Who's Protecting Your Personal Data?: Leveraging the National Institute of Standards and Technology in the U.S. Data Privacy Regulatory Regime

ELANA EGRI-THOMAS*

The data privacy landscape in the United States is ineffective and fragmented across state lines. There is no federal data privacy law or data protection administrative agency. The state data privacy laws that do exist are heavily influenced by the tech industry and ignore substantive harms to consumers. Privacy scholars argue that given the power imbalance and information asymmetry between consumers and companies, consumers cannot exercise meaningful control over their data while online.

Missing from the conversation surrounding potential solutions to the data privacy landscape is the National Institute of Standards and Technology (NIST) and the NIST Privacy Framework. Due to the lack of federal action, companies use the Privacy Framework as a baseline for their privacy programs, and at least one state privacy law incorporates it. But the process by which NIST created the Privacy Framework was limited, failing to consider structural harms or equity considerations resulting in an industry-friendly framework.

This Note argues that NIST should redevelop the Privacy Framework to address social harms and alleviate the need for federal action by engaging with all relevant stakeholders and considering critiques and potential alternatives to current data privacy laws. Part I of this Note addresses the current data privacy landscape. Part II surveys critiques of data privacy laws. Part III outlines the history and purpose of NIST, the creation of its Privacy Framework, and the role NIST could play in the data privacy

* Note Editor, Colum. J.L. & Soc. Probs., 2024–2025. J.D. Candidate 2025, Columbia Law School. The author thanks her note advisor, Professor Daniel Richman, and the editorial staff of the *Columbia Journal of Law & Social Problems* for their support and helpful feedback.

realm. Part IV recommends a process NIST should engage in to reformulate the Privacy Framework.

CONTENTS

INTRODUCTION

Companies collect a vast amount of personal information[1] online in exchange for services.[2] Big technology companies like Alphabet and Meta ("big tech") can use personal information in ways that cause irreparable harm. Personal information can be used to exploit and manipulate consumers, influence voting tendencies, deny employment opportunities, increase insurance rates, contribute to identity theft, facilitate online discrimination of marginalized communities, and harm dignitary interests through the unwanted sharing of sensitive or intimate information.[3] Data privacy laws are intended to regulate the collection and use of this personal information.[4]

Despite being the global leader of big tech,[5] the United States has a limited federal data privacy regulatory regime.[6] There is no data privacy administrative agency[7] nor comprehensive federal data privacy regulation.[8] Congress has been unable to pass a federal data privacy law due to disagreements surrounding the specific requirements of data privacy legislation and federalism

---

1. *See* Cal. Civil Code § 1798.140(v)(1) (West 2025) (defining "personal information" as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household"). Personal information and personal data are used interchangeably throughout this Note.

2. *See* Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 1, 1 (2020).

3. *See infra* Part I.C.

4. Federal laws dealing with protected health information, children's information, or financial information are outside the scope of this Note, which is specific to data privacy as it relates to personal information.

5. *See* Leonard Lee, *The Future of U.S. Technology Leadership*, FORBES (Apr. 27, 2023), https://www.forbes.com/councils/forbestechcouncil/2023/04/27/the-future-of-us-technology-leadership/.

6. *See* STEPHEN P. MULLIGAN & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., IF11207, DATA PROTECTION AND PRIVACY LAW: AN INTRODUCTION (2022).

7. *See id.* at 2 (observing that the FTC is seen as the leading data protection enforcement agency, but it has its limitations); *see also The U.S. Urgently Needs a Data Protection Agency*, ELEC. PRIV. INFO. CTR., https://epic.org/campaigns/dpa/ [https://perma.cc/M2AA-B77B].

8. *See* American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022); CHRIS D. LINEBAUGH ET AL., CONG. RSCH. SERV., LSB11161, THE AMERICAN PRIVACY RIGHTS ACT 1 (2024); *see also* Müge Fazlioglu, *U.S. Privacy Legislation in 2023: Something Old, Something New?*, INT'L ASS'N OF PRIV. PROS. (July 26, 2023), https://iapp.org/news/a/u-s-federal-privacy-legislation-in-2023-something-old-something-new/ [https://perma.cc/8ZZX-3Z39].

concerns.[9] The United States lags behind other governments, especially the European Union, in regulating data privacy.[10] Without a federal data privacy law, the data privacy landscape in the United States is fragmented along state lines. In the last decade, 19 states have passed laws regulating the collection and use of personal information.[11] Generally, states' data privacy laws give consumers the right to access and delete their personal information collected by companies and opt out of the sale of their personal information.[12]

The state data privacy laws that do exist are heavily influenced by the tech industry[13] and promote privacy self-regulation, which requires individuals to manage their own data privacy online by reading data privacy notices, choosing their privacy preferences, and consenting to the use of their data.[14] Many privacy scholars critique this model of data privacy because consumers lack meaningful control over the use or dissemination of their personal information.[15] Information asymmetries stemming from power and wealth disparities between companies and consumers complicate personal data privacy management.[16] While companies are financially incentivized to manipulate consumers into consenting to the use of their personal data, consumers do not have the requisite knowledge or time to control their personal data use online.[17]

---

9. Due to federal inaction, many states have passed data privacy laws and Congress is reluctant to pass a federal data privacy law that would preempt state privacy laws. *See* Joseph Duball, *State Views on Proposed ADPPA Preemption Come into Focus*, INT'L ASS'N OF PRIV. PROS. (Sept. 27, 2022), https://iapp.org/news/a/state-level-views-on-proposed-adppa-preemption-come-into-focus/ [https://perma.cc/568H-YBR9].

10. *See generally* Regulation 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, 2016 O.J. (L 119) (EU) [hereinafter "GDPR"].

11. *See* C. Kibby, *US Privacy Legislation Tracker*, INT'L ASS'N OF PRIV. PROS., https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ [https://perma.cc/5QRD-JK3V] (Nov. 18, 2024).

12. *See State Laws Related to Digital Privacy* (2022), NAT'L CONF. OF STATE LEGISLATURES, https://www.ncsl.org/technology-and-communication/state-laws-related-to-digital-privacy [https://perma.cc/4QM9-BU7Z] (June 7, 2022).

13. *See* Brendan Bordelon & Alfred Ng, *Tech Lobbyists Are Running the Table on State Privacy Laws*, POLITICO (Aug. 16, 2023, 4:30 AM), https://www.politico.com/news/2023/08/16/tech-lobbyists-state-privacy-laws-00111363 [https://perma.cc/RAC7-JU8D].

14. *See* NAT'L CONF. OF STATE LEGISLATURES, *supra* note 12; *see also* Kibby, *supra* note 11.

15. *See infra* Part II.a.

16. *See infra* Part II.b.

17. *See infra* Part II.a.

In lieu of a federal data privacy law, the National Institute of Standards and Technology (NIST) Privacy Framework has been filling the gap for national privacy standards. NIST is a non-regulatory entity within the Department of Commerce that creates technical standards.[18] Created in response to industry requests in 2020,[19] the NIST Privacy Framework provides guidelines for voluntary best practices companies can follow. Although NIST claimed to consider input from all stakeholders, the NIST Privacy Framework primarily contains procedural suggestions for industry without acknowledging broader notions of data privacy. The Framework, for example, fails to address equity considerations or the harms accruing to individual consumers that can stem from a lack of data privacy protections.[20] This inattention to broader notions of data privacy is increasingly important as NIST begins to play a more influential role in the data privacy regulatory realm. Increasingly, companies have drawn on the Privacy Framework to create their privacy procedures and policies.[21] Tennessee has even incorporated it into its state data privacy law as an affirmative defense to privacy claims.[22] Tennessee's embrace of the NIST

18. *See About NIST*, NAT'L INST. OF STANDARDS & TECH. (Jan. 11, 2022), https://www.nist.gov/about-nist [https://perma.cc/E7S4-33ED].

19. *See* NAT'L INST. OF STANDARDS & TECH., NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT, VERSION 1.0 i (2020) [hereinafter NIST PRIVACY FRAMEWORK]; Walter Copan, Director, Nat'l Inst. of Standards & Tech., Keynote Address at Center for Strategic and International Studies Event: A Conversation on the NIST Privacy Framework 3 (Feb. 19, 2020) (NIST director Walter Copan describing how "industry stakeholders" like IBM requested that NIST create a privacy framework in response to major privacy breaches and increasing global regulations in 2018).

20. *See Cybersecurity & Privacy Stakeholder Engagement,* NAT'L INST. OF STANDARDS & TECH. (Aug. 7, 2023), https://www.nist.gov/cybersecurity/cybersecurity-privacy-stakeholder-engagement [https://perma.cc/RVD2-YGBE].

21. *See generally* Jamie Danker, *Spotlight on the NIST Privacy Framework: Three-Years Old and Making an Impact*, CTR. FOR CYBERSECURITY POL'Y & L. (May 1, 2023), https://www.centerforcybersecuritypolicy.org/insights-and-research/spotlight-on-the-nist-privacy-framework-three-years-old-and-making-an-impact [https://perma.cc/G2W2-CPNE] (reporting that the "framework is gaining traction" following case studies); Privacy Abbreviated, *Business Case for the NIST Privacy Framework*, BBB NAT'L PROGRAMS (June 28, 2023), https://bbbprograms.org/media-center/pd/priv-nist-privacy-framework [https://perma.cc/H8JY-BXE8] (the head of privacy and governance at Doordash discussed real-world applications of the NIST Privacy Framework and its benefits); *Privacy Framework Perspectives and Success Stories*, NAT'L INST. OF STANDARDS & TECH. (Oct. 3, 2023), https://www.nist.gov/privacy-framework/getting-started-0/perspectives-and-success-stories [https://perma.cc/LTL7-LVKG] (companies from various industries providing testimonials about the NIST Privacy Framework).

22. *See* H.B. 1181, 113th Gen. Assemb., Reg. Sess. (Tenn. 2023). In Tennessee, companies can avoid liability by showing they aligned with the NIST Privacy Framework in response to a privacy violation. *See id.*; *see also* F. Paul Pittman et al., *Tennessee Passes*

Privacy Framework signals that the framework is seen as a reliable legal standard.

By default, NIST has been playing a greater regulatory role in data privacy than originally envisioned due to the lack of a federal data privacy law or data protection agency.[23] NIST can be a source of productive regulation and alleviate the need for immediate federal action by Congress or the executive branch. This Note argues that NIST should reconsider the creation process of the Privacy Framework in light of its potential use as a legal standard.[24] In order to construct a democratically accountable Privacy Framework, NIST should facilitate a process that considers all stakeholders' views—including consumer advocates, public interest organizations, academia, and industry—and the shortfalls of current data privacy laws. Part I of this Note provides a brief overview of the current data privacy landscape, while Part II surveys critiques of U.S. data privacy laws. Part III outlines the history and purpose of NIST, the process by which NIST created the Privacy Framework, and the role NIST could play in the data privacy regulatory regime. Part IV recommends a process NIST should engage in to reformulate a Privacy Framework that can be used as a legal standard.

I. THE U.S. DATA PRIVACY REGULATORY LANDSCAPE

The current U.S. data privacy landscape is fragmented across state lines for lack of a federal data privacy law or data privacy administrative agency.[25] These state laws are heavily influenced by the tech industry and promote privacy self-regulation.[26] A privacy self-regulation model requires companies to provide consumers with privacy notices explaining how they will use their data, but puts the responsibility on the individual to read, understand, and consent to the use of their data.[27] Companies benefit financially from personal data collection and use, which

---

Comprehensive Privacy Law, WHITE & CASE (June 23, 2023), https://www.whitecase.com/insight-alert/tennessee-passes-comprehensive-data-privacy-law [https://perma.cc/2YSV-PHZV].

23. *See* MULLIGAN & LINEBAUGH, *supra* note 6, at 2.

24. *See* Pittman et al., *supra* note 22.

25. *See* MULLIGAN & LINEBAUGH, *supra* note 6, at 2.

26. *See* Bordelon & Ng, *supra* note 13.

27. *See* Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 5 (2021).

leads to information asymmetries that inhibit individuals from controlling the use of their personal data.[28] Due to the current failures of data privacy laws, consumers are susceptible to serious harm. Many data privacy scholars critique the current notice and consent structure of data privacy laws and recommend seeing data privacy as a collective issue with broader social harms.[29]

A. THE FEDERAL DATA PRIVACY REGIME & THE COMPARATIVE PERSPECTIVE

The United States regulates data use by sector, including the use of financial, health, and children's data, but there is no federal regulation for the use of personal data.[30] A federal data privacy law proposed in 2022, the American Data Privacy and Protection Act (ADPPA), would have restricted companies more than most state data privacy laws, but proposed a similar notice and consent structure.[31] The ADPPA would prohibit targeted advertising for youth, create a private right of action for violations, and include an explicit civil rights provision that would proscribe covered entities from discriminating based on protected characteristics.[32] In April 2024, Congress released a joint draft federal data privacy law, the American Privacy Rights Act (APRA), that incorporates many of the rights and obligations of the ADPPA.[33] Unlike the ADPPA, the APRA gives individuals the ability to opt out of certain algorithms and does not expressly preserve certain state data privacy laws.[34] At the end of the 2024 legislative session, the proposed bill was in the House Committee on Energy and Commerce.[35]

The United States' inability to pass a comprehensive federal data privacy law that holds companies accountable is particularly unsettling when compared to the European Union, which has a robust data privacy regulatory regime.[36] The European Union's

---

28. *See* Anita L. Allen, *Dismantling the "Black Opticon": Privacy, Race Equity, and Online Data Protection Reform*, 131 YALE L. J. 907, 908 (2022).

29. *See infra* Part II.b.

30. *See* MULLIGAN & LINEBAUGH, *supra* note 6, at 2.

31. *See* JONATHAN M. GAFFNEY ET AL., CONG. RSCH. SERV., LSB10776, OVERVIEW OF THE AMERICAN DATA PRIVACY AND PROTECTION ACT, H.R. 8152 (2022).

32. *See id*.

33. *See* LINEBAUGH ET AL., *supra* note 8.

34. *See id*.

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

36. *See generally* ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD 132 (2020).

General Data Protection Regulation (GDPR) is one of the most stringent data privacy regulations in the world, applying to any entity that collects or processes personal data of E.U. residents.[37] Considering many companies operate internationally, U.S. senators have called for GDPR requirements to apply to U.S. citizens or to create a "U.S. GDPR."[38] While companies operating in the European Union need to comply with the GDPR, the right to privacy and the respective legal systems in the United States and the European Union differ such that it is unlikely the United States will adopt a data privacy law that is as rights-protective as the GDPR.[39] While the U.S. Constitution does not include an explicit right to privacy,[40] the EU Charter of Fundamental Rights has enshrined data privacy and protection as a fundamental human right.[41]

Although the United States has not established a federal data privacy administrative agency, the Federal Trade Commission (FTC) regulates deceptive data privacy practices. The FTC can enforce companies' privacy policies through its authority to monitor unfair and deceptive trade practices under Section 5(a) of the FTC Act.[42] The FTC focuses on whether an organization is

37. *See* GDPR, *supra* note 10; *A User-Friendly Guide to the General Data Protection Regulation (GDPR)*, GDPR EU, https://www.gdpreu.org/ [https://perma.cc/43L2-587U] ("The [GDPR] is one of the strictest and most wide-ranging data protection measures in the world.").

38. Emmanuel Pernot-Leplay, *EU Influence on Data Privacy Laws: Is the US Approach Converging with the EU Model?*, 18 COLO. TECH. L.J. 25, 121 (2020).

39. *See* Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C.L. REV. 1687, 1727–28 (2020) (arguing that the GDPR is necessary in the European Union to "vindicate fundamental rights," but "consumer-law protections like the FTC Act's prohibition on unfair and deceptive trade practices are not compelled by the U.S. Constitution"); *Data Protection*, EUR. DATA PROT. SUPERVISOR, https://www.edps.europa.eu/data-protection/data-protection_en [https://perma.cc/2AZ7-3RBV].

40. *See* U.S. CONST. amend. I (right to free speech and association); U.S. CONST. amend. III (right to not quarter soldiers); U.S. CONST. amend. IX (right against unreasonable searches and seizures); *see also* Hartzog & Richards, *supra* note 39, at 1728 ("American constitutional law protects privacy against the government implicitly in a few areas, including the First Amendment's right to anonymous expression, the Third Amendment's protection against the quartering of soldiers in private homes during peacetime, the Fourth Amendment's "reasonable expectation of privacy" against government searches and seizures, and the Fifth and Fourteenth Amendments' substantive due process rights to information privacy and decisional autonomy."); *cf.* Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501, 1505 (2015) (arguing that data privacy regulations are consistent with the First Amendment).

41. *See* Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 1.

42. *See A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N, https://www.ftc.gov/about-

complying with their own privacy terms, rather than determining if certain data practices should be proscribed.[43] The FTC's litigation nearly always results in settlement agreements.[44] Publicized FTC settlements can serve a precedential role akin to traditional common law rulings.[45] Companies look to previous settlements to identify and avoid activities triggering enforcement.[46]

Data privacy is also regulated through the common law.[47] There are four privacy torts—intrusion upon seclusion, public disclosure of private facts, publicity placing a person in false light, and misappropriation of name or likeness, which in many states is the right of publicity.[48] In the internet age, however, federal privacy claims often fail because consumer plaintiffs cannot establish standing.[49] In data breach cases implicating privacy rights, the courts are split on whether there needs to be an actual showing of monetary damage from identify theft to establish a particularized injury in fact for standing, or if the possibility of

---

ftc/mission/enforcement-authority [https://perma.cc/2GWT-FM38] (May 2021) [hereinafter *Overview of FTC Authority*].

43. *See* Daniel Susser, *Notice After Notice-And-Consent: Why Privacy Disclosures Are Valuable Even if Consent Frameworks Aren't*, 9 J. INFO. POL'Y 148, 154 (2019).

44. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy,* 114 COLUM. L. REV. 583, 585 (2014).

45. *See id*. at 621.

46. *See id.*

47. *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) (arguing that there is a right to privacy at common law and included the nature of the right, its limitations, and remedies).

48. *See* RESTATEMENT (SECOND) OF TORTS, §§ 652B, 652D, 652E, 652C (AM. L. INST. 1977).

49. Under Article III of the Constitution, to establish standing a plaintiff must show (1) injury in fact, (2) causation between plaintiff's injury and defendant's actions, and (3) redressability. *Article III Standing*, ELEC. PRIV. INFO. CTR., https://epic.org/issues/consumer-privacy/article-iii-standing/ [https://perma.cc/4BQV-EG43]. There is a similar standing obstacle in state court because not all states recognize the privacy torts and most state data privacy laws do not include a private right of action. *See* Cheryl Saniuk-Heinig, *Private Rights of Action in US Privacy Legislation*, INT'L ASS'N OF PRIV. PROS. (May 2024), https://iapp.org/resources/article/private-rights-of-action-us-privacy-legislation/#state-laws-and-pras [https://perma.cc/JXK8-SJDF]; *cf.* TransUnion LLC v. Ramirez, 594 U.S. 413, 442 (2021) (holding that only the plaintiffs whose credit reports were actually disclosed to third parties, causing harm, had standing to sue under the Fair Credit Reporting Act (FCRA)). In *TransUnion*, the Court emphasized the need for non-speculative harm that can be analogized to a common law harm, such as loss of income. *See id.* at 438–42. Even though *TransUnion* dealt with FCRA, the impact of *TransUnion* is that without a tangible harm—common in a privacy violation that has psychological, but not necessarily physical impacts—plaintiffs will have difficulty establishing standing. *See id.* at 453 (Thomas, J., dissenting).

identity theft is enough.[50] Generally, standing analysis makes it difficult for individuals to vindicate their privacy rights at common law.[51] Despite potential privacy claims at common law and in individual FTC settlements, the data privacy regulatory environment remains limited by its emphasis on sectoral regulation and deceptive data practices. This creates a significant gap in the data privacy regulatory regime that states are attempting to address through state data privacy laws.

B. STATE DATA PRIVACY LAWS

Thus far, only 19 states have implemented data privacy laws.[52] In 2018, California passed the first state data privacy regulation in the United States, the California Consumer Privacy Act (CCPA).[53] The CCPA, as amended by the California Privacy Rights Act (CPRA), gives California consumers the right to know what information companies collect about them, delete or correct that information, opt out of the sale of their personal information, and limit the use and disclosure of their sensitive personal information.[54]

The CPRA is similar to the GDPR, which applies to any entity that collects or processes personal data of E.U. residents.[55] But unlike the GDPR, California's CPRA only applies to companies that do business in California.[56] Other state data privacy laws also

---

50. *Compare* Reilly v. Ceridian Corp., 664 F.3d 38, 41 (3d Cir. 2011) (granting motion to dismiss because of the Plaintiff's failure to "adequately allege the damage, injury, and ascertainable loss elements of their claims"), *with* In re Zappos.com, Inc., 888 F.3d 1020, 1029 (9th Cir. 2018) (holding that a showing of mere "increased risk of future identity theft" is sufficient for Article III standing).

51. *See supra* text accompanying note 49.

52. *See* Kibby, *supra* note 11.

53. *See California Consumer Privacy Act (CCPA)*, STATE OF CAL. DEPT. OF JUST., https://oag.ca.gov/privacy/ccpa [https://perma.cc/82MD-2MTY] (Mar. 13, 2024).

54. *See id.* California enacted the CPRA in 2020. *See id.*

55. *See* GDPR, *supra* note 10.

56. *See* California Consumer Privacy Act, CAL. CIV. CODE § 1798.100 (West 2018). The CCPA applies to for-profit businesses that do business in California and meet any of the following requirements: have a gross annual revenue of over $25 million; buy, sell, or share the personal information of 100,000 or more California residents, households, or devices; or derive 50% or more of their annual revenue from selling California residents' personal information. *See id.* § 1798.140. The California Office of Attorney General defines "doing business" broadly and has stated that the phrase "should be given meaning according to the plain language of the words and other California law." Cathy Cosgrove, *Top-10 Operational Impacts of the CPRA: Part 2—Defining 'Business' Under the Law*, INT'L ASS'N OF PRIV. PROS. (Dec. 22, 2020), https://iapp.org/news/a/cpras-top-operational-impacts-part-2-defining-business [https://perma.cc/G4GB-9F5R]. "Doing business" is defined in California's

only apply to companies that conduct businesses in that state, creating a disjointed data protection landscape across the country. In addition to California, 18 other states, including Colorado, Virginia, and Utah, have passed data privacy laws, some of which are already in effect or soon will be.[57] Although more states are in the process of passing data privacy laws, 15 states have no data privacy law at all.[58] This means that over the next five years, companies conducting business nationwide will likely need to comply with about 23 different state data privacy laws.[59] Companies may have different obligations in different states and consumers may have greater privacy rights in certain states compared to others.[60] For example, some states require companies to receive opt-in consent to process consumers' sensitive personal information or allow them to opt out of automated decision making.[61] So far, the CPRA is the only state data privacy law that includes a private right of action.[62] Maryland and Minnesota's state data privacy laws are the only ones that include an explicit civil rights provision, prohibiting the use of personal information to discriminate based on protected characteristics.[63]

Although distinct, the various state data privacy laws are structured similarly to the CPRA and follow the same notice and consent structure.[64] While the specific rights afforded consumers may differ by state, each law generally gives consumers data privacy rights and requires companies to provide basic safeguards in exchange for collecting and using consumers' personal information.[65] For example, each law gives consumers the right to

---

Revenue and Tax Code as "actively engaging in any transaction for the purpose of financial or pecuniary gain or profit." CAL. REV. & TAX CODE § 23101(a).

57. *See* Kibby, *supra* note 11.

58. *See id.*

59. Similarly, regional businesses will need to comply with more than one state data privacy law. *See id.*

60. *See* CAITRIONA FITZGERALD ET AL., ELEC. PRIV. INFO. CTR., THE STATE OF PRIVACY: HOW STATE "PRIVACY" LAWS FAIL TO PROTECT PRIVACY AND WHAT THEY CAN DO BETTER 6 (2024), https://s3.documentcloud.org/documents/24400016/state-of-privacy-feb-2024.pdf [https://perma.cc/F946-SNZJ].

61. *See* Kibby, *supra* note 11.

62. Without a private right of action, consumers cannot bring their privacy claims to state court. *See* Saniuk-Heinig, *supra* note 49.

63. *See State Data Privacy Laws & Civil Rights Protections*, THE LEADERSHIP CONF. ON CIV. & HUM. RTS., https://civilrights.org/state-data-privacy-laws/ [https://perma.cc/J5SX-CPG3].

64. *See* Ari Ezra Waldman, *Privacy, Practice, and Performance*, 110 CAL. L. REV. 1221, 1224 (2022); *infra* Part II.a.

65. *See* Kibby, *supra* note 11.

know the personal information collected about them, delete that information, or opt out of allowing the company to share their personal information. This also includes business obligations such as providing notice, receiving consent, and conducting risk assessments.[66] The procedural requirements in these laws, such as processes and procedures to implement, mirror each other.[67]

Despite the state data privacy laws in place, consumers are still vulnerable to the harms that stem from the lack of a robust data privacy regulatory regime. The remainder of Part I lays out the risks of failing to regulate data privacy.

C. THE HARMS FROM FAILING TO REGULATE PERSONAL DATA COLLECTION AND USE

Mining large amounts of personal data can be financially lucrative. By collecting consumers' personal data, companies can predict and manipulate consumers' behavior to better market towards them, potentially increasing their purchases and creating massive profits.[68] Given these incentives, companies collect as much personal information as possible, often without consumers' knowledge.[69] Potential risks of failing to regulate the collection and use of personal information are identity theft, secret surveillance of consumers, the spread of misinformation, interference with dignitary interests, negative impact on mental health, and algorithmic discrimination.[70]

Fewer than 20 states have enacted comprehensive data privacy laws, but the majority of those laws do not prohibit the discriminatory use of data, and only two states have explicit civil

66. *See id*.

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

68. *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR HUMAN FUTURE AT THE NEW FRONTIER OF POWER 14–15 (2019).

69. *See id*.

70. *See id*. (secret surveillance); FITZGERALD ET AL., THE STATE OF PRIVACY, *supra* note 60, at 9 (identity theft); Lawrence J. Trautman, *Governance of the Facebook Privacy Crisis,* 20 PITT. J. TECH. L. & POL'Y 43, 93 (2020) (spread of misinformation); Danielle Keats Citron, *A New Compact for Sexual Privacy*, 62 WM. & MARY L. REV. 1763, 1766, 1777, 1794, 1797, 1798 (2021) (interference with dignitary interests); *State Data Privacy Laws & Civil Rights Protections*, *supra* note 63; *see also* Allen, *Black Opticon*, *supra* note 28, at 914 (algorithmic discrimination); Cecilia Kang & David McCabe, *'Your Product Is Killing People': Tech Leaders Denounced over Child Safety*, N.Y. TIMES (Jan. 31, 2024), https://www.nytimes.com/2024/01/31/technology/senate-child-safety-social-media.html (on file with the *Columbia Journal of Law & Social Problems*) (negative impact on mental health).

rights protections.[71] In 2022, on behalf of the Leadership Conference on Civil and Human Rights, 57 civil rights, consumer protection, and civil liberties organizations wrote a letter to Congress urging lawmakers to pass a comprehensive data privacy law that prevents discrimination based on data and protects civil rights online.[72] Although many of the state data privacy laws mention civil rights and discrimination, they fail to include "a prohibition on using personal data to discriminate on the basis of protected characteristics," leaving marginalized people, especially people of color, vulnerable.[73] Without a specific civil rights provision, data indicating one's race can be used to deny access to resources online, job opportunities, or health benefits.[74] Privacy laws also do not address biased algorithms. Companies use algorithms to make predictions; these predictions, however, can often perpetuate bias and discrimination.[75] The risk of biased algorithms exists in many areas, such as the employment or lender contexts, as well as in facial recognition used to assist in criminal investigations.[76]

In addition to algorithmic decision making, companies can create automated user profiles that can predict and influence future purchases or even voting patterns. Scholar Shoshana

---

71. *See State Data Privacy Laws & Civil Rights Protections*, *supra* note 63.

72. *See* Support a Comprehensive Consumer Privacy Law that Safeguards Civil Rights Online, THE LEADERSHIP CONF. ON CIV. & HUM. RTS. (May 25, 2022), https://civilrights.org/resource/support-a-comprehensive-consumer-privacy-law-that-safeguards-civil-rights-online/ [https://perma.cc/Y69E-KWQX].

73. *State Data Privacy Laws & Civil Rights Protections*, *supra* note 63; *see also* Allen, *Black Opticon*, *supra* note 28, at 924.

74. *See* Cristiano Lima-Strong, *More States Are Passing Privacy Laws. Few Tackle Civil Rights.*, WASH. POST (Sept. 24, 2024), https://www.washingtonpost.com/politics/2024/09/24/more-states-are-passing-privacy-laws-few-tackle-civil-rights/ (on file with the *Columbia Journal of Law & Social Problems*); *see also* Allen, *Black Opticon*, *supra* note 28, at 920.

75. *See* Allen, *Black Opticon*, *supra* note 28, at 923 ("Discriminatory practices (i.e., those that rely on racialized sorting by humans and machines that reinforce racism and deny equal access to services and opportunities) thrive on online platforms."). For example, if an algorithm is used to predict future recidivism rates but the input data includes a majority of people of color, the algorithm will predict that people of color have a higher risk of recidivism. *See* Ari Ezra Waldman, *Power, Process, and Automated Decision-Making*, 88 FORDHAM L. REV. 613, 621–22 (2019).

76. *See* Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html (on file with the *Columbia Journal of Law & Social Problems*); *see also* Waldman, *Automated Decision-Making*, *supra* note 75, at 632. In a 2016 report, the American Civil Liberties Union found that social media platforms shared users' information with Geofeedia, a location analytics company. Police departments used Geofeedia's access to social media posts and facial recognition technology to identify and arrest Black Lives Matter protestors. *See* Allen, *Black Opticon*, *supra* note 28, at 918.

Zuboff describes the monetization of personal information as "surveillance capitalism."[77] She writes that Google was the first company to employ surveillance capitalism to enhance its business model of tracking consumers and monetizing targeted advertisements.[78] By tracking individuals across web searches and reading emails, Google legally invaded individuals' privacy to predict future behavior and market towards that predicted behavior, thus increasing profit margins.[79] Other companies employ these tools. For example, in the early 2000s, Target's marketing team identified women in their second trimester of pregnancy by combining a series of data sets; this ensured that Target could market more effectively to these women.[80]

Targeted advertising can, at times, be predatory.[81] Political micro-targeting is the use of harvested personal information and algorithms to influence voting patterns and election outcomes.[82] Political micro-targeting influenced individual voting patterns in the 2016 election of Donald Trump.[83] For example, Facebook facilitated the spread of misinformation surrounding the 2016 election because its limited security safeguards allowed Russian actors to promote election propaganda.[84] Facebook presented all articles on users' feeds as if they were factually accurate, regardless of the news source.[85] It targeted certain news articles

77. ZUBOFF, *supra* note 68, at 14–15.

78. *See id.*

79. *See id.* at 20.

80. *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html (on file with the *Columbia Journal of Law & Social Problems*).

81. For example, a whistleblower at Cambridge Analytica told the *London Observer*, "[W]e exploited Facebook to harvest millions of people's profiles and built models to exploit what we knew about them and target their inner demons." Daniel Susser et al., *Online Manipulation: Hidden Influences in a Digital World*, 4 GEO. L. TECH. REV. 1, 10–11 (2019). Discriminatory predation is the practice of using people of color's data to "lure them into making exploitative agreements and purchases." Allen, *Black Opticon*, *supra* note 28, at 925–26.

82. *See* Jacquelyn Burkell & Priscilla M. Regan, *Voting Public: Leveraging Personal Information to Construct Voter Preference*, *in* BIG DATA, POLITICAL CAMPAIGNING AND THE LAW: DEMOCRACY AND PRIVACY IN THE AGE OF MICRO-TARGETING 47, 59–60 (Normann Witzleb et al. eds., 2020); *see also* Susser et al., *Online Manipulation*, *supra* note 81, at 9–11 (describing how Cambridge Analytica tried to impact the 2016 U.S. presidential election).

83. *See* Trautman, *supra* note 70, at 95; Susser et al., *Online Manipulation*, *supra* note 81, at 10–11.

84. *See* Sheera Frenkel, et al., *Delay, Deny and Deflect: How Facebook's Leaders Fought Through Crisis*, N.Y. TIMES (Nov. 14, 2018), https://www.nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html (on file with the *Columbia Journal of Law & Social Problems*).

85. *See* Trautman, *supra* note 70, at 93.

to specific individuals based on their Facebook interactions in a way that amplified individual biases.[86] In 2021, Congress attempted to regulate political micro-targeting by prohibiting the dissemination of targeted political advertisements to individuals based on their personal information.[87] The bill has not been reintroduced since 2021.[88] Current data privacy regulations do not address the influence of algorithms on politics.[89]

In addition to the risk of surveilling consumers and contributing to the spread of misinformation, lack of data privacy protections can injure dignitary interests. Take, for example, the unwanted sharing of intimate sexual health information,[90] particularly in states with restricted access to abortion.[91] In 2021, Flo, a menstrual cycle tracker application, shared intimate personal health information for advertising purposes without users' knowledge.[92] Users thought they were sharing confidential fertility information with Flo for enhanced services. But, without user knowledge or consent, Flo shared this potentially incriminating information with Facebook and Google.[93] In states

---

86. *See id.*; *see also* YOCHAI BENKLER ET AL., NETWORK PROPAGANDA: MANIPULATION, DISINFORMATION, AND RADICALIZATION IN AMERICAN POLITICS 9 (2018).

87. *See* Banning Microtargeted Political Ads Act of 2021, H.R. 4955, 117th Cong. (2021).

88. *See id*.

89. *See California Consumer Privacy Act (CCPA)*, STATE OF CAL. DEP'T OF JUST., https://oag.ca.gov/privacy/ccpa [https://perma.cc/82MD-2MTY] (Mar. 13, 2024).

90. For example, in 2018, news reports claimed that Grindr provided third parties with users' HIV information without their knowledge. *See Grindr Shared Information About Users' HIV Status with Third Parties*, GUARDIAN (Apr. 3, 2018), https://www.theguardian.com/technology/2018/apr/03/grindr-shared-information-about-users-hiv-status-with-third-parties [https://perma.cc/XN8Z-TG8M]. In 2024, users filed a class action lawsuit in the UK, alleging the app shared users' HIV information for commercial purposes without their consent. *See* Jasper Jolly, *Lawsuit in London to Allege Grindr Shared Users' HIV Status with Ad Firms*, GUARDIAN (Apr. 22, 2024), https://www.theguardian.com/technology/2024/apr/22/lawsuit-in-london-to-allege-grindr-shared-users-hiv-status-with-ad-firms [https://perma.cc/6ELP-6LTM]. Reproductive health technology applications, which can track menstrual cycles, ovulation, and fertility, are prone to security problems and unknowingly share female sexual health information with third parties. *See* Shiona McCallum & Tom Singleton, *Period Trackers 'Coercing' Women into Sharing Risky Information*, BBC (May 15, 2024), https://www.bbc.com/news/articles/cmj6j3d8xjjo [https://perma.cc/2N24-BJEH].

91. *See* Citron, *New Compact*, *supra* note 70, at 1777.

92. *See* Ryan S. Houser, *"Guarding the Sanctity of Choice and Privacy:" Data Privacy and Abortion—The Next Frontier of the Fourth Amendment*, 21 NW. J. TECH. & INTELL. PROP. 201, 210 (2024).

93. *See* Alisha Haridasani Gupta & Natasha Singer, *Your App Knows You Got Your Period. Guess Who Told It?*, N.Y. TIMES (Jan. 28, 2021), https://www.nytimes.com/2021/01/28/us/period-apps-health-technology-women-privacy.html (on file with the *Columbia Journal of Law & Social Problems*). Following an FTC complaint, Flo settled with the FTC.

that criminalize abortions, this information can be used in related prosecutions, a major consequence that can stem from failing to regulate personal information collection and use.[94] The failure to regulate the use of personal information has also led to the prevalence of deepfakes and revenge porn online.[95]

Unregulated data collection and use increases the risk of identity theft and puts consumers' security at risk.[96] Because companies can collect a vast amount of personal information, store it for an unspecified time, and share it with third parties, there is a higher likelihood that the data will be exposed in a breach or used in a cybercrime.[97] Existing data privacy laws do not have data minimization requirements, resulting in companies collecting personal information beyond what is reasonably necessary to provide services and potentially exposing an extensive amount of data to hackers.[98]

The mental health and safety of children, in particular, can be severely negatively impacted when they share their personal information with online platforms. Because there are no restrictions on the information collected from children or how

---

The settlement requires Flo to receive consent before sharing users' personal health information with third parties and prohibits Flo from "misleading users about its data-handling practices." *Id*.

94. *See* Abigail Dubiniecki, *Post-Roe, Your Period App Data Could Be Used Against You*, FORBES (Nov. 25, 2024), https://www.forbes.com/sites/abigaildubiniecki/2024/11/14/post-roe-your-period-app-data-could-be-used-against-you/ [https://perma.cc/T6SN-AVSP] (reporting risks related to sharing intimate sexual health information with "femtech" applications due to the increase in abortion prosecutions and curtailment of reproductive rights).

95. *See* Citron, *New Compact*, *supra* note 70, at 1770. Deepfakes are fake videos that feature a person's face without their consent, which can be used in contexts including pornography. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-24-107292, SCIENCE & TECH SPOTLIGHT: COMBATING DEEPFAKES (2024), https://www.gao.gov/products/gao-24-107292 [https://perma.cc/4KVD-AS6F]. Revenge porn is the posting of pornographic photos or videos without consent. *See* Shelbie Marie Mora, Comment, *Revenge Porn: The Result of a Lack of Privacy in an Internet-Based Society*, MAINE STUDENT J. INFO. PRIV. L. (Oct. 15, 2022), https://sjipl.mainelaw.maine.edu/2022/10/15/revenge-porn-the-result-of-a-lack-of-privacy-in-an-internet-based-society/ [https://perma.cc/ABM8-AB5J]. The FTC has sued a revenge porn operator under Section 5 of the FTC Act for posting images of individuals and their personal information without their consent. *See FTC and Nevada Seek to Half Revenge Porn Site*, FED. TRADE COMM'N, (Jan. 9, 2018) https://www.ftc.gov/news-events/news/press-releases/2018/01/ftc-nevada-seek-halt-revenge-porn-site [https://perma.cc/SA6V-FJUG].

96. *See* FITZGERALD ET AL., THE STATE OF PRIVACY, *supra* note 60, at 9.

97. *See id*.

98. *See id.*; Kennedy Meda, *Identity Theft Is Being Fueled by AI & Cyber-Attacks*, THOMSON REUTERS (May 3, 2024), https://www.thomsonreuters.com/en-us/posts/government/identity-theft-drivers/ [https://perma.cc/CG5L-5G9K].

algorithms can then show content to them, children can be presented content that facilitates child sexual exploitation, exacerbates body image issues, and contributes to cyberbullying.[99] In 2023, the U.S. Surgeon General issued a statement that social media use is contributing to the youth mental health crisis.[100]

The thin data privacy protections in place do not effectively curtail big tech's personal information collection or use.[101] Through heavy lobbying, big tech companies have successfully stopped certain data privacy regulatory provisions at the state level.[102] The CPRA, California's data privacy law, remains the most stringent state data privacy law. But thanks to aggressive big tech lobbying, other state privacy laws are weaker and more industry friendly.[103] For example, reports suggest that Amazon lobbyists wrote Virginia's state data privacy law.[104] Under the law's provisions, consumers must submit individual requests to delete their data to each entity that could potentially have their data and consumers have no way to hold companies accountable in court for violating the privacy law.[105] Unsurprisingly, the Virginia law benefits the tech industry without adequately protecting

---

99. *See* Cecilia Kang & David McCabe, *'Your Product Is Killing People': Tech Leaders Denounced over Child Safety*, N.Y. TIMES (Jan. 31, 2024), https://www.nytimes.com/2024/01/31/technology/senate-child-safety-social-media.html (on file with the *Columbia Journal of Law & Social Problems*) (describing how, during an online child safety Senate Judiciary Committee hearing, members of the committee denounced tech leaders for prioritizing profits and ignoring its contributions to the rise in child sexual abuse, the youth mental health crisis, and the youth suicide rate); Susser et al., *Online Manipulation*, *supra* note 81, at 6 (a leaked internal Facebook document described how Facebook helped advertisers target vulnerable teenagers); Georgia Wells et al., *Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show*, WALL ST. J. (Sept. 14, 2021), https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739 (on file with the *Columbia Journal of Law & Social Problems*).

100. *See* Press Release, U.S. Dep't of Health & Hum. Servs., Surgeon General Issues New Advisory About Effects Social Media Use Has on Youth Mental Health (May 23, 2023), https://www.hhs.gov/about/news/2023/05/23/surgeon-general-issues-new-advisory-about-effects-social-media-use-has-youth-mental-health.html [https://perma.cc/2HWW-WT3B].

101. *See* FITZGERALD ET AL., THE STATE OF PRIVACY, *supra* note 60, at 15.

102. *See* Bordelon & Ng, *supra* note 13.

103. *See id.*

104. *See* Todd Feathers, *Big Tech Is Pushing States to Pass Privacy Laws, and Yes, You Should Be Suspicious*, THE MARKUP (Apr. 15, 2021), https://themarkup.org/privacy/2021/04/15/big-tech-is-pushing-states-to-pass-privacy-laws-and-yes-you-should-be-suspicious; Caitriona Fitzgerald, *A Proposed Compromise: The State Data Privacy and Protection Act*, ELEC. PRIV. INFO. CTR. 13–14 (Feb. 22, 2023), https://epic.org/a-proposed-compromise-the-state-data-privacy-and-protection-act/ [https://perma.cc/7WY3-Z572].

105. *See id.*

consumers.[106] Americans are rightfully uneasy about the collection of their personal information and feel they have very little control over what companies do with their data.[107] Given these failings, it is expected that there are many criticisms of U.S. data privacy laws.

II. CRITIQUES OF CURRENT DATA PRIVACY LAWS

This Part paints a high-level picture of the current critiques of the data privacy regulatory regime and its shortfalls. The criticisms can be grouped into two buckets: first, why the notice and consent structure in state data privacy laws does not effectively protect individual data privacy, and second, why data privacy should be seen as a collective problem.[108]

A. CRITICISMS OF THE NOTICE AND CONSENT STRUCTURE

Many scholars and lawmakers criticize the notice and consent structure of data privacy laws. An overarching critique is that putting the onus on individuals to control the use of their personal information on the internet is neither scalable nor adequate.[109] Professor Daniel Solove refers to this as privacy self-management.[110] Companies provide privacy notices to consumers and must receive user consent before using their personal information, but the individual must make difficult, split-second decisions about their privacy—whether via reading privacy notices, accepting cookies, opting out of the sale of personal

106. *See* Jeffrey Dastin et al., *Virginia is for Amazon Lovers*, REUTERS (Nov. 19, 2021), https://www.reuters.com/investigates/special-report/amazon-privacy-lobbying/ [https://perma.cc/C9NC-4TQD]; Fitzgerald, *A Proposed Compromise*, *supra* note 104.

107. *See* Colleen McClain et al., *How Americans View Data Privacy*, PEW RSCH. CTR. (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/ [https://perma.cc/E24J-YX2M].

108. The lack of data privacy protections negatively impacts all individuals in a way that cannot be individually remedied, and thus needs to be seen as a collective problem rather than an individual problem. *See* Waldman, *Privacy, Practice, and Performance*, *supra* note 64, at 1254; *see also* Susser et al., *Online Manipulation*, *supra* note 81, at 43 (noting that companies implementing unregulated manipulative tactics threaten autonomy and collective self-government).

109. *See* Solove, *Introduction*, *supra* note 67, at 1888–89; *see also* Thomas B. Norton, *The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model*, 27 FORDHAM INTELL. PROP. MEDIA & ENT. L. J. 181, 201 (2016).

110. *See* Solove, *Privacy Paradox*, *supra* note 27, at 5.

information, or changing their privacy settings.[111] Solove argues that it is nearly impossible for individuals to regulate the use of their personal information on every website they visit.[112] If one were to read every single relevant privacy notice, it would take 201 hours a year.[113] Even if the goal of data privacy regulation is to give consumers more control over their personal information, privacy self-management is not scalable to the extent necessary for the effective protection of data privacy.[114]

Privacy scholars also point out that consumers lack requisite understanding of privacy self-management.[115] Individuals fail to appreciate the inadequacy of data governance protections or realize that their data will be aggregated and analyzed to reveal information not shared.[116] Even if one individual does not consent to the sharing of their personal data, companies categorize individuals into like groups and subsequently market to those groups, ignoring individual online privacy preferences.[117] Data aggregators can create valuable and revealing profiles from combined pieces of personal information, yet individuals cannot properly evaluate each piece of personal information.[118] Because these problematic data practices are not regulated, it is impossible for individuals to exercise real control over their personal data at scale. Furthermore, studies show that individuals incorrectly

111. *See id.*; *see also* Norton, *supra* note 109, at 187–88 (noting that, even though consumers are given privacy policies, they rarely read them).

112. *See* Solove, *Privacy Paradox*, *supra* note 27, at 30.

113. *See id.* at 45; *see also* Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DAEDALUS 32, 34 (2011) (citing evidence suggesting consumers do not read privacy policies).

114. *See* Woodrow Hartzog, *The Case Against Idealising Control*, 4 EUR. DATA PROT. L. REV. 423, 428 (2018); Norton, *supra* note 109, at 188. Despite the failures of notice and consent, policy makers continue to promote the structure. *See* Richard Warner & Robert Sloan, *Beyond Notice and Choice: Privacy, Norms, and Consent*, SUFFOLK U.J. HIGH TECH. L. 1, 5 (2013) (discussing the FTC's endorsement of notice and choice).

115. *See* Solove, *Introduction*, *supra* note 67, at 1888; *see also* Norton, *supra* note 109, at 202; Susser, *Notice-and-Consent*, *supra* note 43, at 154; Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 I/S: J.L. & POL'Y FOR INFO. SOC'Y 1, 19 (2011); *see also* Anita L. Allen, *Protecting One's Own Privacy in a Big Data Economy*, 130 HARV. L. REV. F. 71, 73 (2016).

116. Although data aggregation and categorization are issues of data governance, data governance implicates data privacy concerns. *See* Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 603 (2021).

117. *See* Viljoen, *supra* note 116, at 12; Susser et al., *Online Manipulation*, *supra* note 81, at 32.

118. *See* Solove, *Privacy Paradox*, *supra* note 27, at 43–44; MacCarthy, *supra* note 115, at 19 (2011); Susser et al., *Online Manipulation*, *supra* note 81, at 10–11, 31.

think there are privacy protections in place that prohibit the use or selling of information when there are not.[119]

Given the knowledge gap between consumers and corporations, privacy scholars argue that consumers' control over their personal information is illusory.[120] Companies use dark patterns or manipulative tactics on their websites, coercively designed to deceive individuals into sharing their personal information.[121] For example, some companies display multiple checkboxes complicating the "unsubscribe" process,[122] or nudge users into sharing their personal information by displaying buttons that read "no thanks, I hate free stuff."[123] Although companies provide privacy policies to inform consumers how their personal data will be used once shared, these policies are often either too vague or overly complicated.[124] Consent online is either unwitting because consumers do not know what data practices they are agreeing to, or coerced because corporations manipulate consumers to share as much information as possible.[125] Because of the foregoing

---

119. *See* Solove, *Privacy Paradox*, *supra* note 27, at 19; Susser et al., *Online Manipulation*, *supra* note 81, at 32; *see also* Warner & Sloan, *supra* note 114, at 13, 18 (stating that personal information collected for one purpose may be used for a variety of other purposes).

120. *See* Hartzog, *supra* note 114, at 427; Susser, *Notice-and-Consent*, *supra* note 43, at 154; *see also* Warner & Sloan, *supra* note 114, at 18 (arguing that it is impossible for notices to include enough information to sufficiently inform consumers, rendering consent inadequate).

121. *See* Solove, *Privacy Paradox*, *supra* note 27, at 18; California Consumer Privacy Act, CAL. CIV. CODE § 1798.140(*l*) ("'Dark pattern' means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation."); *see also* Susser et al., *Online Manipulation*, *supra* note 81, at 43 ("[O]nline manipulation is aimed precisely at individual choosers, and it is the specific information about each target that enables online manipulators to exploit the target's vulnerabilities.").

122. In November 2024, the FTC promulgated a final "click-to-cancel" rule that would require companies to simplify the unsubscribe process for consumers. *See* 16 C.F.R pt. 425.6 (2024); *Federal Trade Commission Announces Final "Click-to-Cancel" Rule Making It Easier for Consumers to End Recurring Subscriptions and Memberships*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/news/press-releases/2024/10/federal-trade-commission-announces-final-click-cancel-rule-making-it-easier-consumers-end-recurring (Oct. 16, 2024).

123. *See* Neil M. Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U.L. REV. 961, 975 (2021); Susser et al., *Online Manipulation*, *supra* note 81, at 30.

124. *See* Neil M. Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U.L. REV. 1461, 1479–80, 1495 (2019); Norton, *supra* note 109, at 201. *But see* Susser, *Notice-and-Consent*, *supra* note 43, at 156 (arguing that although notices are currently insufficient for consumers to make informed consent, it is better than providing consumers with no information at all). "Quasi-informed citizen-consumers are preferable to mostly ignorant ones." *Id.*

125. *See* Richards & Hartzog, *Pathologies*, *supra* note 124, at 1486; Susser et al., *Online Manipulation*, *supra* note 81, at 43; *see also* Norton, *supra* note 109, at 203 (consumers

considerations, consumers are likely to agree to data sharing for reasons other than genuine meeting of the minds. Thus, under a fiction of consumer consent, corporations are able to use consumers' personal information in any way they see fit.[126]

B. DATA PRIVACY AS A COLLECTIVE PROBLEM

Privacy scholars argue that current data privacy regulations ignore that data privacy is a collective problem with broader societal impacts. Instead of seeing data privacy as a benefit to individuals by providing autonomy over personal data usage, scholars think that data privacy should be seen as an "element of a free and democratic society."[127] Professor Zeynep Tufekci argues that privacy is a public good because it is difficult for individuals to value their personal information appropriately or understand the risks of sharing their personal information.[128] Moreover, Professors Avi Goldfarb and Verina Que note the negative externalities inherent to providing personal information, such as sharing too much personal information or mistakenly sharing data that provides probabilistic information about another

---

cannot seek recourse through contract law if their personal information is used for reasons not agreed to in the privacy policy).

126. *See* Waldman, *Privacy, Practice, and Performance*, *supra* note 64, at 1257. For example, in 2019, Facebook moved to dismiss the lawsuit regarding Cambridge Analytica's unlawful mining of Facebook users' data. The judge asked if Facebook breaking a promise to not share user's personal data with third parties was an invasion of privacy. In response, Facebook pointed to users' consent, arguing that if users consent to sharing their data, Facebook can use that data and share it with third parties. *See id.* at 1257–58.

127. Solove, *Privacy Paradox*, *supra* note 27, at 41; *see* Waldman, *Privacy, Practice, and Performance*, *supra* note 64, at 1254; *see also* Susser, *Notice-and-Consent*, *supra* note 43, at 156–57 ("[C]ritics of notice-and-consent point out that the interests privacy protects are not only individual interests, but social or collective interests too."). Professors Daniel Susser, Beate Roessler, and Helen Nissenbaum also call attention to the resulting harm to autonomy when individual privacy choices are manipulated: "Since autonomy lies at the normative core of liberal democracies, the harm to autonomy rendered by manipulative practices extends beyond personal lives and relationships, reaching public institutions at a fundamental level." Susser et al., *Online Manipulation*, *supra* note 81, at 37; *see also* Allen, *supra* note 115, at 75 (arguing that privacy should be seen as a "public, communal good").

128. Tufekci has said, "Data privacy is more like air quality or safe drinking water, a public good that cannot be effectively regulated by trusting in the wisdom of millions of individual choices." Hartzog, *supra* note 114, at 430; *see also* Solove, *Privacy Paradox*, *supra* note 27, at 5. Other academics concur. "Priscilla Regan and Joel Reidenberg both argue, for instance, that privacy has social benefits. Julie Cohen argues that privacy is necessary for individual creativity and innovation, which in turn are necessary for ethical and cultural development. Lior Strahilevitz draws attention to the distributive effects of different privacy regimes. And for Nissenbaum, privacy is—in the first place—a set of social norms, not a set of individual decisions." Susser, *Notice-and-Consent*, *supra* note 43, at 156–57.

individual.[129] These negative externalities "may mean that even fully informed and rational consumers provide data to firms in excess of the welfare-maximizing amount," further supporting the conclusion that individual control is insufficient.[130]

To regulate the internet collectively, Professor Danielle Keats Citron proposes a cyber civil rights online legal regime.[131] She argues that cyber civil rights are necessary to protect against online harassment, discrimination, and threats that target women, people of color, and other vulnerable groups.[132] Building on Citron's framework, Professor Ari Ezra Waldman conceptualizes the business obligations in privacy regulations, such as the notice and consent requirements, as performative.[133] He argues that data privacy law itself has been reduced to the procedures that compliance professionals put in place, ignoring the substantive obligations of companies that are necessary to protect individuals' data privacy.[134] Professors Woodrow Hartzog and Neil Richards explain that this procedural focus "specifies what is needed to process data (whether consent or notification is needed, etc.)," while a substantive focus puts "limits on kinds or purposes of processing."[135] Waldman argues that regulators should "give advocacy organizations representing marginalized populations, and not corporations, a seat at the table" to promote cyber civil rights in data privacy laws.[136]

Tufekci, Goldfarb, Citron, and Waldman's critiques demonstrate how current data privacy regulations in the United States are failing at their purported goal of giving consumers control over the collection and use of their personal information

---

129. *See* Avi Goldfarb & Verina F. Que, *The Economics of Digital Privacy*, 15 ANN. REV. ECON. 267, 276 (2023). Professor Mark MacCarthy similarly argues that the imbalance of bargaining power and knowledge asymmetries result in collectors of personal information using the information in a way unknown to the data subject resulting in a privacy harm that is a negative privacy externality. *See* MacCarthy, *supra* note 115, at 19, 21.

130. Goldfarb & Que, *supra* note 129, at 279 (arguing that negative externalities occur when there is a transaction cost that neither party must pay; negative externalities can be addressed through government regulation).

131. *See* Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 64, 66 (2009).

132. *See id.*

133. *See* Waldman, *Privacy, Practice, and Performance*, *supra* note 64, at 1269.

134. *See id.* at 1241–42.

135. Richards & Hartzog, *Duty of Loyalty*, *supra* note 123, at 982.

136. Waldman, *Privacy, Practice, and Performance*, *supra* note 64, at 1277; *see also* Allen, *supra* note 115, at 76 ("Collectively, individuals can push for reforms and be critical of government.").

due to information asymmetries and power imbalances.[137] Merely focusing on individualized control is too narrow a conception of data privacy and ignores broader goals of equity. Although many data privacy scholars argue that the current data privacy regime should take on different forms, state legislators propose and pass data privacy laws that emphasize notice and consent, suggesting a failure to engage with these critiques.[138]

Given the fragmented state data privacy landscape, the lack of federal action, and the failure to engage with the above critiques in legislation, legislators should identify a federal institution to contribute productively to the data privacy regime. One potential answer is the National Institute of Standards and Technology (NIST). Missing from the debate about the current data privacy regime is the role of NIST and its Privacy Framework, as well as how it can improve.

III. THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

This Part discusses the history and purpose of NIST, the process by which NIST created the privacy framework, and the role NIST and its Privacy Framework can play in the data privacy landscape. In response to the fragmented data privacy landscape and requests from industry, in 2020, NIST created a voluntary Privacy Framework, which is increasingly popular amongst corporate America and has been incorporated in one state's data privacy law.[139] Because NIST did not envision the regulatory role

137. The notice and consent structure has been criticized by many additional privacy scholars not discussed in this note. *See, e.g.*, Norton, *supra* note 109 (arguing that notice and consent leaves consumers who suffer a privacy breach without legal recourse because privacy policies are not legally binding); MacCarthy, *supra* note 115 (negative privacy externalities present an obstacle to informed consent and recommending policymakers adopt an "unfairness" model instead); Susser, *Notice-and-Consent*, *supra* note 43 (although the role of consent should be minimized because it is ineffective, notice should still play a role in privacy regulations); Nissenbaum, *supra* note 113 (because consumers cannot give informed consent, privacy regulations should include substantive norms that constrain the personal information collected and shared online); Warner & Sloan, *supra* note 114, at 13, 18 (informational norms should govern online data collection and use rather than notice and consent).

138. *See* Waldman, *Privacy, Practice, and Performance*, *supra* note 64, at 1224; *see also* Nissenbaum, *supra* note 113, at 45 ("To leave the protection of privacy online to negotiations of notice-and-consent is not only unfair, it is to pass up a critical public policy opportunity that will have ramification for the shape and future of the Net.").

139. *See infra* Part III.b.

the Privacy Framework ultimately took on, the institute facilitated only a limited process in its creation.[140] Now that NIST is playing an expanded regulatory role, the process through which it created the Privacy Framework needs to be reconsidered so as to avoid inadvertent legal standard-making.

A. THE HISTORY AND PURPOSE OF NIST

NIST is a technical standards organization within the Department of Commerce.[141] NIST's mission is "to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in a way that enhances economic security and improves our quality of life."[142] Its focus on promoting industrial competitiveness supports the Department of Commerce's overarching goal of improving America's economy.[143] Although NIST lacks enforcement authority because it is not an agency with rulemaking power, it has an institutional reputation as a "neutral arbiter of technical standards."[144] A core value of NIST is to "work collaboratively to harness the diversity of people and ideas" to advance its mission.[145] Although NIST is not an organization of elected representatives, nor is there a legislative process guiding NIST's procedures, NIST adheres to an administrative notice and comment process similar to that required by the Administrative Procedure Act.[146]

NIST is the oldest physical laboratory in the United States. Congress created NIST—originally named the National Bureau of Standards (NBS)—in 1901 and moved the agency to the

140. *See id*.

141. *See* 15 U.S.C. § 272; *About NIST*, *supra* note 18.

142. *About NIST*, *supra* note 18.

143. *See About Commerce*, U.S. DEP'T OF COM., https://www.commerce.gov/about [https://perma.cc/8G7N-AWLE]; Albert N. Link & John T. Scott, *Evaluating Technology-Based Public Institutions: Lessons from the National Institute of Standards and Technology*, *in* POLICY EVALUATION IN INNOVATION & TECHNOLOGY 257, 259 (GEORGE PAPACONSTANTINOU & WOLFGANG POLT eds., 1997) [hereinafter Link & Scott, *Lessons*]; ALBERT N. LINK & JOHN T. SCOTT, PUBLIC ACCOUNTABILITY: EVALUATING TECHNOLOGY-BASED INSTITUTIONS 27 (1998) [hereinafter LINK & SCOTT, PUBLIC ACCOUNTABILITY]; JOHN F. SARGENT JR., CONG. RSCH. SERV., R43908, THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: AN APPROPRIATIONS OVERVIEW (2022).

144. BRYAN H. CHOI, LAWFARE, NIST'S SOFTWARE UN-STANDARDS 35 (2024).

145. *About NIST*, *supra* note 18.

146. Under the Administrative Procedure Act's rulemaking provisions, NIST does not have rulemaking authority, but it posts its frameworks to the Federal Register for notice and comment in a similar way that agencies post rules to the Federal Register. *See* 5 U.S.C. § 553.

Department of Commerce in 1905.[147] At its inception, NBS consisted of physical science laboratories and employed scientists who evaluated new technology, such as the camera and radio, and created national standards for the construction of these goods.[148] In a push to regulate the federal government's computer usage, Congress passed the Brooks Act of 1965, which required NIST to create the Federal Information Processing Standards (FIPS) Framework that included uniform federal standards for automatic data processing equipment.[149] NIST conducts research on a diverse range of areas, including data and technology. Today, NIST plays a leading role in developing best practices for data management.[150] For example, NIST conducts research on cybersecurity, privacy, and artificial intelligence (AI), and has created voluntary best practices frameworks for each of those areas.[151]

Developed over multiple administrations, NIST's cybersecurity, privacy, and AI frameworks reflect the divergent political engagement prior to and during their creation. In 2013, the Obama administration issued the Improving Critical Infrastructure Cybersecurity Executive Order requiring NIST to create the Cybersecurity Framework.[152] The Executive Order had its origins in a failed cybersecurity legislative proposal to establish minimum necessary standards for critical infrastructure.[153] The NIST Cybersecurity Framework is a voluntary baseline framework

147. *See* Link & Scott, *Lessons*, *supra* note 143, at 259; LINK & SCOTT, PUBLIC ACCOUNTABILITY, *supra* note 143, at 27.

148. *See* Link & Scott, *Lessons*, *supra* note 143, at 259–60; LINK & SCOTT, PUBLIC ACCOUNTABILITY, *supra* note 143; Harry Law, *A Short History of the National Institute for Standards and Technology (Part One)*, LINKEDIN (June 23, 2023), https://www.linkedin.com/pulse/short-history-national-institute-standards-technology-harry-law/ [https://perma.cc/G2B6-HRE9].

149. *See* CHOI, *supra* note 144, at 6. NIST stopped creating FIPS in the 1990s because they were ineffective. *See id.* at 32.

150. *See id.* at 33; SARGENT JR., *supra* note 143, at 1.

151. *See Information Technology*, NAT'L INST. OF STANDARDS & TECH. (Jan. 11, 2022), https://www.nist.gov/information-technology [https://perma.cc/4XDF-F7PK].

152. *See* Exec. Order No. 13,636, 78 Fed. Reg. 11,739 § 7(a) (Feb. 12, 2013); Lei Shen, *The NIST Cybersecurity Framework: Overview and Potential Impacts*, 10 SCITECH LAW. 16, 17 (2014).

153. *See* Michael S. Schmidt & Nicole Perlroth, *Obama Order Gives Firms Cyberthreat Information*, N.Y. TIMES (Feb. 12, 2013), https://www.nytimes.com/2013/02/13/us/executive-order-on-cybersecurity-is-issued.html (on file with the *Columbia Journal of Law & Social Problems*).

to reduce cyber risk for critical infrastructure and provides cybersecurity best practices for organizations across industries.[154]

Although the Framework is voluntary, the FTC notes that alignment with the NIST Cybersecurity Framework is a signal that a company has proper security safeguards in place.[155] The FTC can bring an enforcement action if a company violates Section 5(a) of the FTC Act by engaging in unfair or deceptive security practices.[156] Because there is no federal cybersecurity legislation, the FTC establishes data security norms through enforcement actions and subsequent consent decrees.[157] Although alignment with the NIST Cybersecurity Framework will not prevent an FTC enforcement action, the FTC advises businesses to follow the core functions of the Framework in order to avoid penalties.[158] As a result, 50% of companies adhere to NIST's Cybersecurity Framework, and it is considered a leading framework in the cybersecurity community.[159] For example, Ohio's Data Protection

---

154. *See* Exec. Order No. 13636, 78 Fed. Reg. 11,739 (Feb. 12, 2013) (President Obama signed the Executive Order in response to rising cybersecurity threats); Shen, *supra* note 152, at 17; *see also Cybersecurity Framework: History and Creation of the CSF 1.1*, NAT'L INST. OF STANDARDS & TECH., https://www.nist.gov/cyberframework/online-learning/history-and-creation-framework [https://perma.cc/6CMU-TN98] (Feb. 26, 2024). Although the Cybersecurity Framework is voluntary, the White House considered different incentives for adoption, such as limiting cybersecurity liability or leveraging federal grants, to increase implementation of the framework. *See* Michael Daniel, *Incentives to Support Adoption of the Cybersecurity Framework*, THE WHITE HOUSE BLOG (Aug. 6, 2013), https://obamawhitehouse.archives.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework [https://perma.cc/U96X-M3NS]; Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305, 340, 345 (2015).

155. *See* Andrea Arias, *The NIST Cybersecurity Framework the FTC*, FTC BUS. BLOG (Aug. 31, 2016), https://www.ftc.gov/business-guidance/blog/2016/08/nist-cybersecurity-framework-and-ftc [https://perma.cc/7FET-2RR2]; Shackelford et al., *supra* note 154, at 345; *see also* Shen, *supra* note 152, at 5–6 (arguing that without cybersecurity legislation, the Cybersecurity Framework could become the de facto legal standard).

156. *See Overview of FTC Authority*, *supra* note 42.

157. *See* Solove & Hartzog, *supra* note 44, at 620; *see also* Shackelford et al., *supra* note 154, at 342 ("The NIST Cybersecurity Framework could be utilized to argue the appropriate standard of care.").

158. *See supra* note 155; *Understanding the NIST Cybersecurity Framework*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework [https://perma.cc/UY3G-GFRJ].

159. *See* Kelley Spakowski, *NIST Cybersecurity Framework (CSF) Controls Fundamentals*, AUDITBOARD (Sept. 6, 2023), https://www.auditboard.com/blog/fundamentals-of-nist-cybersecurity-framework-controls/ [https://perma.cc/REG8-D8Q5]; Shen, *supra* note 152, at 18; Daniel, *supra* note 154 (emphasizing that companies should implement the Cybersecurity Framework); *see also* Cynthia Brumfield, *NIST Seeks Information on Updating Its Cybersecurity Framework*, CSO (Feb. 24, 2022),

Act offers a safe harbor to businesses that create, maintain, and comply with a cybersecurity program that aligns with the NIST Cybersecurity Framework.[160]

NIST continues to play a major role in cybersecurity standard-making. In 2021, President Biden issued an Executive Order on "Improving the Nation's Cybersecurity," which directed NIST to work with the Department of Homeland Security to establish "cybersecurity performance goals" for critical infrastructure owners, operators, and federal contractors.[161] Additionally, in March 2023, the White House published the U.S. National Cybersecurity Strategy, which requires federal contractors, technology companies, and critical infrastructure owners to align with the NIST Cybersecurity Framework.[162]

As in cybersecurity, NIST's role in the AI field has expanded through legislation and executive orders. The Artificial Intelligence Initiative Act of 2020 required NIST to create the Artificial Intelligence Risk Management Framework.[163] In 2023, President Biden issued an Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence which tasked NIST, in coordination with other agencies, to create guidelines for the safe development and deployment of AI systems, specifically generative AI.[164] It also created the U.S. AI Safety Institute to be housed within NIST.[165] But immediately upon

---

https://www.csoonline.com/article/572127/nist-seeks-information-on-updating-its-cybersecurity-framework.html [https://perma.cc/HJ9C-WKRD].

160. See Data Protection Act, S.B. 220, 132nd Gen. Assemb., Reg. Sess. (Ohio 2018).

161. *See* Exec. Order No. 14,028, 88 Fed. Reg. 26,663 (May 12, 2021). Critical infrastructure is considered vital when its destruction would have catastrophic impacts on national security, national public health or safety, or the economy. *See Critical Infrastructure Sectors*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors [https://perma.cc/2PXL-3T7R]. Critical infrastructure sectors include water, emergency services, energy, etc. *See id.*

162. *See* WHITE HOUSE, NATIONAL CYBERSECURITY STRATEGY (2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf [https://perma.cc/XYP6-B49P].

163. The Artificial Intelligence Initiative Act became law in 2021. *See* William M. Thornberry National Defense Authorization Act, H.R. 63495, 116th Cong. (2021); NAT'L INST. OF STANDARDS & TECH., ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK (AI RMF 1.0) (2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf [https://perma.cc/S7HD-MN27].

164. *See* Exec. Order No. 14110, 88 Fed. Reg. 75191 (Oct. 30, 2023). The Executive Order acknowledged that "irresponsible use [of AI systems] could exacerbate societal harms such as fraud, discrimination, bias, and disinformation . . . ." *Id.*

165. *See id.*

taking office President Donald Trump rescinded the order.[166] In November 2023, Senator Jerry Moran introduced the Federal Artificial Intelligence Risk Management Act, which, if passed, will direct federal agencies to use NIST's AI Framework for their AI risk management efforts.[167] The inclusion of the NIST Artificial Intelligence Risk Management Framework in a bill that would regulate government agencies suggests that NIST is playing a broader regulatory role in the AI field.

Unlike the Cybersecurity and AI frameworks, there was no catalyzing executive order or failed federal law that prompted NIST to create the Privacy Framework.[168] NIST created the Privacy Framework in 2020 to provide privacy best practices for organizations across industries.[169] Despite limited political discussion surrounding its creation many companies have adopted the NIST Privacy Framework for risk assessments.[170] Many companies' internal policies align with the NIST Privacy Framework because it provides voluntary broad guidelines that map onto state and international privacy laws.[171] Under the Tennessee Information Protection Act (TIPA), alignment with the

166. *See* Madison Alder, *Trump Rescinds Biden AI Order, Creates DOGE, Orders in-Person Work*, FEDSCOOP (Jan. 20, 2025), https://fedscoop.com/trump-rescinds-biden-ai-order-creates-doge-orders-in-person-work/ [https://perma.cc/Q8CQ-5LFG]. President Trump aims to deregulate AI in an effort to increase innovation and enhance military AI capabilities. *See* Benj Edwards, *Trump plans to dismantle Biden AI safeguards after victory,* ARS TECHNICA (Nov. 6, 2024), https://arstechnica.com/ai/2024/11/trump-victory-signals-major-shakeup-for-us-ai-regulations/ (on file with the *Columbia Journal of Law & Social Problems*).

167. *See* Federal Artificial Intelligence Risk Management Act, S. 3205, 118th Cong. (2023).

168. In 2020, the only data privacy law in the U.S. was the California Consumer Privacy Act. *See supra* note 53.

169. *See* NIST PRIVACY FRAMEWORK, *supra* note 19 at i. NIST is in the process of updating the 2020 Privacy Framework to version 1.1. *See* Privacy Framework, Version 1.1, NAT'L INST. OF STANDARDS & TECH (Oct. 16, 2024), https://www.nist.gov/privacy-framework/new-projects/privacy-framework-version-11 [https://perma.cc/Q49F-ZUYP].

170. *See* Danker, *supra* note 21; *Business Case for the NIST Privacy Framework*, *supra* note 21; *Privacy Framework Perspectives and Success Stories*, *supra* note 21. When conducting risk assessments, companies compare their existing privacy protocols or lack thereof to NIST's standards to identify potential risks, such as failing to provide a privacy notice, the ability to opt out of data collection and sharing, or the companies' failure to secure personal information. *See* Andrea Tang, *Privacy Risk Management,* ISACA (June 30, 2020), https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/privacy-risk-management [https://perma.cc/3UKU-6RG9].

171. The guidelines are designed to be compatible with domestic and international privacy laws. Companies can claim they comply with data privacy laws by aligning with the broad NIST Privacy guidelines. *See Privacy Framework: Frequently Asked Questions,* NAT'L INST. OF STANDARDS & TECH. (Jan. 14, 2021), https://www.nist.gov/privacy-framework/frequently-asked-questions [https://perma.cc/A7YA-D5ZM].

NIST Privacy Framework is an affirmative defense to a privacy complaint.[172] In other words, while TIPA gives consumers the right to access, correct, delete, and obtain a copy of their personal information, as well as opt out of targeted advertising, selling, or profiling, a company can show how its privacy program aligns with the NIST Privacy Framework to avoid liability for violating an individual's data privacy rights.[173] But NIST did not create the Privacy Framework in response to federal action, and it was unaware of the Privacy Framework's future use as a legal standard. The result was an inadequate, undemocratic process to create the Privacy Framework that ended up dominated by industry voices.

B. THE FOX IN THE HENHOUSE: THE ORIGINS OF THE NIST PRIVACY FRAMEWORK

NIST claimed it worked closely with industry, government, and academia to create the NIST Privacy Framework.[174] The guidelines suggest companies create external privacy notices and internal privacy procedures, hire privacy personnel, document personal information collected, and identify risky data processes.[175] The Framework, however, does not acknowledge consumers or provide redress for the substantive harms and equity considerations that stem from a lack of data privacy protections.[176] Instead the Framework is primarily responsive to comments from industry voices, a feature that Professors Cary Coglianese, Richard Zeckhauser, and Edward Parson warn can lead to "biased regulatory decision making."[177]

---

172. *See* Tennessee Information Protection Act, H.B. 1181, 113th Gen. Assemb., Reg. Sess. (Tenn. 2023); *see also* Pittman et al., *supra* note 22.

173. *See* Tennessee Information Protection Act, H.B. 1181, 113th Gen. Assemb., Reg. Sess. (Tenn. 2023); Alan Friel & Julia Jacobson, *Final Tennessee Privacy Act Signed into Law, Expanding Consumer Rights and Data Controller Flexibility in Developing and Measuring a Written Privacy Program that May Qualify for an Affirmative Defense to Violations of the Act*, PRIV. WORLD (May 4, 2023), https://www.privacyworld.blog/2023/05/final-tennessee-privacy-act-signed-into-law/#page=1 [https://perma.cc/6NQX-9FW8].

174. *See* Kevin Stine, *Stakeholders: The "Be-All and End-All" of NIST's Cybersecurity and Privacy Framework*, NAT'L INST. OF STANDARDS & TECH. BLOG (Mar. 24, 2021), https://www.nist.gov/blogs/cybersecurity-insights/stakeholders-be-all-and-end-all-nists-cybersecurity-and-privacy-work [https://perma.cc/8SP3-97M4].

175. *See id*.

176. *See* NIST PRIVACY FRAMEWORK, *supra* note 19; *see infra* Part III.b.

177. Cary Coglianese et al., *Seeking Truth for Power: Informational Strategy and Regulatory Policymaking*, 89 MINN. L. REV. 277, 288 (2004).

Before publishing the Privacy Framework, in 2018, NIST posted a request for information for the NIST Privacy Framework on the Federal Register and received 82 comments.[178] In response, NIST created a summary analysis document in which it identified key themes from these comments that helped to develop the Privacy Framework.[179] The majority of the comments that NIST received and responded to were from companies such as Workday, Salesforce, Microsoft, Google, IBM, and Apple.[180] The overarching feedback within the summary analysis document included organizations' desire for national and international regulatory compatibility, transparency and accountability in regards to privacy policies and practices to improve consumer trust, alignment with the NIST Cybersecurity Framework, and guidelines for data minimization and anonymization.[181]

Of the 82 comments, only four addressed the substantive and systemic impacts of unregulated data processing and the lack of real data privacy protections.[182] One comment from Public Knowledge, a public interest advocacy organization, discussed big tech's role in the surveillance economy and the financial incentives to "obfuscate privacy-invasive practices."[183] Public Knowledge requested that the NIST Privacy Framework "describe the impacts of privacy violations as harms."[184] This comment highlighted impacts on dignitary legal interests that can result from a lack of data privacy protections:

---

178. *See Request for Information for the NIST Privacy Framework*, NAT'L INST. OF STANDARDS & TECH, https://www.nist.gov/privacy-framework/rfi [https://perma.cc/ZC7G-YSMD] (Jan. 16, 2020); Developing a Privacy Framework, 83 Fed. Reg. 56824 (Nov. 14, 2018).

179. *See* NAT'L INST. OF STANDARDS & TECH., *supra* note 178.

180. *See generally* NAT'L INST. OF STANDARDS AND TECH., SUMMARY ANALYSIS OF THE RESPONSES TO THE NIST PRIVACY FRAMEWORK REQUEST FOR INFORMATION (Feb. 27, 2019), https://www.nist.gov/system/files/documents/2019/02/27/rfi_response_analysis_privacyframework_2.27.19.pdf. [https://perma.cc/3KDN-TC3W] [hereinafter NIST, SUMMARY ANALYSIS].

181. *See generally id.*

182. *See Request for Information for the NIST Privacy Framework*, *supra* note 178.

183. Dylan Gilbert, Public Knowledge, Comment Letter on Proposed National Institute of Standards and Technology Privacy Framework 1 (Jan. 14, 2019), https://www.nist.gov/system/files/documents/2019/02/05/public_knowledge_dylan_gilbert.pdf [https://perma.cc/42YG-87BM]. "Public Knowledge promotes freedom of expression, an open internet, and access to affordable communications tools and creative works . . . to shape policy on behalf of the public interest." PUB. KNOWLEDGE, https://publicknowledge.org [https://perma.cc/39PL-JAH4].

184. Gilbert, *supra* note 183, at 2.

> For example, a data breach may expose information that could be embarrassing or cause reputational harm, undermining one's employment or social prospects. . . . Harms may also come in the form of Cambridge Analytica-style "psychographics," misinformation, or distortions of the public record that undermine public trust in U.S. democratic institutions and put our national security at risk. Irresponsible data use can exacerbate informational disparities, enable unfair price discrimination, limit awareness of opportunities, and contribute to employment, housing, health care, and other forms of discrimination.[185]

An additional comment, from a coalition of public interest organizations including the Center for Democracy & Technology, Human Rights Watch, and Lawyers' Committee for Civil Rights Under Law, stated that:

> Legislation must further prevent processing of data to discriminate unfairly against marginalized populations (including women, people of color, the formerly incarcerated, immigrants, religious minorities, the LGBTQIA/+ communities, the elderly, people with disabilities, low-income individuals, and young people) or to target marginalized populations for such activities as manipulative or predatory marketing practices.[186]

In addition to substantive safeguards, the comment also called for the regulation of automated decision-making to ensure such technology follows anti-discrimination laws and promotes fairness.[187]

Although 34 public interest organizations signed onto the comment, NIST's summary response did not acknowledge the need for substantive safeguards against unfair data processing.[188] The

---

185. *Id.* at 3.

186. Public Interest Organizations, Comment Letter on Proposed National Institute of Standards and Technology Privacy Framework, 2 (Jan. 14, 2019), https://www.nist.gov/system/files/documents/2019/02/14/publicinterest_collectivegroups.pdf [https://perma.cc/C4FP-Y2QV] [hereinafter Public Interest Organization Coalition Comment Letter]

187. *See id.*

188. NIST did not provide individual responses for each comment. The organization did provide a summary analysis that identified major themes to assist in the development of the NIST privacy framework and specific RFI response examples to support the themes. NIST did not cite the Public Collective Group's comment. NIST did cite to the Public

summary analysis report likewise did not address themes such as discrimination in the housing, employment, health, education, and lending contexts; equal opportunity; equity; the protection of civil rights; or monitoring algorithms that perpetuate bias.[189] NIST also did not acknowledge the serious harms raised in the Public Knowledge comment that can result from a lack of data privacy protections.[190] The Privacy Framework's summary analysis document did not include a section on the substantive unfair impacts that stem from a lack of data privacy protection, such as equity considerations, discrimination or bias, or the inability for individual consumers to effectively control the use of their personal data. NIST referenced only one comment that mentioned bias at all.[191]

NIST's failure to address public interest concerns in the Privacy Framework is particularly concerning because NIST sees itself as an influential source for data protection regulations. In a 2020 interview, Walter Copan, the director of NIST from 2017 to 2021, said, "We believe that the Privacy Framework . . . has the potential . . . to shape the approach to consumer privacy in the United States and internationally."[192] Copan went on to emphasize that NIST is

---

Knowledge comment, but NIST did not include Public Knowledge's recommendations to address substantive harms and financial incentives. *See generally* NIST, SUMMARY ANALYSIS, *supra* note 180. During a panel with members of NIST, the former Executive Vice President of the Center for Democracy & Technology (CDT) stated that CDT worked closely with NIST on the Privacy Framework. *See* Chris Calabrese, Executive Vice President, Priv. Ctr. for Democracy & Tech., Panel Discussion at Center for Strategic and International Studies Event: A Conversation on the NIST Privacy Framework 12 (Feb. 19, 2020), https://www.csis.org/analysis/conversation-nist-privacy-framework [https://perma.cc/KNS7-AE22].

189. *See generally* NIST, SUMMARY ANALYSIS, *supra* note 180.

190. *See id.* In its summary, NIST included only one comment, by Amie Stepanovich on behalf of digital human rights nonprofit Access Now, that suggested individual privacy risks be construed expansively and include potential harms such as emotional, psychological, physiological, and human rights violations, in addition to financial harm. *See id.* at 8. NIST did not include these suggestions in the Privacy Framework. *See* NIST PRIVACY FRAMEWORK, *supra* note 19.

191. *See id.* at 22 (under the "Emerging Technologies" theme, NIST included a comment that requested NIST provide guidelines directed towards "root[ing] out any inherent or sample-bias that has been embedded in the algorithm). Katie McInnis posted this comment on behalf of Consumer Reports, an independent nonprofit that informs consumers about the value, quality, or authenticity of goods and services and incentivizes corporations to act responsibly. This comment is one of the few that can be categorized as in the public interest, as compared to comments from corporations.

192. Walter Copan, Director, Nat'l Inst. of Standards & Tech., Keynote Address at Center for Strategic and International Studies Event: A Conversation on the NIST Privacy Framework 3 (Feb. 19, 2020), https://www.csis.org/analysis/conversation-nist-privacy-framework [https://perma.cc/KNS7-AE22].

trustworthy because it is not a lawmaking institute but rather an entity "rooted in research and measurement science and standards."[193] During the same panel, Naomie Lefkowitz, a senior privacy analyst at NIST who had previously worked at the FTC, said that the United States has an "opportunity now to chart a course on privacy that can impact people and societies around the world for many years to come."[194] Although NIST failed to predict that the Privacy Framework would be the only federal legal standard, it wanted to influence the privacy landscape through its Privacy Framework. While NIST's intentions were laudable, the positive influence of the Privacy Framework is limited due to NIST's failure to engage with public interest concerns and social harms.

The NIST Privacy Framework provides procedural guidelines for companies to create privacy policies to notify and receive consumer consent, create internal privacy procedures to manage the personal information collected, hire privacy personnel, and identify potential data processing risks.[195] Despite the potential harm to consumers from uninhibited personal data collection and dissemination, the Framework does not prohibit specific types of data processing or advise companies on how to prevent consumer harms.[196] The Framework also fails to address power disparities between companies and consumers, surveillance capitalism, and bad acts driven by the financial incentives of personal data collection and use.[197]

The "risk-assessment" category of the NIST Privacy Framework could address discriminatory or manipulative data processing, automated decision-making, or profiling. Instead, it focuses on how risks to consumers can implicate companies, "including mission, functions, other risk management priorities (e.g., compliance, financial), reputation, workforce, and culture."[198] Within the risk assessment category, one subcategory suggests that "data analytic inputs and outputs [should be] identified and

193. *Id.*

194. Naomi Lefkovitz, Senior Privacy Policy Advisor, Nat'l Inst. of Standards & Tech., Panel Discussion at Center for Strategic and International Studies Event: A Conversation on the NIST Privacy Framework 12 (Feb. 19, 2020), https://www.csis.org/analysis/conversation-nist-privacy-framework [https://perma.cc/KNS7-AE22].

195. *See generally* NIST PRIVACY FRAMEWORK, *supra* note 19.

196. *See id.*

197. *See id.*

198. *Id.* at tbl.2.

evaluated for bias"; however, there is no guidance for what companies should do if a data analytic output is biased, or why biased outcomes in data analysis have broader societal harms.[199] The word "harm" is not included in the substantive guidelines of the Privacy Framework.[200]

Because NIST's engagement with public interest groups while creating the guidelines was limited, it is troublesome that Tennessee explicitly included it in the Tennessee Information Protection Act (TIPA).[201] Under the TIPA, companies are required to create a privacy program that aligns with the NIST Privacy Framework.[202] TIPA also establishes an affirmative defense to a cause of action for a violation of the law if the company aligns its privacy program with the NIST Privacy Framework, thus allowing companies to evade liability.[203] This results in industry functionally regulating itself,[204] with a worryingly self-interested and light hand.[205] Tennessee is also at fault for including an industry-friendly Privacy Framework in its state data privacy law, but NIST's trustworthy reputation likely led to the uptake of the Privacy Framework without further consideration by the Tennessee legislature.[206]

It is unclear why NIST disregarded consumer advocates and public interest organizations' input in the Privacy Framework. One explanation for the industry-friendly guidelines may be that NIST's mission to promote industrial competitiveness resulted in it prioritizing industry input during the creation process over input from consumer advocates and public interest organizations. A more likely explanation is that the lack of congressional or

199. *See id.* Data analytics is the process of analyzing input data to identify trends and correlations in the output. *See Data Analytics: What It Is, How It's Used, and 4 Basic Techniques*, INVESTOPEDIA (Apr. 22, 2024), https://www.investopedia.com/terms/d/data-analytics.asp [https://perma.cc/D4TT-2KH4]; Waldman, *Automated Decision-Making*, *supra* note 75, at 618 (explaining why biased outcomes have broader societal harms).

200. NIST includes a brief introduction before the privacy framework that recognizes data processing problems can include embarrassment, stigmas, discrimination, economic loss, or physical harm. The Framework guidelines, however, do not acknowledge potential harms. *See* NIST PRIVACY FRAMEWORK, *supra* note 19, at 3.

201. *See* Tennessee Information Protection Act, H.B. 1181, 113th Gen. Assemb., Reg. Sess. (Tenn. 2023); CHOI, *supra* note 144, at 35.

202. *See* Tennessee Information Protection Act, H.B. 1181, 113th Gen. Assemb., Reg. Sess. (Tenn. 2023).

203. *See id.*

204. *See supra* notes 96–101 and accompanying text.

205. *See* FITZGERALD ET AL., THE STATE OF PRIVACY, *supra* note 60, at 6.

206. *See* CHOI, *supra* note 144, at 3.

executive instruction for the Privacy Framework led to limited engagement from public interest organizations and enabled powerful industry voices to dominate the creation process.[207] NIST did not expect, nor received instructions, that the Privacy Framework would be used as the national regulatory guidelines;[208] therefore, NIST facilitated only limited discussion surrounding broader notions of data privacy during the creation process. There is no evidence to suggest NIST ignored comments in bad faith, but the combination of these different factors resulted in one-sided guidelines. Still, NIST prides itself on considering the views of all stakeholders[209] and, based on its past performance of incorporating public interest concerns in the AI Framework,[210] it is capable of engaging in a process that acknowledges that legitimate data privacy necessitates the protection of consumers. NIST has the potential, and authority, to contribute productively to the data privacy regulatory ecosystem.

C. THE POTENTIAL PRODUCTIVE ROLE OF THE NIST PRIVACY FRAMEWORK IN THE U.S. PRIVACY LANDSCAPE

Because NIST is widely regarded as a neutral and trustworthy institution,[211] it can work closely with consumer advocates and public interest organizations to create privacy guidelines that consider both industry wants and individual data privacy rights. NIST loses democratic accountability when it exclusively engages with business interests to create guidelines.[212] Guidelines created with input from only one set of corporate stakeholders are biased towards those stakeholders, ignore privacy expertise, and fail to adequately reflect the views of those most affected.[213] Without considering both sides, the NIST Privacy Framework will continue to fail to adequately protect the more vulnerable stakeholder: consumers. Despite previously disregarding public interest organizations' concerns while creating the Privacy Framework, NIST can make a conscious effort to work closely with consumer

207. *See supra* Part III.a.
208. *See supra* note 192.
209. *See* Stine, *supra* note 174.
210. *See infra* Part III.c.
211. *See* CHOI, *supra* note 144, at 3.
212. *See* Waldman, *Privacy, Practice, and Performance*, *supra* note 64, at 1273–74.
213. *See id.* at 1277.

advocates and academia while still incorporating the tech industry's feedback through the notice and comment process.[214]

Government agencies need information from industry to create effective regulations because "the best source of information about . . . the behavior of individuals and firms, the costs of remediation or mitigation . . . will be the very firms that the government agency regulates."[215] Regulators can also incentivize companies to share information about business practices that will benefit the regulator.[216] However, close relationships between industry and regulators can lead to regulatory bias or corruption.[217] This is especially prevalent in the context of regulating data privacy due to the power and influence of big tech companies.

NIST, however, can create a Privacy Framework that considers potential harms to individuals by looking to its AI Risk Management Framework as a blueprint. The AI Risk Management Framework, promulgated in 2023, exemplifies a more consumer-protective approach.[218] There, NIST identified characteristics of trustworthy AI—namely, that AI should be valid, reliable, safe, secure and privacy-enhanced, fair, and manage harmful bias.[219] NIST went so far as to publish a comprehensive framework and supplementary guidelines on safe and trustworthy AI.[220] Unlike the NIST Privacy Framework, the NIST AI Framework and playbook provide in-depth explanations of how AI can perpetuate bias and discrimination, how to identify risks posed by AI, and how to remedy those risks and potential harms.[221] The

214. *See* Stine, *supra* note 174.

215. Cary Coglianese et al., *Seeking Truth for Power: Informational Strategy and Regulatory Policymaking*, 89 MINN. L. REV. 277, 278 (2004).

216. *See id.* at 302. Companies are the best source for information about the "risk of products, the behavior of individuals and firms, and the costs of remediation or mitigation, or the feasibility of different technologies." *Id.* at 278.

217. *See id.* at 337.

218. The Summary Analysis Response Document for the AI Risk Management Framework included equity concerns in the development of AI systems. *See* NAT'L INST. OF STANDARDS AND TECH., SUMMARY ANALYSIS OF RESPONSES TO THE NIST ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK (AI RMF) - REQUEST FOR INFORMATION (RFI) (Oct. 15, 2021), https://www.nist.gov/system/files/documents/2021/10/15/AI%20RMF_RFI%20Summary%20Report.pdf [https://perma.cc/4MW7-B46N] [hereinafter NIST, AI RMF SUMMARY ANALYSIS].

219. *See Trustworthy and Responsible AI*, NAT'L INST. OF STANDARDS & TECH., https://www.nist.gov/trustworthy-and-responsible-ai [https://perma.cc/C4BD-ACLN].

220. *See AI Risk Management Framework*, NAT'L INST. OF STANDARDS & TECH., https://www.nist.gov/itl/ai-risk-management-framework/ai-rmf-development [https://perma.cc/2AY5-SE6D] (Jan. 2, 2024).

221. *See* REVA SCHWARTZ ET AL., NAT'L INST. OF STANDARDS & TECH., Special Publication 1270, TOWARDS A STANDARD FOR IDENTIFYING AND MANAGING BIAS IN ARTIFICIAL

AI Framework explicitly addresses fairness in AI systems and how bias and discrimination contribute to inequality and inequity in response to "specific concerns and suggestions about managing AI risks related to civil rights, civil liberties, and equity."[222] NIST demonstrated its commitment to addressing the structural and systemic harms posed by AI—such as the perpetuation of institutional racism and sexism or biased outputs due to an unrepresentative dataset—that negatively impact marginalized communities.[223] The same types of harms exist in the collection and use of personal data more broadly, and NIST is capable of creating a Privacy Framework that addresses these issues.

Despite doubt surrounding its effectiveness,[224] corporations and states are turning to the NIST Privacy Framework for regulatory guidance in the absence of a federal data privacy law. NIST is a reliable institution with privacy expertise that is well positioned to contribute to the data privacy ecosystem.[225] NIST is already playing a quasi-regulatory role in the cybersecurity and AI fields. If the NIST Privacy Framework is going to be used as a legal standard in state data privacy laws, NIST should engage in a more robust process with key stakeholders and consider critiques of current data privacy laws. In so doing, it will ensure that the Framework does not merely codify industry best practices and instead adequately protects consumer interests.

IV. REFORMULATING THE NIST PRIVACY FRAMEWORK

Although current conversations surrounding the shortfalls of data privacy legislation in the United States do not acknowledge NIST's potential role in the data privacy landscape, NIST can contribute even more productively to this legal ecosystem.

INTELLIGENCE 1 (March 2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf [https://perma.cc/Z8GN-J3KU].

222. *See* NIST, AI RMF SUMMARY ANALYSIS, *supra* note 218; *id.* at iii (NIST published an accompanying document to assist companies in identifying and addressing biased AI systems).

223. *See id.* at 9, 26.

224. *See* Cameron F. Kerry, *NIST's AI Risk Management Framework Plants a Flag in the AI Debate*, BROOKINGS INST. (Feb. 15, 2023) https://www.brookings.edu/articles/nists-ai-risk-management-framework-plants-a-flag-in-the-ai-debate/ [https://perma.cc/9QVQ-MVZ6] (stating that, because of the impact of the GDPR and the California Consumer Privacy Act, the Privacy Framework "has limited space . . . to affect privacy and data protection standards, practices, and processes").

225. *See* CHOI, *supra* note 144, at 31.

Corporations already draw on the NIST Privacy Framework as a guidepost for their data privacy programs.[226] Likewise, Tennessee has functionally codified the Framework into a legal standard.[227] Absent a federal data protection agency or data privacy law, NIST is filling this gap and providing regulatory guidelines for privacy compliance. But given NIST's expanded regulatory role, the process by which NIST created the Privacy Framework needs to be reconsidered. NIST should engage with the views of all relevant stakeholders, the critiques of current data privacy legislation, and the scholarly recommendations below to create a Privacy Framework that diminishes the need for federal action.

A. A PROCESS TO REFORMULATE THE NIST PRIVACY FRAMEWORK

The process by which NIST reformulates the Privacy Framework should more heavily involve public interest organizations and consumer advocates to ensure the tech industry is not superficially regulating itself through the Privacy Framework. A comprehensive discussion with a range of stakeholders would spotlight the existing information asymmetries and power imbalances between corporations and consumers, which currently make it impossible for consumers to control their personal information effectively.[228] By acknowledging the existence of information asymmetries in the Privacy Framework, NIST could address the structural problems of self-regulating data privacy and focus on data privacy as a collective issue.[229] NIST should consider the critiques laid out in Part II, as well as the benefits of a substantive and procedural privacy framework. Focusing only on procedural requirements fails to acknowledge bad acts, like dark patterns used to manipulate consumers into oversharing their personal information or discriminatory algorithms.[230] Without explicitly advising against certain types of data processing, companies will

226. *See* Danker, *supra* note 21; *Business Case for the NIST Privacy Framework, supra* note 21; *Privacy Framework Perspectives and Success Stories, supra* note 21.

227. *See* H.B. 1181, 113th Gen. Assemb., Reg. Sess. (Tenn. 2023).

228. *See* Hartzog, *supra* note 114, at 427.

229. *See* Richards & Hartzog, *Pathologies*, *supra* note 124, at 1498; *supra* Part II.

230. *See* Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C.L. REV. 1687, 1737 (2020).

continue to use personal information in financially beneficial ways regardless of societal harms.[231]

NIST should participate fully in the notice and comment process by responding to and incorporating public interest organizations' comments, specifically those highlighting how uninhibited data collection and dissemination can contribute to inequality.[232] These comments call for safeguards against data processing that discriminates against marginalized people.[233] In response to this feedback, the "risk-assessment" category of the NIST Privacy Framework could advise against discriminatory algorithmic decision-making, profiling, targeted advertising, and problematic data processing that negatively impacts vulnerable communities.[234] Furthermore, NIST could promote cyber civil rights and advise against data aggregation or processing that discriminates in "housing, employment, credit, insurance, and public accommodations."[235] In addition to prohibiting discriminatory data processing, NIST could consider proscribing the spread of misinformation to influence political votes and the use of dark patterns on websites to manipulate consumers.[236]

B. DIFFERENT CONCEPTUALIZATIONS OF DATA PRIVACY

NIST should also engage with data privacy scholarship that proposes alternatives to the notice and consent model that has plagued data privacy laws and failed to protect individuals' privacy rights.[237] If NIST is going to be a national norm-setter for data privacy, it needs to at least consider, if not adopt, different formulations of data privacy.[238] Different conceptualizations of data privacy include privacy as trust, privacy as loyalty, and

231. *See* Trautman, *supra* note 70, at 50; ZUBOFF, *supra* note 68, at 81.

232. *See* Public Interest Organization Coalition Comment Letter, *supra* note 186.

233. *See id.*

234. *See* SCHWARTZ ET AL., *supra* note 221; *see also* Allen, *Black Opticon*, *supra* note 28, at 931–32.

235. Waldman, *Automated Decision-Making*, *supra* note 75, at 1277 (discussing a recommended bill that emphasizes cyber civil rights); *see also* Allen, *Black Opticon*, *supra* note 28, at 953.

236. *See* Trautman, *supra* note 70; *Deceptive Patterns—User Interfaces Designed to Trick You*, DECEPTIVE DESIGNS (Apr. 25, 2023), https://www.deceptive.design/ [https://perma.cc/NZ44-DJV9].

237. *See supra* Part II.

238. Professor Allen argues that current guidance surrounding data privacy reforms fail to address "the pervasive problems of African Americans in the digital economy—even when it purports to promote equity." *See* Allen, *Black Opticon*, *supra* note 28, at 931.

privacy as a fiduciary duty.[239] Although these conceptions of data privacy are specific to privacy law, they each try to address and remediate the power imbalances between individuals and consumers to create more effective and equitable regulations. NIST can consider these features when redeveloping the NIST Privacy Framework to determine if they help address consumers' vulnerability.

Professor Waldman argues that privacy in the digital world should be based on trust between consumers and corporations.[240] If an individual discloses personal information to a company, and there is an expectation of trust, privacy regulations should prevent disclosures to third parties outside of this relationship of trust.[241] When a corporation manipulates and nudges individuals into sharing their personal information and "aggregat[es], catergoriz[es], and subsequent[ly] disclose[s]" this information to third parties, the "subsequent actions taken with our data violate the expectations we had of the behavior of third parties in whom we entrusted our data."[242] Thus, companies are bound by the trust consumers place in them when personal information is shared and cannot disseminate information outside of this relationship of trust.[243]

Professors Hartzog and Richards agree with this formulation of privacy as trust. They argue that lawmakers should create frameworks that "preserv[e] trustworthy relationships" or rules that are "justified by the vulnerability of users to the platform with which they interact."[244] The trustworthy relationship would require companies to act with discretion, honesty, protection, and loyalty.[245] Honesty would also promote transparency.[246] Requiring corporations to be truthful and forthcoming could better prevent manipulation and dark patterns on websites, the secret sharing of personal intimate information, and the unknown tracking and surveillance that takes place on the web. Thus,

---

239. *See generally* Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69 U. MIAMI L. REV. 559 (2015); Richards & Hartzog, *Duty of Loyalty*, *supra* note 123; Balkin, *supra* note 2, at 11.

240. *See* Waldman, *Privacy as Trust*, *supra* note 239, at 564.

241. *See id*.

242. *Id.* at 598; *see also* Allen, *supra* note 115, at 76.

243. *See* Hartzog & Richards, *supra* note 230, at 1745.

244. *Id.* at 1746.

245. *See id.*; *see also* Allen, *supra* note 115, at 76.

246. *See* Allen, *supra* note 115, at 78.

honesty could be a safeguard against the exploitation of consumers.[247]

Hartzog and Richards also argue that loyalty would be an effective safeguard against the opportunism that drives companies to exploit consumers.[248] Under the duty of loyalty, companies must act in the best interest of the vulnerable party (consumers) within the context of the consumer-business relationship.[249] For example, manipulating consumers to share more information than necessary through deceptive designs online is not in the best interest of the consumer. Loyalty could therefore prevent companies from engaging in self-dealing behavior, such as dark patterns, which takes advantage of vulnerable consumers.[250] The duty of loyalty could be the basis for lawmakers to "create rules and frameworks targeted at specific kinds of activities that are in practice, disloyal."[251] Companies that collect personal information would be bound by the loyalty involved in a trusting relationship, and "would be obligated to act in the best interests of the people exposing their data and engaging in online experiences. . . ."[252] A duty of loyalty would create an obligation between the corporation and consumer such that the corporation would need to limit data collection, use, and dissemination harmful to consumers.[253] Breaching the duty of loyalty would create a per se legal injury that would be sufficient to establish standing.[254]

In addition to privacy as trust and privacy as loyalty, Professor Jack M. Balkin also suggests that digital companies should be considered as information fiduciaries.[255] Although companies present themselves as trustworthy, there is an asymmetry of

247. *See id.* at 1749 (citing Paul Ohm, *Forthright Code*, 56 HOUS. L. REV. 471, 472 (2018)).

248. *See* Richards & Hartzog, *Duty of Loyalty*, *supra* note 123, at 987.

249. *See id.* at 968.

250. *See id.* at 969, 974–75. Self-dealing is when a fiduciary acts in their own interests rather than their clients. *See* Will Kenton, *Self-Dealing: What it Means, Why It's Illegal, Examples*, INVESTOPEDIA (July 27, 2022). Professors Richards and Hartzog argue that under a duty of loyalty usually assigned to fiduciaries, companies would be prevented from engaging in self-dealing behavior and manipulation. *See* Richards & Hartzog, *Duty of Loyalty*, *supra* note 123, at 964. Deceiving consumers via dark patterns on websites is self-dealing behavior because it benefits the company while manipulating and going against the interests of consumers. *See id.* at 967.

251. Hartzog & Richards, *supra* note 230, at 1750.

252. Richards & Hartzog, *Duty of Loyalty*, *supra* note 123, at 961.

253. *See id.* at 997; *see also* Allen, *Black Opticon*, *supra* note 28, at 910.

254. *See id.* at 1012.

255. *See* Balkin, *supra* note 2, at 11.

information, knowledge, and control such that there should be a fiduciary relationship between companies and consumers.[256] Information asymmetry exists because companies know about consumers through the collection of their personal information, but consumers do not know about companies, such as why they are collecting their personal information or who they are sharing that information with.[257] Companies are not transparent and can manipulate consumers into disclosing personal information. However, interacting with these digital companies is inevitable because they provide services that are near-impossible to live without,[258] all while exposing consumers to data collection and surveillance.

Balkin argues that due to the power imbalance between companies and consumers, the asymmetry of information, the inability of consumers to monitor companies, and the subsequent vulnerability of consumers in the digital age, corporations should have a fiduciary obligation to consumers.[259] Similar to the duties of loyalty and trust, the fiduciary relationship would prevent companies from "manipulating end users or betraying their trust."[260] Companies would be required to act in the interest of consumers rather than follow the financial incentives of surveillance capitalism.

Imposing a duty of loyalty and creating an information fiduciary relationship between platforms and users is seen in practice as well as in scholarship. The Consumer Financial Protection Bureau (CFPB), which is authorized to prohibit abusive acts or practices that exploit consumers' vulnerabilities, imposes a similar duty of loyalty between consumers and companies in the context of financial products or services.[261] The Data Care Act of 2023, introduced in the 2023–2024 legislative session, would require internet service providers (ISP) to act as fiduciaries for

256. *See id.*

257. *See id.*; Nissenbaum, *supra* note 113, at 34.

258. *See* Balkin, *supra* note 2, at 13 ("It is increasingly difficult to avoid dealing with digital companies that collect and use our data. Cell phone companies, broadband providers, social media companies, search engines, platform businesses like Uber, Airbnb, and Instacart, health and fitness applications like Fitbit, games like Pokémon GO and Fortnite, video-meeting applications like Zoom, streaming services like Hulu, Disney+, and Netflix—each of these companies collects data about us and our experiences as they provide us with different kinds of services.").

259. *See id.* at 13–14.

260. *Id.* at 14.

261. *See* Richards & Hartzog, *Duty of Loyalty*, *supra* note 123, at 1011.

their users.[262] The law would impose a duty of loyalty that prevents ISPs from using personal data in a way that benefits the ISP but is detrimental to the individual.[263]

In contrast, former FTC chair Lina Khan and Professor David Pozen have critiqued treating online platforms as information fiduciaries because, under Delaware law, for-profit corporations must always prioritize the interests of company shareholders.[264] The interests of shareholders and users will likely conflict because, for example, data manipulation and surveillance capitalism is profit maximizing and good for business but bad for users.[265] These interests could align if consumers are unwilling to use the online services due to bad data practices, because less consumer activity means less profit for the corporation and shareholders.[266] To address the harms posed by data use, Khan and Pozen suggest a greater push for antitrust enforcement that can combat the power of big tech.[267] Limiting the dominance of big tech companies could facilitate competition for privacy protection and reduce the possibility of major harm by one tech giant.[268] While Balkin agrees that antitrust enforcement is important, he posits that focusing only on antitrust and competition policy may not solve the current threats of digital privacy.[269] Richards and Hartzog also note that "fiduciary law has adapted to regularly resolve conflicting loyalties" because shareholders can have diverging interests, and obligations to vulnerable users should be prioritized.[270]

NIST should engage with the ideas from this data privacy scholarship to ensure it is considering power imbalances and manipulation, asymmetry of information, and vulnerability of consumers in addition to the interests of industry while creating the Privacy Framework. Seeing the relationship between consumers and corporations as fiduciary or through a duty of trust or loyalty can assist NIST in creating a Privacy Framework that goes beyond mere procedural notice and consent requirements. Moreover, the above scholarship counterbalances strong industry

262. *See* Data Care Act of 2023, S.744, 118th Cong. (2023).
263. *See id.*
264. *See* Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 504 (2019).
265. *See id.* at 505–06.
266. *See id.* at 508.
267. *See id.* at 528.
268. *See id.*
269. *See* Balkin, *supra* note 2, at 11.
270. Richards & Hartzog, *Duty of Loyalty*, *supra* note 123, at 1011.

interests. NIST should consider these formulations as viable alternatives to the illusory control given to consumers through the notice and consent framework.[271]

While some big tech companies may push back against these formulations of data privacy as being too consumer protective, others have called for federal regulation, effectively acknowledging that their own practices will need to change.[272] Public opinion is in line with a more consumer-centric data privacy regulatory regime, so transparent use of consumers' data may foster trust and benefit companies economically in the long run.[273] For example, Apple markets itself as pro-privacy; users can monitor the collection and use of their personal information on Apple products.[274] Supporting a framework tech companies can contribute to could also allow businesses to avoid more restrictive regulation. Even if big tech opposes more consumer-protective formulations of data privacy, a more open process in redeveloping the Privacy Framework would give each side an opportunity for advocacy and debate.

To revise the Privacy Framework, NIST should facilitate a process that considers the downfalls of the current notice and consent-based data privacy regime, the inherent power and wealth imbalances between companies and consumers, social harms, and potential alternative conceptualizations of how to regulate data privacy. By doing so, NIST could create a more democratically accountable Privacy Framework that can be used as a legal standard and alleviate the need for federal action.

---

271. *See* Hartzog, *supra* note 114, at 428.

272. *See* Kif Leswing, *Apple CEO Tim Cook Pushes for Privacy Legislation 'As Soon As Possible' After Visit to Congress*, CNBC (June 10, 2022), https://www.cnbc.com/2022/06/10/apple-ceo-cook-pushes-for-privacy-legislation-after-visit-to-congress.html [https://perma.cc/AU2U-9LFG]; Jeff Horwitz & Deepa Seetharaman, *Facebook's Zuckerberg Backs Privacy Legislation*, WALL ST. J. (June 26, 2019), https://www.wsj.com/articles/facebooks-zuckerberg-backs-privacy-legislation-11561589798 (on file with the *Columbia Journal of Law & Social Problems*); *see also* Hartzog & Richards, *supra* note 230, at 1737. *But see* Tyler Cowen, *Attack Monopoly Power with Deregulation, Not Antitrust Law*, BLOOMBERG (May 18, 2023), https://www.bloomberg.com/opinion/articles/2023-05-18/attack-monopoly-power-with-deregulation-not-antitrust-law (on file with the *Columbia Journal of Law & Social Problems*) (arguing that because larger tech companies are better equipped to deal with regulatory burdens, more regulation can raise the cost of entry for new smaller competitors and entrench market dominance for a few tech companies).

273. *See* McClain et al., *supra* note 107; Khan & Pozen, *supra* note 264, at 508.

274. *See Privacy. That's Apple.*, APPLE, https://www.apple.com/privacy [https://perma.cc/JXZ6-EHDZ].

C. ALTERNATIVES TO NIST

NIST is not the only potential solution to the fragmented data privacy landscape in the United States. Because NIST sits within a regulatory agency but does not have rulemaking or enforcement authority,[275] a data protection agency or federal data privacy law would both enforce privacy protections beyond NIST's capabilities.[276] At the time of its development, NIST hoped the Privacy Framework would provide guidance for a federal data privacy law that would be the muscle to stop big tech companies from engaging in bad acts.[277] However, voluntary compliance fails to generate effective results and the broad guidelines "cannot be used to determine an objective standard of care, because they do not dictate any particular set of conduct."[278]

But five years after NIST released the Privacy Framework, there is no federal data privacy law nor data protection agency. Companies depend on the Framework as a regulatory standard;[279] Tennessee even incorporated the Framework into its state law.[280] NIST is filling a gap at the federal level—and could contribute positively to the data privacy regulatory ecosystem if it were to engage with all relevant stakeholders—but there is room for alternatives.

Existing administrative agencies with enforcement authority, such as the Consumer Financial Protection Bureau (CFPB), could undertake data privacy rulemaking. NIST is currently housed within the Department of Commerce, which promotes national economic success.[281] A framework that limits companies in their

---

275. *See supra* Part III.a.

276. *See* Fazlioglu, *supra* note 8; *The U.S. Urgently Needs a Data Protection Agency*, *supra* note 7. Arguments that Congress should pass a federal data privacy regulation or that the Executive should create a data protection agency are outside the scope of this Note, as they have been covered extensively in other scholarship. By contrast, NIST is positioned uniquely within the Department of Commerce and is actively providing data privacy best practices through a voluntary framework.

277. *See* Copan, *supra* note 192.

278. CHOI, *supra* note 144, at 33. The framework's guidelines are so broad that they are not standard-setting. "In many or most cases, adopting such a framework merely means the entity has generated documentation to justify the practices it already performs." *Id.*

279. *See* Danker, *supra* note 21; *Business Case for the NIST Privacy Framework*, *supra* note 21; *Privacy Framework Perspectives and Success Stories*, *supra* note 21.

280. *See* Pittman et al., *supra* note 22; H.B. 1181, 113th Gen. Assemb., Reg. Sess. (Tenn. 2023).

281. *See About Commerce*, U.S. DEP'T OF COMM., https://www.commerce.gov/about [https://perma.cc/JX25-QJRR].

pursuit of societally harmful but financially beneficial activities may not be best located within the Department of Commerce. By contrast, agencies such as the CFPB have a mission to protect and enhance the lives of individuals.[282] The CFPB can prohibit financial practices that take advantage of consumers' inability to understand present risks and inherent vulnerabilities.[283] But the technical expertise needed to understand privacy and data may not currently exist within the CFPB. Moreover, the NIST AI framework addresses the vulnerability of consumers and the harms that result from discriminatory algorithms, suggesting that the fact that NIST is located within the Department of Commerce does not inhibit its ability to serve as a check on industry interests.

In addition to the CFPB, the FTC already brings enforcement actions against corporations. Unlike the CFPB, however, which has standard notice and comment rulemaking authority, the FTC has Magnuson-Moss rulemaking authority, which is procedurally burdensome and arguably ineffective.[284] Magnuson-Moss rulemaking goes beyond the Administrative Procedure Act's notice and comment process and requires the FTC to hold hearings and provide opportunities for testimony, cross examinations, and rebuttals.[285] The FTC's role could be expanded: it could monitor companies more closely for abusive data privacy tactics resulting

---

282. *See The CFPB*, CONSUMER FIN. PROT. BUREAU, https://www.consumerfinance.gov/about-us/the-bureau [https://perma.cc/54NL-SMJN].

283. *See* Richards & Hartzog, *Duty of Loyalty*, *supra* note 123, at 1011.

284. The following provides an overview of Magnuson-Moss rulemaking:

> In Magnuson-Moss rulemaking, the FTC must first issue an [advance notice of proposed rulemaking (ANPRM)] that contains a brief description of the issue and invites interested persons to submit responses. Following the ANPRM, the FTC may only proceed with the rulemaking if it determines that it has either issued cease-and-desist orders regarding such acts or practices or has any other information indicating a "widespread pattern" of unfair or deceptive acts or practices. If the FTC decides to proceed with the rulemaking, it must issue an NPRM and give interested persons an opportunity to comment, as well as provide for an informal hearing to resolve any disputed issues of material fact. These informal hearings are overseen by a Chief Presiding Officer and include oral testimony and, to the extent necessary, opportunities for cross-examination and rebuttals. Following the informal hearing, the Chief Presiding Officer must recommend a decision to the Commission based on the Officer's findings and conclusions of all the material evidence.

CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10839, FTC CONSIDERS ADOPTING COMMERCIAL SURVEILLANCE AND DATA SECURITY RULES 2–3 (2022); *see also* Solove & Hartzog, *supra* note 44, at 620 ("The FTC must rely heavily on its settlements to signal the basic rules that it wants companies to follow."); Arias, *supra* note 155.

285. The FTC rarely uses Magnuson-Moss rulemaking. *See* LINEBAUGH, *supra* note 284.

from information asymmetry and power imbalances.[286] But even if regulating data privacy more closely falls within the FTC's mandate to regulate deceptive practices, this is not an argument against NIST's role. The FTC can utilize a more robust NIST Privacy Framework when bringing enforcement actions, just as the agency uses the Cybersecurity Framework.[287] One argument against regulating data privacy within an administrative agency, and in favor of preserving NIST's role, is the impact of *Loper Bright* on deference to administrative action. Although the effects of *Loper Bright* have not yet been fully realized, it is probable that if data privacy were regulated by an administrative agency, judges would be more likely to conduct independent review of the agency's authority to make rules regulating this space.[288] This could be an argument against regulating data privacy within an administrative agency.[289] But *Loper Bright* will not impact NIST or the deference afforded to NIST's Frameworks because NIST is not an administrative agency and does not have enforcement power. NIST circumvents the administrative agency rulemaking process, but the Privacy Framework can and has been given legal effect through state data privacy legislation.[290] In a post-*Chevron* world, NIST's expanded regulatory role could have a greater impact on compliance than agency action that would be a near-certain target of industry litigation.

NIST may not be a regulatory agency, but it is providing regulatory guidelines nationwide, at both state and federal levels of government, for cybersecurity, privacy, and AI. Although there is room for improvement, the NIST Privacy Framework fills a gap created by the lack of a data protection agency, federal data privacy law, and the current fragmented data privacy landscape. The NIST Privacy Framework can be a mechanism through which companies successfully protect individuals' data privacy.

---

286. *See* Khan & Pozen, *supra* note 264, at 522; *see also* Allen, *Black Opticon*, *supra* note 28, at 946.

287. *See supra* notes 155–158 and accompanying text.

288. *See* Loper Bright Enters. v. Raimondo, 603 U.S. 369 (2024); *see generally* Cass R. Sunstein, *The Consequences of Loper Bright* (Harv. Pub. L. Working Paper No. 24-29, 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4881501.

289. Because NIST is not an administrative agency, this Note does not focus on the impacts of *Loper Bright* on NIST. In addition, because *Loper Bright* was decided so recently, the impacts of the decision on administrative agencies is unclear. *See* Sunstein, *supra* note 288.

290. *See* H.B. 1181, 113th Gen. Assemb., Reg. Sess. (Tenn. 2023).

CONCLUSION

The current data privacy landscape in the United States is disjointed, ineffective, and subject to many critiques. There is no federal data privacy law nor data protection agency.[291] The states that do have data privacy laws are heavily influenced by the tech industry, which results in the industry regulating itself.[292] As a result, it is nearly impossible for consumers to exercise meaningful control over the use of their personal information due to power imbalances between consumers and companies and consumers' reliance on digital services.[293] The lack of data privacy protections has significant societal and structural consequences and can impede an individual's ability to obtain employment, a loan, or insurance.[294]

In the absence of a federal regime, NIST plays a quasi-regulatory role in the privacy field, and its Privacy Framework can influence companies to protect consumers' data privacy. Because the NIST Privacy Framework has been incorporated into data privacy legislation and adopted as a legal standard, the process through which NIST created the Privacy Framework and its failure to consider consumer protection stakeholders needs to be reconsidered. NIST should engage with all relevant stakeholders, including public interest organizations, address the critiques of current data privacy laws and their failure to address social harms, and consider alternative formulations of how to regulate data privacy. The NIST Privacy Framework will then be a democratically accountable legal standard that productively contributes to the data privacy ecosystem, alleviating the need for federal action.

---

291. *See* Kibby, *supra* note 11.
292. *See* Bordelon & Ng, *supra* note 13.
293. *See* Hartzog, *supra* note 114, at 426.
294. *See* Waldman, *Privacy, Practice, and Performance*, *supra* note 64, at 1256; Richards & Hartzog, *Duty of Loyalty*, *supra* note 123, at 1005–06.