intended to keep privacy front of mind during design).

[22] On setting up privacy programs: *E.g.*, COPRA §§ 201 & 202(b)(1) (requiring privacy professionals involved and responsible for compliance to implement comprehensive privacy programs and internal reporting structures); MYOBA §§ 6(a)(7), 7(b)(1)(A)-(B) (requiring organizational measures to protect privacy including biennial review of information provided to consumers for exercising opt out requests); Privacy Bill of Rights, S. 1214, 116th Cong. § 13(a)(1) (2019); Minn. H.R. 3936 § 325O.04(b)(1) (requiring processors to have organizational measures to assist data controller with compliance). On audits: *E.g.*, COPRA § 202(b)(2); MYOBA § 5(a)(1); Minn. H.R. 3936 § 325O.04(d)(3).

[23] SAFE DATA Act § 206(b)(4); COPRA § 108(b); MYOBA § 7(b)(G); Privacy Bill of Rights § 13(b)(3); Minn. H. 3936 §§ 325O.05 subdiv. 3, 325O.085(a) (requiring an internal appeals process and independent tests of facial recognition).

Your Own Business Act requires companies to develop an internal process to track opt-out requests of consumers with whom they are not in a direct relationship but nevertheless hold their data.[24]

Five laws call for companies to hire or designate at least one privacy officer.[25] Five proposals require companies to develop internal processes for ensuring that third party vendors comply with the law.[26] Two laws require executive attestations and certifications of compliance.[27] And the SAFE DATA Act calls on a "professional standards body" to write its own rules that, if followed, would constitute compliance with the law.[28]

This shift to compliance is part of what sociolegal scholars call the "managerialization of law," or the "infusion of managerial or business values and ideas into law."[29] Second wave privacy law explicitly envisions that compliance professionals — privacy professionals, privacy lawyers, and other compliance experts — will bring the law into their organizations, translate its requirements for their bosses, and implement it throughout the company.[30] The second wave seeks management of data up and down the line to keep privacy in mind during collection and processing.[31] But along with that shift in responsibility comes the "reconceptualization of law so that it is more consistent with general principles of good management."[32]

[24] MYOBA § 6(a)(4).

[25] CDPSA §§ 6(c)(1), 7(b); SAFE DATA Act § 301(a)-(b); COPRA § 202(a)(1)-(2); MYOBA § 7(b)(C); Privacy Bill of Rights § 14; GDPR, supra note 4, at arts. 28, 39(1)(b).

[26] Data Care Act of 2021, S. 919, 117th Cong. § 3(b)(3)(C) (2021); COPRA § 203(c)(1)(A)-(B); MYOBA § 6(a)(8); Privacy Bill of Rights § 10; Tex. H.R. 4390 § 541.059.

[27] COPRA § 201; MYOBA § 5(b).

[28] SAFE DATA Act §§ 206(c), 404(a). Many of these practices are also part of Canada's proposed Consumer Privacy Protection Act, a second wave law that its drafters explicitly modeled on the GDPR. Part 1, Section 8 requires the designation of a privacy coordinator. Part 1, Section 9 requires a comprehensive privacy program. The law also allows industry-developed certification programs to stand in for evidence of compliance. And the law requires companies to provide evidence of compliance to a data protection agency. The law also guarantees rights of access, transparency, and portability. *See* An Act to Enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to Make Consequential and Related Amendments to Other Acts, H. of Commons C-11, 43rd Parliament, 2d Sess., at 6, 7, 33-34 (2020) (Can.).

[29] LAUREN B. EDELMAN, WORKING LAW: COURTS, CORPORATIONS, AND SYMBOLIC CIVIL RIGHTS 25 (2016).

[30] *See* Kaminski, *supra* note 15, at 1559-60.

[31] *See id.* at 1561.

[32] EDELMAN, *supra* note 29, at 25-26; *see* JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 144-45 (2019).

Theoretically, managerialism is agnostic as to legal values; good management is not necessarily in conflict with the underlying purpose of social legislation. But managerialism does give regulated entities themselves — the intermediaries between the laws on the books and the people those laws are meant to protect — unique power to define what the law means in practice.

### *B. Exercising Rights of Control*

The second wave also provides individual rights to users. First wave privacy law's focus on privacy policies was based on a slimmed down version of the Fair Information Practice Principles ("FIPPs"), which included rights to notice, choice, and security.[33] The FIPPs were outlined in a 1973 report from the Department of Housing, Education, and Welfare, long before the data-extractive business models of today's information industry.[34] But some version of them persisted as the baseline for the first wave's notice-and-consent regime.[35]

The second wave adds new individual rights, including rights to access all the personal information the company has about them,[36] have

[33] Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 959 (2017) (explaining how "control" won out as the focus of the FIPPs and privacy law).

[34] *See* U.S. DEP'T OF HEALTH, EDUC., & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS 41-42 (1973).

[35] *See* Hartzog, *supra* note 33, at 959.

[36] Thirty-six proposals include the right to access. CCPA, CAL. CIV. CODE §§ 1798.100(d), 1798.110, 1798.115 (2021); CDPSA, S. 1494, 117th Cong. § 5(b) (2021); DATA, S. ___, 116th Cong. § 201 (2020); SAFE DATA Act, S. 4626, 116th Cong. § 103(a) (2020); COPRA, S. 2968, 116th Cong. § 102(a) (2019); Online Privacy Act of 2019, H.R. 4978, 116th Cong. § 101 (2019); Privacy Bill of Rights Act, S. 1214, 116th Cong. § 6(a)(1) (2019); H.R. 216, 2021 Leg., Reg. Sess. § 3(a) (Ala. 2021); S. 190, 73d Gen. Assemb., 1st Reg. Sess. § 6-1-1306(1)(b) (Colo. 2021); S. 893, 2021 Gen. Assemb., Jan. Sess. § 4(a)(4) (Conn. 2021); H. 3910, 102d Gen. Assemb., 1st Reg. Sess. § 10(d) (Ill. 2021); S. 46, 192d Gen. Ct., Reg. Sess. § 3(a) (Mass. 2021); S. 6701, 2021 Leg., 244th Sess. § 1102(3) (N.Y. 2021); S. 569, 2021 Gen. Assemb., 2021 Sess. § 75-71(a)(1) (N.C. 2021); H.R. 1126, 205th Gen. Assemb., 2021 Sess. § 4(a)(4) (Pa. 2021); H.R. 3741, 87th Leg., Reg. Sess. § 541.053(1) (Tex. 2021); S. 1392, 2020 Gen. Assemb., 1st Spec. Sess. § 59.1-573(A)(4) (Va. 2021); S. 5062, 67th Leg., Reg. Sess. § 103(1) (Wash. 2021); S. 1614, 54th Leg., 2d Reg. Sess. § 18-701(A)-(D) (Ariz. 2020); S. 2330, 101st Gen. Assemb., 1st Reg. Sess. § 20 (Ill. 2020); H. 5603, 101st Gen. Assemb., 2d Reg. Sess. §§ 10, 20, 25 (Ill. 2020); H. 784, 2020 Gen. Assemb., Reg. Sess. § 14-4203 (Md. 2020); H. 1656, 2020 Gen. Assemb., Reg. Sess. § 14-4203 (Md. 2020); H.R. 3936, 91st Leg., 2d Reg. Sess. § 325O.05, subdiv. 1(1) (Minn. 2020); Legis. 746, 106th Leg., 2d Reg. Sess. §§ 6, 8 (Neb. 2020); Assemb. 3255, 219th Leg., 1st Ann. Sess. § 2(b)-(e) (N.J. 2020); H.D. 473, 2020 Gen. Assemb., Reg. Sess. § 59.1-574(A)(4) (Va. 2020); S.

a company delete the personal information it has already collected,[37] and opt out of tracking or the sale or transfer of data to third parties.[38] Some proposals include rights against retaliation for exercising opt-out rights,[39] rights to correct inaccurate or outdated data,[40] rights to move

418, 30th Leg., Reg. Sess. § 487J-C (Haw. 2019); S. 2263, 101st Gen. Assemb., 1st Reg. Sess. § 20(1) (Ill. 2019); H. 1253, 2019 Leg., 134th Reg. Sess. §§ 3(1), 5, 6 (Miss. 2019); S. 176, 54th Leg., 1st Sess. § 3(a) (N.M. 2019); S. 5642, 2019 Leg., Reg. Sess. § 1103(1), (5) (N.Y. 2019); H.R. 1049, 203d Gen. Assemb., 2019 Sess. § 4(a)(4), (b) (Pa. 2019); S. 234, 2019 Gen. Assemb., 2019 Leg. Sess. §§ 6-48.1-3(a), 6-48.1-6 (R.I. 2019); H.R. 4518, 86th Leg., Reg. Sess. §§ 541.051(a), 541.053 (Tex. 2019); S. 2834, 218th Leg., 1st Ann. Sess. § 3 (N.J. 2018).

[37] Thirty-five proposals include a right to delete. CCPA § 1798.105; CDPSA § 5(d); DATA § 204; SAFE DATA Act § 103(a)(1)(C); COPRA § 103; Online Privacy Act of 2019 § 103; Privacy Bill of Rights Act § 6(a)(5); Ala. H.R. 216 § 4(a)-(c); Colo. S. 190 § 6-1-1306(1)(d); Conn. S. 893 § 4(a)(3); Ill. H. 3910 § 15(a); Mass. S. 46 § 3(b); N.C. S. 569 § 75-71(a)(3); N.Y. S. 6701 § 1102(6); Pa. H.R. 1126 § 4(e); Tex. H.R. 3741 § 541.054; Wash. S. 5062 § 103(3); Va. S. 1392 § 59.1-573(A)(3); Ariz. S. 1614 § 18-701(E); Ill. S. 2330 § 25(3); Ill. H. 5603 § 15; Md. H. 784 § 14-4205; Md. H. 1656 § 14-4205; Minn. H.R. 3936 § 325O.05, subdiv. 1(3); Miss. H. 1253 § 4; Neb. Legis. B. 746 § 9; N.J. Assemb. 3255 § 3; Va. H. 473 § 59.1-574(A)(3); Haw. S. 418 § 487J-D; Ill. S. 2263 § 20(2); N.M. S. 176 § 3(B); N.Y. S. 5642 § 1103(3); Pa. H.R. 1049 § 4(e); R.I. S. 234 § 6-48.1-4; Tex. H.R. 4518 § 541.052.

[38] Thirty proposals include a right to opt out of some tracking. CCPA §§ 1798.120, 1798.135(a)-(b); Information Transparency & Personal Data Control Act of 2021, H.R. 1816, 117th Cong. § 3(a)(4); SAFE DATA Act § 104(d); COPRA § 105(b); MYOBA, S. 2367, 116th Cong. § 6 (2019); Colo. S. 190 § 6-1-306(1)(a); Conn. S. 893 § 4(a)(5); Ill. H. 3910 § 30(a); Pa. H.R. 1126 § 4(a)(3); N.C. S. 569 § 75-71(a)(5); Va. S. 1392 § 59.1-573(A)(5); Wash. S. 5062 § 103(5); Ariz. S. 1614 § 18-701(G); H.R. 963, 2020 Leg., 122d Reg. Sess. § 501.062(2)(b) (Fla. 2020); Ill. S. 2330 § 25(1); Ill. H. 5603 § 30; Md. H. 784 § 14-4206; Md. H. 1656 § 14-4206; Minn. H.R. 3936 § 325O.05, subdiv. 1(5); Va. H. 473 § 59.1-574; Haw. S. 418 § 487J-F; Ill. S. 2263 § 20(6); Miss. H. 1253 § 7; N.M. S. 176 §§ 3(d), 4(f); N.J. Assemb. 3255 § 6; Pa. H.R. 1049 § 4(a)(3); R.I. S. 234 § 6-48.1-7; Tex. H.R. 4518 § 541.054; Assemb. 2188, 218th Leg., 1st Ann. Sess. § 4 (N.J. 2018); N.J. S. 2834 § 4.

[39] Sixteen proposals include this right. DATA § 104(d); SAFE DATA Act § 101(a); Wash. S. 5062 § 107(7); Ill. H. 5603 § 35; Md. H. 784 § 14-4207; Md. H. 1656 § 14-4207; Minn. H.R. 3936 § 325O.07, subdiv. 3; Neb. Legis. 746 § 10; N.J. Assemb. 3255 § 7; Va. H.D. 473 § 59.1-574; Haw. S. 418 § 487J-G; Miss. H. 1253 § 8; N.M. S. 176 § 5(a); Pa. H.R. 1049 § 4(k); R.I. S. 234 § 6-48.1-8; N.J. Assemb. 2188 § 4(b).

[40] Nineteen proposals guarantee this right. CDPSA § 5(c); DATA § 203; SAFE DATA Act § 103(a); COPRA § 104; Online Privacy Act of 2019 § 102; Privacy Bill of Rights Act § 6(a)(4); Colo. S. 190 § 6-1-1306(c); Conn. S. 893 § 4(a); N.Y. S. 6701 § 1102(5); N.C. S. 569 § 75-71(a)(2); Mass. S. 46 § 3(b); Tex. H.R. 3741 § 541.052; Va. S. 1392 § 59.1.573; Wash. S. 5062 § 103(2); Ill. S. 2330 § 25(2); Minn. H.R. 3936 § 325O.05, subdiv. 1(2); Va. H.D. 473 § 59.1-574; Ill. S. 2263 § 20(2); N.Y. S. 5642 § 1103(2).

data from one company to another,[41] and rights to restrict processing of personal data.[42] Five draft bills include opt-in rights for certain types of data collection and processing.[43] The proposed New York Privacy Act would give citizens a right against purely algorithmic or automated decisions about their lives.[44] And in addition to many of the rights above, the Privacy Bill of Rights would guarantee a right to data security.[45] The Data Accountability and Transparency Act, or DATA Act, guarantees a right to object to data processing and human review of automated decision-making systems.[46]

Guaranteeing these rights gives rise to two sets of social practices: individuals have to exercise their rights and companies have to develop processes to evaluate customer requests. To opt out of certain data processing, for example, individuals must click on a link and complete a form. Indeed, they have to take the initiative to exercise almost all second wave rights. Companies also have to build forms and add functionality to their websites. Notably, nearly one-quarter of state second wave laws explicitly require companies to create "Do Not Sell My Information" buttons.[47] Requests to delete, correct, and port data also have to be evaluated. That means that companies must create internal processes for verifying and responding to these requests, processes that include hiring privacy professionals to review user requests, tasking engineers to code new functionality, and developing an internal reporting structure for approving, rejecting, and even appealing decisions. Therefore, as second wave privacy laws on the

[41] DATA § 201; SAFE DATA Act § 103(a); COPRA § 105(a); Privacy Bill of Rights Act § 6(a)(3)(B); Wash. S. 5062 § 103(1); Minn. H.R. 3936 § 325O.05, subdiv. 1(4); Va. H.D. 473 § 59.1-574.

[42] GDPR, *supra* note 4, at art. 18; Va. H.D. 473 § 59.1-574(A)(1); Ill. S. 2263 § 20(4).

[43] SAFE DATA Act § 104(a) (opt in to transfers and processing of sensitive information); Privacy Bill of Rights Act § 5(a)(1)-(2); Mass. S. 46 § 6; N.C. S. 569 § 75-72(a)(5); N.J. Assemb. 3255 §§ 2, 9.

[44] *See* N.Y. S. 5642 § 1103(6).

[45] Privacy Bill of Rights Act § 13.

[46] DATA §§ 205, 206.

[47] CCPA, CAL. CIV. CODE § 1798.135(a)(1); S. 1614, 54th Leg., 2d Reg. Sess. § 18-701(L)(4) (Ariz. 2020); H. 5603, 101st Gen. Assemb., 2d Reg. Sess. § 45(a)(2) (Ill. 2020); H. 4812, 123d Gen. Assemb., 2d Reg. Sess. § 37-31-70(A)(1) (S.C. 2020); S. 418, 30th Leg., Reg. Sess. § 487J-H(c)(1)-(2) (Haw. 2019); H.R. 1253, 2019 Leg., 134th Reg. Sess. § 10(1)(a)-(b) (Miss. 2019); S. 176, 54th Leg., 1st Sess. § 4(F)(1)-(2) (N.M. 2019); H.R. 1049, 203d Gen. Assemb., 2019 Sess. § 4(l)(3)-(4) (Pa. 2019); S. 234, 2019 Gen. Assemb., 2019 Leg. Sess. § 6-48.1-10(1)-(2) (R.I. 2019); H.R. 4518, 86th Leg., Reg. Sess. § 541.054(b)(2) (Tex. 2019); Assemb. 2188, 218th Leg., 1st Ann. Sess. § 4(a) (N.J. 2018); S. 2834, 218th Leg., 1st Ann. Sess. § 4(a) (N.J. 2018).

books establish individual rights to data, they are also creating corporate practices for implementing and evaluating those rights.

Notably, some second wave privacy laws also build on the first wave's right-to-consent paradigm. Almost all state and federal proposals in the U.S. are opt-out regimes, which means that data collection and processing is presumed lawful unless individuals affirmatively withdraw their consent. Some laws go further, doubling down on the power of consent. For instance, two proposals in Arizona allow companies that obtain consent to sell customer data, avoid all restrictions on data processing, and make decisions based on consumer.[48] Two proposals introduced in the Illinois Senate would allow companies to skirt limits on processing sensitive data, even processing that posed a significant risk to privacy, if they obtain consent.[49] And Maine's privacy law, which took effect in 2020, lifts all restrictions on use, disclosure, sale, and third-party access to personal information if companies obtain consent.[50]

Therefore, when viewed from perspective of social practice, many second wave privacy proposals in the U.S. look similar. They all take a similar rights-and-compliance approach. They envision similar regulatory, compliance, and customer behavior. And although there are variations at the margins, this section has shown that similarities run deep.[51]

### *C. The Political Economy of the First and Second Waves*

The previous sections clarified some of the practical developments in privacy law. First wave privacy law walled off the information industry from government intervention. Indeed, notice-and-consent was originally developed as a way to stave off potentially more robust regulation that could threaten the industry's innovation imperative.[52]

---

[48] *See* Ariz. S. 1614 § 18-701(H); H.R. 2729, 54th Leg., 2d Reg. Sess. §§ 18-574(B), 18-577(G)(3) (Ariz. 2020).

[49] *See* S. 2330, 101st Gen. Assemb., 1st Reg. Sess. § 35(l)(3) (Ill. 2020); S. 2263, 101st Gen. Assemb., 1st Reg. Sess. § 30(3) (Ill. 2019).

[50] ME. REV. STAT. ANN. tit. 35-A, § 9301(3) (2020).

[51] Some of these variations include focusing on biometric privacy or relying on fiduciary duties to rein in data processing. For example, the Illinois Biometric Information Privacy Act ("BIPA") is the "strongest" of three biometric privacy laws in the U.S. Biometric Information Privacy Act, 740 ILL. COMP. STAT. ANN. 14/15 (2021). Three new proposals call for imposing fiduciary duties on data collectors. *E.g.*, Data Care Act of 2021, S. 919, 117th Cong. § 3 (2021); S. 2351, 88th Gen. Assemb., 2020 Sess. § 3 (Iowa 2020); S. 5642, 2019 Leg., Reg. Sess. § 1102 (N.Y. 2019).

[52] *See* Solove & Hartzog, *supra* note 5, at 592-94; *see also* Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041, 2046-47 (2000)

The first wave was also premised on notions of autonomy, liberty, and freedom. As one leading scholar noted, "[p]roviding people with notice, access, and the ability to control their data is key to facilitating some autonomy in a world where decisions are increasingly being made about them with the use of personal data."[53] The first wave put the onus of privacy navigation on the user, making the agreement between users and data collectors on the terms of a privacy policy the locus of the law's concern.[54] Policy reforms to hold platforms more accountable were attacked as "break[ing] the internet" and undermining a growing market of e-commerce and social media.[55] Therefore, the first wave arguably reflected a "hands off," or classically liberal, approach to law and the information economy.[56]

The second wave is different. As we have seen, its practices are largely about compliance, including reliance on industry best practices, impact assessments, audits, and privacy offices that manage, rather than restrict, data use. These governance mechanisms are managerial in that they integrate management values like efficiency into organizational decision-making and rely on professionals to make those decisions in ways that accord with good management.[57] The second wave represents a choice to filter privacy law through corporate compliance and to manage data collection and processing from within. By using internal and managerialized corporate structures to do regulatory work, second wave practices reflect a neoliberal approach.[58]

(suggesting that the threat of new privacy legislation led to an increase in websites posting privacy policies); Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 130-31 (2008) (noting that self-regulation was an alternative to the potential for more regulation).

[53] Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1899 (2013).

[54] *See id. See generally* Grewal & Purdy, *supra* note 8, at 13 (noting that the contract was the "touchstone" of individual freedom in classical liberalism).

[55] Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 FORDHAM L. REV. 401, 401 (2017); *see* Eric Goldman, *Why the State Attorneys General's Assault on Internet Immunity Is a Terrible Idea*, FORBES (June 27, 2013, 10:44 AM EST), https://www.forbes.com/sites/ericgoldman/2013/06/27/why-the-state-attorneys-generals-assault-on-internet-immunity-is-a-terrible-idea/ [https://perma.cc/B2N5-RJUE].

[56] Classical liberalism "sought to define an area of social life standing outside of . . . political governance and not appropriate for political decision." Grewal & Purdy, *supra* note 8, at 10.

[57] *See* COHEN, *supra* note 32, at 144-45.

[58] *See id.* at 7; David Harvey, *Neoliberalism as Creative Destruction*, 610 ANNALS OF AM. ACAD. POL. & SOC. SCI. 22, 22 (2007). The term "neoliberalism" is admittedly overused and can be confusing. *See* JAMIE PECK, CONSTRUCTIONS OF NEOLIBERAL REASON

Classical liberalism and neoliberalism share some common elements, as their names suggest. They both "assert[] and defen[d] . . . economic power against political intervention."[59] But where classical liberalism envisions a consistently *laissez faire* relationship between law and markets, neoliberalism advocates for a state that is thoroughly infused with market thinking — a belief that the market is the best way to advance social welfare, and that only market-based options are workable.[60] Neoliberal governance can be interventionist or noninterventionist, but it is always infused with market values. Such market-based thinking includes valorizing efficiency in institutions, focusing on wealth maximization of private actors, minimizing transaction costs, using cost-benefit analyses to make decisions,[61] and relying on law to intervene to protect those values.[62]

Neoliberal assumptions about the relationship between law and markets, the role of efficiency in governance, and the role of regulators pervade second wave privacy law. For instance, second wave privacy law treats privacy as a field of law that is "about the market," in which the quest for efficiency becomes a descriptive and normative goal of the law.[63] Even in its ideal form, the rights-compliance model is supposed to take the "benefits of self-regulation without its pitfalls" while still offering the possibility of "better approximat[ing] a market-driven optimum."[64] The Brookings Institution, which has released its own proposal for a second wave law, implicitly adopted this assumption in its proposed legislative findings as well, noting that law has to evolve

15 (2010); Terry Flew, *Michel Foucault's* The Birth of Biopolitics *and Contemporary Neo-liberalism Debates*, 108 THESIS ELEVEN 44, 44-45 (2012).

[59] Grewal & Purdy, *supra* note 8, at 1.

[60] *See id.* at 6, 13-14; *see also* Jamie Peck & Adam Tickell, *Conceptualizing Neoliberalism, Thinking Thatcherism*, *in* CONTESTING NEOLIBERALISM: URBAN FRONTIERS 26, 33 (Helga Leitner et al. eds., 2007).

[61] *See* Jedediah Britton-Purdy, David Singh Grewal, Amy Kapczynski & K. Sabeel Rahman, *Building a Law-and-Political-Economy Framework: Beyond the Twentieth-Century Synthesis*, 129 YALE L.J. 1784, 1796-1800, 1812 (2020).

[62] *See* Britton-Purdy et al., *supra* note 61, at 1784, 1796-1800; Grewal & Purdy, *supra* note 8, at 6. Scholars have called the diffusion of this ideology, as it applies to law, the Twentieth-Century Synthesis. Britton-Purdy et al., *supra* note 61, at 1790. The Synthesis involves the reorientation of some areas of law, especially those involving significant economic activity, toward achieving "efficiency" rather than any other social goal. *Id.* at 1790, 1806. As the next two sections show, neoliberal assumptions about the relationship between law and markets, the role of efficiency in governance and the role of regulators have been normalized in second wave privacy law. This fits the second wave squarely within the Synthesis.

[63] *Id.* at 1790.

[64] Kaminski, *supra* note 15, at 1561.

"as technology, innovation, and services — and risks to privacy — evolve."[65] This view perpetuates overlapping discourses, taken as a given among many policymakers today, that innovation is normatively good, regulation is normatively bad, the two are in tension, and the market is the ideal.[66]

Compliance requirements like privacy impact assessments also reflect neoliberalism's primacy in second wave privacy law. Even though PIAs are supposed to "identif[y] and evaluate[] potential threats to individual privacy . . . [and] the appropriate risk mitigation measures," they are often recast to incorporate the profit-seeking interests of industry. They evaluate risks *to the company* of reduced profit or litigation without considering the privacy risks *of consumers*.[67] In practice, PIAs also tend to boil down to cost-benefit analyses. Practitioners admit this. The Future of Privacy Forum (FPF) published a guide explicitly for the purpose of helping "organizations in their weighing of the benefits of new or expanded data processing against attendant privacy risks."[68] Kelsey Finch and Omer Tene identify "benefit-risk analysis" as one of five components of data stewardship.[69]

Other second wave practices also integrate market values. Many companies outsource some of their privacy compliance functions to technology vendors, hoping to achieve efficiencies and reduce costs.[70] Granted, outsourcing is not required by any of the second wave's

---

[65] Cameron F. Kerry & John B. Morris, *Framing a Privacy Right: Legislative Findings for Federal Privacy Legislation*, BROOKINGS (Dec. 8, 2020), https://www.brookings.edu/research/framing-a-privacy-right-legislative-findings-for-federal-privacy-legislation/ [https://perma.cc/5M4Y-E9EL].

[66] *See, e.g.*, *Consumer Perspectives: Policy Principles for a Federal Data Privacy Framework in the United States: Hearing Before the S. Comm. on Com., Sci., & Transp.*, 116th Cong. (2019) (statement of Sen. Maria Cantwell, Chair, S. Comm. on Com., Sci. & Transp.).

[67] EDELMAN, *supra* note 29, at 77-99; *see* Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 789-803 (2020).

[68] JULES POLONETSKY, OMER TENE & JOSEPH JEROME, FUTURE OF PRIV. F., BENEFIT-RISK ANALYSIS FOR BIG DATA PROJECTS 1 (2014), https://fpf.org/wp-content/uploads/FPF_DataBenefitAnalysis_FINAL.pdf [https://perma.cc/LLJ6-LQWF].

[69] Kelsey Finch & Omer Tene, *Smart Cities: Privacy, Transparency, and Community*, *in* THE CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 125, 130-31 (Evan Selinger et al. eds., 2018); *see also* Ira S. Rubinstein & Bilyana Petkova, *Governing Privacy in the Datafied City*, 47 FORDHAM URB. L. J. 755, 791-92 (2020).

[70] Ari Ezra Waldman, *Outsourcing Privacy*, 96 NOTRE DAME L. REV. REFLECTION 194, 195-96 (2021); *see* IAPP & TRUSTARC, MEASURING PRIVACY OPERATIONS 7-8, 11 (2018), https://iapp.org/media/pdf/resource_center/IAPP-Measuring-Privacy-Operations-FINAL.pdf [https://perma.cc/T3GH-VY5P] (justifying the turn to privacy technology outsourcing as means to achieve efficiencies and lower costs); *see also* COHEN, *supra* note 32, at 156-57.

provisions, but its proliferation highlights the second wave's managerialism and proceduralism: when legal compliance means checking boxes and filling out forms, it is easy to shift those responsibilities off campus.[71] Second wave laws empower industry to set its own codes of conduct and standards, certify compliance with those standards, and rely on certification as a safe harbor to introduce the needs and preferences of market actors in determining legal compliance.[72] FTC regulators are on the record supporting compliance safe harbors, as well.[73]

What is more, second wave rights of control, all of which have to be exercised by individuals through affirmative requests, reflect neoliberalism's concern with providing "equal enjoyment of unfettered choice" to consumers and the normative argument that individual choices in the market is the fastest route to general welfare.[74] More importantly, it reflects neoliberalism's ideological preference for reducing legal interests to individual claims subject to individual remedies: access to *my* data, correcting *my* data, objecting to the processing of *my* data.[75]

Understood in this way, the second wave is decidedly neoliberal. That should come as no surprise. Neoliberal managerialism is what passes for regulation in the United States. Julie Cohen argues that the legal institutions of informational capitalism as a whole are decidedly managerial.[76] They rely on audits and compliance tools as hollowed out public institutions turn to industry to self-certify their compliance with the law.[77] Cost-benefit analyses are engrained in modern environmental, health, and safety law,[78] opening the door to

[71] *See* RONAN MCIVOR, THE OUTSOURCING PROCESS: STRATEGIES FOR EVALUATION AND MANAGEMENT 40-59 (2005) (exploring some of the conditions, including the drive for efficiency and rote procedures, that make outsourcing more likely).

[72] *See, e.g.*, SAFE DATA Act, S. 4626, 116th Cong. §§206(c)(3), 404(a) (2019); *see also* Kaminski, *supra* note 15, at 1574; Orly Lobel, *The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought*, 89 MINN. L. REV. 342, 375, 389, 392 (2004).

[73] *Redressing Privacy Violations: A Conversation with Experts*, UNIV. OF WASH. TECH POL'Y LAB & MICROSOFT (Dec. 10, 2020), https://medius.studios.ms/Embed/video-nc/CELAReadress-2020 [https://perma.cc/GH4W-V9Q2] (comments by former FTC Commissioners Brill and McSweeney).

[74] Grewal & Purdy, *supra* note 8, at 13.

[75] Neoliberalism is centered on "the consenting individual" as "the author of the norms under which she will live." Britton-Purdy et al., *supra* note 61, at 1814-15.

[76] COHEN, *supra* note 32, at 144-45.

[77] *See id.* at 192-93.

[78] DOUGLAS A. KYSAR, REGULATING FROM NOWHERE: ENVIRONMENTAL LAW AND THE SEARCH FOR OBJECTIVITY 100-05 (2010); *see also* Cary Coglianese, *The Managerial Turn*

considering market costs in regulatory decision-making.[79] Financial regulation in the wake of the 2008 Financial Crisis relies on audits, independent committees, and other internal structures that amount to outsourcing regulation to regulated entities themselves.[80] Cost-benefit comparisons in intellectual property law and antitrust law have helped large information platforms amass unparalleled power and market share.[81] Judith Resnick described how judges, infused with neoliberal discourses about efficiency, actively encourage settlement, often to the detriment of plaintiffs.[82] An obsession with judicial efficiency has similarly expanded the role of employer-friendly arbitration and played an important role in justifying forced arbitration clauses in employment contracts.[83] And, as Lauren Edelman has shown, the corporate practices associated with Title VII have become little more than policy statements, diversity offices, bias training, and internal appeals, many of which have frustrated the realization of actual gender parity and equality in the workplace.[84] The practical content of the GDPR, the CCPA, and their second wave cousins is similar.

## II. QUESTIONS FOR FUTURE RESEARCH

This taxonomy offers privacy scholars a new way of understanding the evolution of privacy law in the U.S., providing ammunition for critiquing current legislative approaches. The taxonomy also raises myriad questions that privacy scholars must answer if we want to create

*in Environmental Policy*, 17 N.Y.U. ENV'T L.J. 54, 55-60 (2008) (describing managerialism in environmental law); Thomas O. McGarity, *The Goals of Environmental Legislation*, 31 B.C. ENV'T AFFS. L. REV. 529, 551 (2004) (describing the Risk Assessment and Cost-Benefit Act of 1995, which would have required cost-benefit analysis in all regulatory programs).

79 Britton-Purdy et al., *supra* note 61, at 1811-12; Martha C. Nussbaum, *The Costs of Tragedy: Some Moral Limits of Cost-Benefit Analysis*, 29 J. LEGAL STUD. 1005, 1029-30 (2000); Amartya Sen, *The Discipline of Cost-Benefit Analysis*, 29 J. LEGAL STUD. 931, 936 (2000).

80 Rory Van Loo, *The New Gatekeepers: Private Firms as Public Enforcers*, 106 VA. L. REV. 467, 485-86 (2020) (demonstrating how CFPB regulators outsource regulation of third parties to banks); Rory Van Loo, *Regulatory Monitors: Policing Firms in the Compliance Era*, 119 COLUM. L. REV. 369, 397-98 (2019) (describing the role of internal compliance departments in financial regulation as a form of "collaborative governance").

81 *See* COHEN, *supra* note 32, 15-24; Lina M. Khan, Note, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 720-21 (2017).

82 Judith Resnick, *Managerial Judges*, 96 HARV. L. REV. 374, 379, 424-31 (1982).

83 Judith Resnick, *Diffusing Disputes: The Public in the Private of Arbitration, the Private in Courts, and the Erasure of Rights*, 124 YALE L.J. 2804, 2836-47 (2015).

84 EDELMAN, *supra* note 29, at 11.

better privacy laws. This part surfaces just three of those questions: Why do all second wave privacy laws look roughly the same? Regardless of its origins, is the second wave capable of addressing the structural problems of informational capitalism? If not, are there alternative governance frameworks that could do better? This section canvases the current literature for answers and, in so doing, evaluates the second wave, invites researchers to contribute to a new research agenda, and asks lawmakers to learn from rather than repeat the mistakes of the past.

### *A. Second Wave Isomorphism*

Many second wave privacy laws in the U.S. have the same rights-compliance model. Given political polarization, that isomorphism is remarkable, but not unsurprising. At the beginning of the second wave, Anu Bradford predicted this uniformity would be the result of a "Brussels Effect."[85] Multinational companies, Bradford argued, will voluntary adopt E.U. rules in part because of the E.U.'s unique combination of market power, regulatory capacity, and preference for strict rules.[86] And since data flows are difficult to constrain within political boundaries, companies in the information industry will be uniquely susceptible to E.U. regulatory power.[87] In the privacy space, E.U. law also bans data transfers from the E.U. to other countries if those countries do not have "adequate" data protection laws.[88] Therefore, Bradford presciently predicted that industry and governments would strengthen their practices to meet E.U. demands.[89]

This theory seems cogent: Many second wave proposals look like the GDPR. However, it does not explain why policymakers have not gone further and adopted stronger laws or imposed substantive limits on data collection that would also win an adequacy determination. E.U. regulators have made clear that there is no one path to adequacy, yet U.S. lawmakers have chosen only one set of practices.[90] Plus, the E.U. has had a privacy law for decades — the E.U. Privacy Directive went into effect in 1995 — and it did not spur Congress or the states to act.[91]

---

[85] Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 3, 22-26 (2012).

[86] *Id.* at 10-19.

[87] *Id.* at 17-19, 25-26.

[88] *Id.* at 24-26; *see also* GDPR, *supra* note 4, at 61-62; Council Directive 95/46, On the Protection of Individuals with Regard to the Processing of Personal Data, 1995 O.J. (L 281), art. 25 [hereinafter Privacy Directive].

[89] Bradford, *supra* note 85, at 24-26.

[90] *See* Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 783-85, 787, 794 (2019) (recognizing various approaches to achieving "adequacy").

[91] Privacy Directive, *supra* note 88.

Privacy scholars Anupam Chander, Bill McGeveran, and Margot Kaminski suggest that it was the norm entrepreneurship of California privacy activists that catalyzed the explosion of recent second wave privacy proposals.[92] Perhaps, but that argument ignores the fact that privacy law-as-compliance dates as far back as 2011, when the FTC first required Google to develop a "comprehensive privacy program,"[93] and privacy law-as-individual-rights is even older.[94] The current literature is incomplete.

This essay's taxonomy, which focuses on on-the-ground practices rather than the laws on the books, suggests scholars should look elsewhere for inspiration. The sociolegal scholar Lauren Edelman has argued that law can develop endogenously from the ground up, socially constructing the specific requirements of vague statutory provisions from the practices regulated entities develop in their wake.[95] Edelman's work, which focused on Title VII's ban on sex discrimination in the workplace, suggested that the law's endogeneity undermined its ability to achieve its intended purpose. Rather than a law of substantive equality, Title VII became the law of nondiscrimination policies, employee trainings, diversity offices, compliance documents, and internal procedures. As I have argued elsewhere, the same may be true of privacy law's second wave.[96]

### *B. What Is Privacy (Law) For?*

In addition to exploring why the second wave looks the way it does, we should also ask whether the proposals will be effective. But effective at doing what? Evaluating the substantive adequacy of the second wave depends on identifying and assessing the normative value of its goals. Legal scholars lament that privacy is a "concept in disarray."[97] There are many different definitions of privacy, many of which orient privacy law toward achieving different goals. Second wave practices, governance, and ideology suggest that these laws see privacy as an individual right to control what happens to one's data. Whether these proposals can

[92] *See* Chander et al., *supra* note 9, at 1737 (suggesting that the creative use of legal processes in California by entrepreneurial pro-privacy advocates was a key driver of the proliferation of new privacy proposals in the US).

[93] Google, Inc., No. C-4336, at *4 (F.T.C. Oct. 13, 2011).

[94] U.S. DEP'T OF HEALTH, EDUC., & WELFARE, RECORDS, *supra* note 34, at xxiii-xxvi (describing the Fair Information Practice Principles, which originally included rights to notice, access, correction, and reasonable security).

[95] EDELMAN, *supra* note 29, at 3-16.

[96] Waldman, *supra* note 67, at 792-93.

[97] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1-12 (2008).

achieve that — and whether that is the goal we need from privacy law — is contestable.

To the extent that second wave privacy laws offer individuals additional rights to access, correct, delete, and port information, they sit within a long tradition of privacy laws focused on atomistic personal autonomy and choice.[98] Most scholars agree that this conception of privacy is outdated and incompatible with today's information ecosystem. Control, as Woodrow Hartzog has argued, "simply does not scale."[99] Even if we theoretically had control over information (whatever "control" actually means), we simply could not exercise that control on the myriad apps, websites, and platforms that give us endless toggles, requests, and options to click.[100] Rights of control can also be weaponized against the individual. Daniel Solove has argued that technology companies "take refuge" in control rights like consent because they allow companies to manipulate us into assuming privacy risks while absolving themselves of subsequent responsibility for data misuse.[101]

What is more, the second wave's governance model — a public-private partnership that relies on internal corporate procedures as guardrails around data extraction — is insufficient to achieve control.[102] The significant risk of capture endemic to the rights-compliance model puts even the most minimal commitment to control at risk.[103] Relying on data-extractive companies to monitor themselves through ongoing internal compliance may undermine second wave privacy law's ability to protect any kind of privacy. As a structural matter, the second wave's approach to data governance elides the asymmetries of power that define informational capitalism.[104] Rules that put procedural requirements around the status quo do not change it. And that status quo is one of extraordinary power imbalance, with power concentrated

98 *See* Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1905 (2013).

99 Hartzog, *supra* note 33, at 956.

100 Ari Ezra Waldman, *Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'*, 31 CURRENT OP. PSYCHOLOGY 105, 106-07 (2020).

101 Solove, *supra* note 53, at 1880.

102 *See generally* Jody Freeman, *The Private Role in Public Governance*, 75 N.Y.U. L. REV. 543 (2000) (analyzing public-private partnerships in administrative law and approving of private actors as "regulatory resources, capable of producing accountability"); Lobel, *supra* note 72 (discussing new roles for private actors in emerging regulatory schemes).

103 *See* Lobel, *supra* note 72, at 465 (conceding that collaborative governance tools will be "used by management merely as mechanisms for monitoring, controlling, and exerting additional pressures on workers").

104 *See* Cohen, *supra* note 98, at 1930.

in the hands of a few powerful companies. Through data extraction and processing, the information industry has the power to influence much our existence — what we read, think, see, want, and even understand to be true can be manipulated by weaponized data-driven tools.[105] Technology companies conscript us in the commodification and subordination of others.[106] Their products discriminate, subordinate, and undermine democracy.[107] Requiring a company to complete an impact assessment before processing data not only leaves those power structures intact, but also suggests that redistributing that power simply isn't the second wave's goal.

That is a fatal blind spot. The second wave conceptualizes privacy as personal control over data and tries to achieve that goal by laying down "rules of the road" for data use rather than restructuring a data-extractive business model to rein in information industry power.[108] But informational capitalism creates population-level harms, not merely atomistic ones.[109] It puts marginalized populations at unique risks.[110] It

[105] *See id.* at 1916-17 (describing the "modulated society").

[106] *See* Salome Viljoen, *Democratic Data: A Relational Theory for Data Governance*, 131 YALE L.J. (forthcoming 2021) (manuscript at 6).

[107] *E.g.*, SIVA VAIDHYANATHAN, ANTI-SOCIAL MEDIA: HOW FACEBOOK DISCONNECTS US AND UNDERMINES DEMOCRACY (2018); Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 694-714 (2016); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 27-32 (2014); Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence*, 66 UCLA L. REV. 54, 70-77 (2019); Julia Angwin, Jeff Larson, Surya Mattu & Lauren Kirchner, *Machine Bias*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [https://perma.cc/LPY9-YPFM].

[108] *See, e.g.*, Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENV. L. REV. 93, 108, 110 (2020) (explaining that the GDPR is a compliance regime that outlines how personal data can be processed lawfully).

[109] Viljoen, *supra* note 106 (manuscript at 20-29).

[110] *See e.g.*, ANITA L. ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY (1988) (describing how "too much of the wrong kind of privacy" undermines women's liberation and equality); SCOTT SKINNER-THOMPSON, PRIVACY AT THE MARGINS 2 (2021) (arguing that privacy protections are uniquely important for queer people and other marginalized populations); Anita L. Allen, *Gender and Privacy in Cyberspace*, 52 STAN. L. REV. 1175, 1178 (2000) (showing how women's privacy is undermined online); Anita L. Allen, *Privacy Torts: Unreliable Remedies for LGBT Plaintiffs*, 98 CALIF. L. REV. 1711, 1721 (2010) (demonstrating how the privacy torts' vision of privacy as control inadequately protects the sexual privacy of LGBTQ people); Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 70, 85 (2009) (showing how traditional civil tort remedies cannot protect women from gendered cyberharassment); Danielle Keats Citron, *Sexual Privacy*, 128 Yale L.J. 1870, 1908 (2019) (calling for special protection for privacy over intimate information in part because of sexual privacy's salience to women, LGBTQ persons, and others) [hereinafter Citron, *Sexual Privacy*]; Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV.

normalizes surveillance and attendant behavior manipulation.[111] Critical privacy scholars recognize this; the second wave does not. Scholars and policymakers should continue to interrogate the conceptions of privacy underlying new approaches to privacy law. As they do, they may find that privacy law has been a sham from the beginning.

### *C. A "Third Wave" for Privacy Law*

Fortunately, there are alternatives. The long scholarly literature suggests that privacy law should seek to guarantee values other than control, including self-determination,[112] intimacy,[113] trust,[114] free thought,[115] liberation from oppression,[116] civility,[117] and human flourishing,[118] among others. Danielle Citron has called for focusing the law on protecting sexual privacy because of its centrality to other fundamental rights.[119] Julie Cohen argues that privacy is "an interest in breathing room to engage in socially situated processes of boundary management."[120] For Cohen, privacy is not solely the province of atomistic individuals; rather, privacy has social value and "furthers fundamental public policy goals relating to liberal democratic citizenship, innovation, and human flourishing."[121] Elsewhere, I have argued that privacy should protect relationships of trust, the lifeblood

345, 347-48 (2014) (showing how traditional means of understanding and protecting privacy are ill-equipped to protect victims of nonconsensual pornography).

111 SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 6 (2019).

112 *E.g.*, Cohen, *supra* note 98, at 1905.

113 *E.g.*, Citron, *Sexual Privacy*, *supra* note 110, at 1888-90.

114 *E.g.*, ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 50 (2018); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 456 (2016).

115 *E.g.*, NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 112 (2015).

116 *E.g.*, ALLEN, *supra* note 110, at 35-37; SKINNER-THOMPSON, *supra* note 110, at 5.

117 *E.g.*, Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 959-68 (1989).

118 *E.g.*, Cohen, *supra* note 98, at 1911.

119 Citron, *Sexual Privacy*, *supra* note 110, at 1890.

120 JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 149 (2012).

121 Cohen, *supra* note 98, at 1927.

of social interaction.[122] Helen Nissenbaum conceptualizes privacy in terms of context-specific norms of information flow.[123]

Privacy law would look different if privacy discourse put choice, consent, and individual rights to the side. Writing from different perspectives, Citron and Kristin Johnson call for writing privacy laws like they're civil rights laws. Citron, concerned about the asymmetrical effect of surveillance on women and sexual minorities,[124] and Johnson, writing in a pathbreaking scholarly tradition highlighting racial disparities in data collection and use,[125] deftly argue that privacy is about power and justice, not about control. Neil Richards and Woodrow Hartzog, who have also conceptualized privacy in terms of trust, vulnerability, and discretion, would impose on information industries fiduciary duties of care and loyalty, as defined by the common law.[126] Hartzog has also called for leveraging tort, contract, and consumer protection law to regulate manipulative, data-extractive platform design.[127] Cohen argues that we must empower public institutions and directly regulate an internet business model that incentivizes mass data collection at scale.[128] Scholars should continue in this tradition. Recognizing the second wave's limitations, privacy scholars and policymakers should look beyond the narrow confines of what passes for privacy regulation in the U.S. and consider new legal paradigms that can rein in data extraction and its attendant power asymmetries and injustices. In other words, even though only a few second wave proposals have been enacted, scholars must start thinking about a third wave.

## CONCLUSION

Privacy law is in the middle of a second wave. New laws and proposals are shifting privacy law from a first wave — a self-regulatory regime

---

[122] WALDMAN, *supra* note 114.

[123] HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010).

[124] Citron, *Sexual Privacy*, *supra* note 110, at 1890-93.

[125] Kristin Johnson, *Privacy in a Pandemic*, B.U. L. REV. (forthcoming 2021); *see also, e.g.*, RUHA BENJAMIN, RACE AFTER TECHNOLOGY (2019) (demonstrating how technologies reinforce White Supremacy while appearing neutral); KHIARA M. BRIDGES, THE POVERTY OF PRIVACY RIGHTS 10 (2017) (highlighting the routine ways the state invades the privacy of poor mothers on public assistance).

[126] Neil M. Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. (forthcoming 2021).

[127] WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 7-9 (2018).

[128] COHEN, *supra* note 32, at 238-68.

focused on notice, transparency, and choice — to managerialized compliance. This essay took a novel, ground up approach, creating a taxonomy that distinguished first and second waves on three metrics: practices, governance, and animating ideologies. In so doing, it identified striking uniformity among second wave practices.

The essay then posed timely questions for future research. Whether we can achieve the kind of substantive results we need — not just stronger privacy protections, but also an end to the information economy's role in perpetuating systemic injustices — is an open question. It is not clear that the second wave is up to the task. A third may be necessary. Either way, we must start to change our perspectives by understanding the risks of privacy law's current approach and envisioning a better, fairer, and more just path.