UNIVERSITY OF PITTSBURGH LAW REVIEW ONLINE
Vol. 83 ● 2022

CONSUMER DATA PROTECTION AND PRIVACY: A PROPOSAL FOR A NEW LAW AND AN INDEPENDENT AGENCY

Suzanne C. Bernstein

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

CONSUMER DATA PROTECTION AND PRIVACY: A PROPOSAL FOR A NEW LAW AND AN INDEPENDENT AGENCY*

Suzanne C. Bernstein**

ABSTRACT

From social media to banking and healthcare, online services increasingly pervade the everyday lives of American consumers. Currently, there is no comprehensive federal regulation to ensure personal data privacy and protection, and consumers have no ownership rights over their personal data. There are various information and sector specific privacy laws, enforced by multiple agencies with overlapping jurisdiction. Moreover, without a principal federal law, many states have developed their own data privacy regulations. Not only is this collective scheme ineffective for American consumers, but it is also an inefficient form of government regulation and makes compliance difficult. This Note proposes creating the Consumer Data Privacy and Protection Bureau, an independent agency that would consolidate jurisdiction for efficient and effective regulation through a consumer protection framework. It would be created through a new law, the Data Privacy and Protection Act. In addition to creating the Consumer Data Privacy and Protection Bureau, this baseline, comprehensive federal legislation would provide basic data rights to consumers, and ease compliance for

* An earlier version of this Note was presented at the 2021 annual meeting of the Law & Society in May 2021 and the Intersection of Law & Public Policy Symposium at Temple University Beasley School of Law in April 2021.

** Candidate for J.D., May 2022, Temple University Beasley School of Law; B.A. University of Pennsylvania, 2017. The author would like to thank the *Pittsburgh Law Review* staff and editors for their time and review, and Professor Nancy Knauer for her invaluable guidance and encouragement. Finally, the author would like to thank her parents Ellan and Len Bernstein for their unwavering support throughout law school and the process of writing this Note.

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

companies in the United States and abroad. With bipartisan support and an increasingly digital society, this type of reform is realistic, necessary, and timely.

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

INTRODUCTION

The average person creates more than 2.5 quintillion bytes of data each day, and much of this data consists of personal information.[1] The volume of personal data collected by companies online is continually increasing, and it ranges from financial and location records to personal photos.[2] Simultaneously, the only compliance mechanism to control this mass data collection is through "notice and consent"—the small-print terms and conditions agreement.[3] It is unlikely that the average consumer can read and understand "how companies are using or sharing their personal information" and whether their information is safe.[4] Companies often assure consumers that their personal data is secure and considered only as "metadata"—service-related, diagnostic, and performance information used to describe larger trends.[5] Realistically, consumers have no real choice but to accept the terms of the agreement.[6]

---

[1] Carole Piovesan, *How Privacy Laws Are Changing to Protect Personal Information*, FORBES (Apr. 5, 2019, 8:58 PM), https://www.forbes.com/sites/cognitiveworld/2019/04/05/how-privacy-laws-are-changing-to-protect-personal-information/#1f5d6cd5753d [https://perma.cc/6CWT-XXU3]; Jacquelyn Bulao, *How Much Data Is Created Every Day in 2021?*, TECHJURY: BLOG (Dec. 7, 2021), https://techjury.net/blog/how-much-data-is-created-every-day/#gref [https://perma.cc/B4WE-HN6T].

[2] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling a Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/A6JX-XYFV] [hereinafter *Americans and Privacy*].

[3] *Is it Time to Rethink Notice and Choice as a Fair Information Privacy Practice?*, COZEN O'CONNER: CYBER L. MONITOR, https://www.cyberlawmonitor.com/2019/02/13/is-it-time-to-rethink-notice-and-choice-as-a-fair-information-privacy-practice/ [https://perma.cc/A9YC-EJA5].

[4] *Id.*

[5] *See* Zak Doffman, *WhatsApp Beaten by Apple's New iMessage Privacy Update*, FORBES (Jan. 3, 2021, 5:30 AM), https://www.forbes.com/sites/zakdoffman/2021/01/03/whatsapp-beaten-by-apples-new-imessage-update-for-iphone-users/?sh=7db7642a3623 [https://perma.cc/8WUC-8ZYK]; gdad-s-river, *Metadata: Story of How Whatsapp and Other Chat Apps Collect Data*, FOSSBYTES: TECH (Jan. 27, 2017), https://fossbytes.com/whatsapp-chats-collect-data-metadata/ [https://perma.cc/NKZ8-5WK5].

[6] *See* Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1735 (2020) ("[N]otice and choice regimes are overwhelming. They simply do not scale because they conceive of control and transparency as something people can never get enough of.").

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

There is no comprehensive federal regulation to ensure protection of personal data, and consumers have no ownership rights over their personal data.[7] Senator Mark Warner (D-Va.), Chairman of the Senate Intelligence Committee, has asserted that there is an immediate need for basic regulation where technology and social media pervade American lives: "The size and reach of these [technology] platforms demand that we ensure proper oversight, transparency and effective management of technologies that in large measure undergird our social lives, economy and our politics."[8]

Additionally, there is "information asymmetry" within the relationship between the consumer and every company that collects personal data online. Information asymmetry occurs when one party in a transaction, in this case, the data collector, has more or better information than the other party, which is the consumer.[9] This Note addresses how information asymmetry disadvantages consumers through a consumer protection lens. It argues that the fundamental framework of consumer protection should cover personal data to ensure that consumers have the chance to make informed decisions about how companies use their data.

Ultimately, this Note proposes a new federal law that would provide Congress with authority to create a new independent agency and put forth a comprehensive consumer data privacy and protection regulatory scheme. The proposed law, The Consumer Data Privacy and Protection Act ("CDPPA"), would enable Congress to create the Consumer Data Privacy and Protection Bureau ("CDPPB"). This agency would broadly apply to many industries, providing basic personal data rights to consumers and imposing straightforward obligations for companies that collect, store, and sell such data. Moreover, much like the Consumer Finance Protection Bureau, the CDPPB would consolidate or share jurisdiction for existing data and

[7] Cameron F. Kerry, *Why Protecting Privacy is a Losing Game Today—and How to Change the Game*, BROOKINGS INST. (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/ [https://perma.cc/7R5C-Q4NB].

[8] SENATOR MARK R. WARNER, POTENTIAL POLICY PROPOSALS FOR REGULATION OF SOCIAL MEDIA AND TECHNOLOGY FIRMS (2018), https://graphics.axios.com/pdf/PlatformPolicyPaper.pdf [https://perma.cc/YL6U-2CJ5]; *see, e.g.*, Hartzog & Richards, *supra* note 6, at 1697 (arguing that America is due for a comprehensive data privacy bill).

[9] Christine S. Wilson, *A Defining Moment for Privacy: The Time is Ripe for Federal Privacy Legislation*, FTC (Feb. 6, 2020), https://www.ftc.gov/system/files/documents/public_statements/1566337/commissioner_wilson_privacy_forum_speech_02-06-2020.pdf [https://perma.cc/5MQD-9RVS].

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

privacy regulations and streamline the implementation of future personal data laws or regulations.[10]

Section I of this Note considers the current data privacy laws. Although there is no principal federal personal data regulation, there are various information-specific and sector-specific privacy laws.[11] Moreover, multiple agencies have jurisdiction over personal data privacy and protection issues, including the Federal Communications Commission ("FCC"), the Federal Trade Commission ("FTC"), the Department of Health and Human Services ("HHS"), the Department of Commerce ("DOC"), and the Consumer Financial Protection Bureau ("CFPB").[12] Lastly, this section will explore related state laws and recent regulatory developments under the Trump and Biden Administrations.

Section II addresses the reasons for change. The first subsection, Section II.A, focuses on regulatory and government efficiency. The current patchwork of regulations and overlapping jurisdiction among federal agencies is inefficient and ineffective.[13] Not only is it difficult for companies to comply with these disparate regulations, but the regulations also assure little consumer protection.[14] Some argue that a "predictable, scalable and extensible mechanism for regulating data . . . may improve the exercise and enforcement of[] rights regarding personal information."[15]

Section II.B considers business and market concerns. Consumer data is a major economic asset, and many sectors of the market rely heavily on consumer data to

[10] *See* 12 U.S.C. § 5491(a) (Consumer Financial Protection Bureau created within the Dodd-Frank Wall Street Reform and Consumer Protection Act to protect consumers through strong implementation and enforcement of Federal consumer financial laws).

[11] *See, e.g.*, Cable Communications Privacy Act, 47 U.S.C. § 551; Driver's Privacy Protection Act, 18 U.S.C. § 2721; Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506; Video Privacy Protection Act, 18 U.S.C. § 2710; Computer Fraud and Abuse Act, 18 U.S.C. § 1030; Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*; Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809, 6821–6827.

[12] *See generally* STEPHEN P. MULLIGAN & CHRIS D. LINEBAUGH., CONG. RSCH. SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW (2019), https://crsreports.congress.gov/product/pdf/R/R45631 [https://perma.cc/5EM7-TZXK].

[13] *Id.*

[14] *Id.*; Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48,600 (Sept. 26, 2018), https://www.federalregister.gov/documents/2018/09/26/2018-20941/developing-the-administrations-approach-to-consumer-privacy [https://perma.cc/DLH6-3PGC] [hereinafter RFC].

[15] Jeffrey Ritter & Anna Mayer, *Regulating Data as Property: A New Construct for Moving Forward*, 16 DUKE L. & TECH. REV. 220, 221 (2018).

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

inform their direction and planning.[16] A more straightforward compliance mechanism would be beneficial for business. Moreover, the current system, without any regulation, is anti-competitive: personal data grows in value as it accumulates, so firms with large amounts of personal data sets have a significant advantage over new industry entrants.[17] This imbalance could stunt innovation.

The last subsection, Section II.C, argues that the regulation of personal data should be implemented through a consumer protection framework. Extending the consumer protection framework to personal data accomplishes the dual goals of increasing personal data rights and security while also creating a sustainable regulatory framework for a massive and otherwise unregulated industry. American consumers face information asymmetry and make uninformed decisions about their personal data daily.[18] By increasing consumers' data rights to ensure they know about and control their personal data and requiring transparency from companies that collect, store, and sell data, the consumer protection framework could address chronicled security, privacy, and equity concerns.

Lastly, Section III proposes comprehensive statutory reform through the CDPPA, thereby enabling Congress to create the independent agency, CDPPB. The goal of this proposal is similar to that of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank"), which created the Consumer Finance Protection Bureau partly "to arm people with the information, steps, and tools that they need to make smart financial decisions."[19] Likewise, the CDPPB's purpose is to provide consumers with sufficient information to make informed decisions about usage of their personal data. The CDPPB would negotiate to consolidate or share jurisdiction that is otherwise spread out among various agencies to accomplish this goal. Centralizing the enforcement of existing data security and privacy regulations would consolidate regulatory efforts and make them more efficient. It would also

[16] Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1371 (2017) ("Companies, such as Facebook and Google, have based their business models on collecting and analyzing user data.").

[17] *See* FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? 1–2 (2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf [https://perma.cc/VW7P-MVYL].

[18] Wilson, *supra* note 9, at 4–5.

[19] *The Bureau*, CFBP, https://www.consumerfinance.gov/about-us/the-bureau/#:~:text=Our%20core%20functions,was%20divided%20among%20several%20agencies [https://perma.cc/ZA5W-8N55].

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

enable the agency to enforce a more comprehensive personal data regulation within the CDPPA.

In addition to providing the statutory authority to create the CDPPB, the CDPPA would provide baseline consumer data protections that have broad application to different types of personal data across industries. Much like the Fair Credit Reporting Act's ("FCRA") limited preemption,[20] the CDPPA would not preempt state laws unless there were direct inconsistencies, allowing states to customize their data protection laws. The CDPPA would ease compliance across the United States by setting a federal baseline for consumer data regulation, thereby increasing consumer protection, and ensuring entity compliance across jurisdictions.

There is bipartisan support for a range of personal data regulations and creative solutions emerging from outside of government.[21] Comprehensive legislation coupled with the creation of an independent agency could harness this momentum in an impactful and long-lasting way. As we continue to dive deeper into the internet age, there is an immediate need for reform to protect consumer data and ensure competition and compliance across industries.

I. A PATCHWORK OF CURRENT FEDERAL AND STATE PRIVACY LAWS

In the United States, there is no single federal law that comprehensively regulates the use of consumer data.[22] Although there is a constitutional right recognized by the Supreme Court to individual privacy in many instances, this right guards against government intrusion but does "little to prevent private actors from abusing personal data online."[23] Additionally, the existing federal regulatory framework lacks uniformity.[24] Section I.A explores each layer of the current federal law—laws that are either information- or sector-specific—and the various federal agencies with jurisdiction to enforce the wide range of privacy laws and regulations.

---

[20] 15 U.S.C. § 1681t.

[21] *See, e.g.*, Cameron F. Kerry & Caitlin Chin, *By Passing Proposition 24, California Voters Up the Ante on Federal Privacy Law*, BROOKINGS INST. (Nov. 17, 2020), https://www.brookings.edu/blog/techtank/2020/11/17/by-passing-proposition-24-california-voters-up-the-ante-on-federal-privacy-law/ [https://perma.cc/A5YU-YKWJ].

[22] MULLIGAN & LINEBAUGH, *supra* note 12, at 2.

[23] *Id.*

[24] *Id.*

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

Next, Section I.B summarizes state laws that are in place or are developing through the legislative process. As of February 2022, California, Virginia, and Colorado have implemented comprehensive consumer data laws, and nearly two dozen other states are considering or drafting similar legislation.[25] This section will also highlight the current trends and similarities across various state laws.

Finally, Section I.C examines the recent action of the Trump and Biden Administrations. In September 2018, the U.S. Department of Commerce's National Telecommunications Information Administration ("NTIA") issued a Request for Comments ("RFC") on a general approach to consumer data privacy.[26] The stated goal was to determine the best "path toward protecting individual's privacy while fostering innovation."[27] The RFC sought ideas with a two-fold approach to achieve these goals.[28] First, the RFC focused on a user-centric focus on consumer data privacy, in which federal action could ensure a reasonably informed consumer.[29] Second, the RFC discussed a harmonized federal framework to implement those federal actions or regulations.[30] While the Biden Administration has yet to put forth a plan to address data privacy, many believe that a proposal is forthcoming.[31]

---

[25] Taylor Kay Lively, *US State Privacy Legislation Tracker*, INT'L ASS'N OF PRIV. PROS., https://iapp.org/resources/article/state-comparison-table/ [https://perma.cc/NY8P-AF87].

[26] Press Release, NTIA, NTIA Seeks Comment on New Approach to Consumer Data Privacy (Sept. 25, 2018), https://www.ntia.doc.gov/press-release/2018/ntia-seeks-comment-new-approach-consumer-data-privacy [https://perma.cc/JBZ4-F485].

[27] RFC, *supra* note 14.

[28] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600 (Sept. 26, 2018) (request for public comments), https://www.govinfo.gov/content/pkg/FR-2018-09-26/pdf/2018-20941.pdf [https://perma.cc/34BY-JSYB].

[29] *Id.* at 48601.

[30] *Id.*

[31] Colin Rahill, *The State of Privacy Under a Biden Administration: Federal Cybersecurity Legislation, Strict Regulatory Enforcement, and a New Privacy Shield with the EU*, JOLT DIG (Feb. 20, 2021), https://jolt.law.harvard.edu/digest/the-state-of-privacy-under-a-biden-administration-federal-cybersecurity-legislation-strict-regulatory-enforcement-and-a-new-privacy-shield-with-the-eu [https://perma.cc/LY3H-KZPL].

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

A. Federal Law

Although there is no principal consumer data law, there is a patchwork of federal privacy laws and regulations ranging in purpose and scope.[32] There are a handful of laws whose jurisdiction is contingent on the kind of information they seek to regulate.[33] Some of these laws have been in place for decades. For example, the Cable Communications Privacy Act has been regulating the privacy of subscriber information for over thirty-five years.[34] Other notable information-specific privacy statutes include the Driver's Privacy Protection Act of 1994,[35] the Children's Online Privacy Protection Act of 1998,[36] the Video Privacy Protection Act,[37] and the Computer Fraud and Abuse Act of 1986.[38]

The second source of federal privacy regulation is sector-specific. The four sectors with associated regulations or laws are financial services, healthcare, telecommunications, and education. In the financial services sector, the Fair Credit Reporting Act, later amended by the Fair and Accurate Credit Transactions Act of 2003, regulates the use of personal information related to credit.[39] Additionally, the Gramm-Leach-Bliley Act ("GLBA") governs the use of personal data that is in the hands of financial services entities like banks and insurance companies.[40] The GLBA oversees the use of "nonpublic personal information," which includes personal information that financial services companies collect in connection with their products or services.[41]

---

[32] *See* Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELS.: DIGIT. AND CYBERSPACE POL'Y PROGRAM (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/M3YA-H7AL].

[33] Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, N.Y. TIMES: WIRECUTTER (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/ [https://perma.cc/5NAH-FD47].

[34] 47 U.S.C. § 551(a)–(h).

[35] 18 U.S.C. § 2721.

[36] 15 U.S.C. §§ 6501–6506 (2018).

[37] 18 U.S.C. § 2710 (2018).

[38] 18 U.S.C. § 1030 (Supp. II 1987).

[39] 15 U.S.C. §§ 1681–1681x (2018). *See also* 12 C.F.R. § 1022 (2019) ("Regulation V").

[40] Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §§ 6801–6809, 6821–6827.

[41] MULLIGAN & LINEBAUGH, *supra* note 12, at 8 (citing 15 U.S.C. § 6809(9)).

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

The significant healthcare privacy and personal data protection law is the Health Information Portability and Accountability Act ("HIPAA").[42] It regulates the use and privacy of health information held by covered entities like hospitals or other medical providers.[43] Additionally, there are security requirements protecting personal health information.[44] Similar to HIPPAA, The Family Educational Rights and Privacy Act ("FERPA") oversees personal records in the education sector.[45] Under FERPA, students and their families have the right to access their educational records, including personal information about the student, and prohibit disclosure of the records without consent.[46] Finally, the Telephone Consumer Protection Act governs the telecommunications sector by regulating automated calls and texts to consumers.[47]

Concluding the overview of current federal privacy laws, various agencies have jurisdiction to enforce the complicated regulatory scheme. However, the U.S. does not have a plenary regulating agency for data protection or privacy. The laws are either sector-specific or information-specific and are enforced by different federal agencies, often with overlapping jurisdiction. Some of these agencies include the Department of Commerce, the Securities and Exchange Commission, the Federal Communications Commission, and the Department of Health and Human Services.[48] The two agencies with the broadest jurisdiction for consumer privacy regulation enforcement are the Federal Trade Commission ("FTC") and the Consumer Finance Protection Bureau ("CFPB").[49]

The FTC has the broadest jurisdiction and authority over data privacy, effectively filling the regulatory gaps left by other federal statutes and regulations.[50] Their authority derives from section five of the FTC Act, which declares unlawful

[42] *See* Health Insurance Portability and Accountability Act of 1996 (HIPAA), 1 Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of the U.S. Code).

[43] *Id.*

[44] *Id.*

[45] 20 U.S.C. § 1232g.

[46] *Id.*

[47] 47 U.S.C. § 227.

[48] *See* MULLIGAN & LINEBAUGH, *supra* note 12.

[49] *Id.* at 8.

[50] Daniel Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 587–88 (2014).

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

"unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[51] Section five of the Act defines the operative term in the clause, "unfair and deceptive acts or practices" ("UDAP") as related to commerce within foreign nations.[52] The FTC considers a UDAP to be either a deceptive practice, an unfair practice, or both.[53] Section five empowers the FTC to protect consumers against UDAP by investigating and bringing enforcement actions against companies that act deceptively or unfairly.[54] The FTC claims that "companies act deceptively when they gather, use, or disclose personal information in a way that contradicts their posted privacy policy or other statements, or when they fail to adequately protect personal information."[55] Additionally, a company can act deceptively by making a false representation that affects the collection of personal information.[56]

Similar to FTC's jurisdiction over UDAP, the CFPB has jurisdiction to address unfair and deceptive acts and practices, as well as "abusive" practices.[57] The CFPB considers an act or practice to be abusive if it "materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service," or if it takes unreasonable advantage of the consumer's lack of understanding or inability to protect their interests.[58] Currently, the CFPB only has jurisdiction within the context of financial services and products.[59] They have been reluctant to expand jurisdiction beyond those boundaries into the wider data privacy and security space.[60]

---

[51] 15 U.S.C. § 45(a)(1).

[52] MULLIGAN & LINEBAUGH, *supra* note 12, at 30 (citing 15 U.S.C. § 45(a)(1)).

[53] *Id.* at 30–31.

[54] *Id.* at 32; *see also* FTC, A BRIEF OVERVIEW OF THE FEDERAL TRADE COMMISSION'S INVESTIGATIVE AND LAW ENFORCEMENT AUTHORITY (May 2021), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [https://perma.cc/KLC7-D773].

[55] *Id.* at 32.

[56] *Id.*

[57] 12 U.S.C. § 5531(d).

[58] *Id.*

[59] MULLIGAN & LINEBAUGH, *supra* note 12, at 35.

[60] *Id.* at 36.

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

B. State Law

Despite the patchwork of federal legislation, "state-level momentum for comprehensive privacy bills is at an all-time high."[61] Nearly two dozen states have proposed their own legislation, designated task forces, or implemented regulations in recent years.[62] It is clear that there is a focus on consumer protection among the states considering such legislation.[63] A theme has emerged across the various states' regulations: a mixture of consumer rights and obligations for businesses. Some of the consumer rights include allowing access, deletion, and opting-out of data collection.[64] For business obligations, some of the regulatory schemes require data breach notifications, risk assessment, opt-in for sale of data, and a transparency requirement.[65]

As of February 2022, three states have successfully enacted comprehensive state privacy laws that regulate consumer data protection: California,[66] Virginia,[67] and most recently, Colorado.[68] Relatedly, Illinois has implemented a biometric data privacy law.[69]

The California Consumer Privacy Act ("CCPA") went into effect in 2020 and has already had a national impact because it applies to any company that collects the personal information of California residents.[70] The CCPA provides consumers three primary rights: first, Californians have the right to know the information that businesses have collected from them and if the businesses have sold this information; second, they have a right to opt-out of the sale of their collected personal information;

---

[61] Lively, *supra* note 25; *see, e.g.*, Hartzog & Richards, *supra* note 6, at 1694 ("U.S. privacy law is in the midst of a 'constitutional moment'—a period of unusual public engagement likely to result in a significant and durable settlement of the issues.").

[62] Hartzog & Richards, *supra* note 6, at 1691. *See* Lively, *supra* note 25.

[63] *See id.*

[64] *Id.* at 1711.

[65] *Id.* at 1713.

[66] California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100–1798.199 (West 2018).

[67] Virginia Consumer Data Protection Act, Va. Code Ann. §§ 59.1-575 to 59.1-585.

[68] Colorado Privacy Act, Colo. Rev. Stat. Ann. §§ 6-1-1301 to 6-1-1313 (West 2021).

[69] Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/1 (2008).

[70] *See* MULLIGAN & LINEBAUGH, *supra* note 12, at 38.

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

and finally, Californians have the right to delete their collected personal data, in certain circumstances.[71]

C. Recent Developments Under the Trump and Biden Administrations

In September 2018, the NTIA published a Request for Comment ("RFC") titled: "Developing the Administration's Approach to Consumer Privacy."[72] NTIA's objective was to determine how to best protect consumer privacy while also fostering innovation.[73] The RFC acknowledged the modern digital environment, including the pervasiveness of personal data collection,[74] and noted that users have growing privacy concerns about their personal information online.[75] It also illustrated how the current fragmented federal regulations disincentivize innovation and make compliance difficult for many companies.[76] The RFC outlined the Trump Administration's general approach to consumer privacy: federal regulations that increase consumer privacy outcomes while also creating a regulatory "ecosystem" that enables easier compliance to enhance competition and innovation.[77] The RFC envisioned the FTC as the appropriate federal agency to enforce the consumer data protection regulations despite acknowledging its lack of jurisdiction over other privacy laws like HIPAA.[78]

Determining how to facilitate a reasonably informed internet user was subject to comment under the RFC.[79] It lamented that the lengthy privacy policies and checkboxes are insufficient and rarely read by consumers.[80] The desired goal of the RFC was a "reasonably informed user, empowered to meaningfully express privacy preferences."[81] There were seven elements in this category for which the RFC sought

[71] *Id.* at 38–39.

[72] RFC, *supra* note 14.

[73] *Id.*

[74] *Id.*

[75] *Id.*

[76] *Id.* at 48,602.

[77] *Id.* at 48,601.

[78] *Id.* at 48,602.

[79] *Id.* at 48,601.

[80] *Id.*

[81] *Id.*

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

comment, two of which were more notable than the others: transparency and control. Transparency would allow users to easily understand how an organization uses, stores, or shares their personal information.[82] Control would provide the user with the right to have reasonable control over their data and enable them to withdraw consent from an organization's use of their data.[83] The other five elements included reasonable minimization of data collection, security, access to correction of personal data, risk management for companies, and accountability.[84]

The second category of the RFC were a set of high-level goals to create a regulatory ecosystem for consumer data privacy protections. The eight high-level goals for Federal action highlighted the need to harmonize the regulatory landscape.[85] Between the overlapping jurisdiction and duplicative regulations, the Administration believed that the emerging "patchwork of competing and contradictory baseline laws . . . harms the American economy and fails to improve privacy outcomes for individuals."[86] The RFC indicates that the eight high-level goals were a "non-exhaustive and non-prioritized list of the Administration's priorities." The other elements for consideration within this category included: outcome-based approaches, interoperability, incentivizing privacy research, and FTC enforcement.[87] On November 13, 2018, NTIA announced that it received over 200 comments in response to the RFC from "individuals, industry associations, companies, civil society and academics."[88]

While the Biden Administration has yet to release a concrete plan for federal data privacy legislation,[89] the Administration has taken a few steps related to data privacy and protection. Notably, NTIA under the Biden Administration has hosted three listening sessions concerning Personal Data in December 2021 specifically

[82] *Id.*

[83] *Id.*

[84] *Id.* at 48,601–02.

[85] *Id.* at 48,602.

[86] *Id.*

[87] *Id.*

[88] Press Release, NTIA, NTIA Releases Comments on a Proposed Approach to Protecting Consumer Privacy (Nov. 13, 2018), https://www.ntia.doc.gov/press-release/2018/ntia-releases-comments-proposed-approach-protecting-consumer-privacy [https://perma.cc/NF4Q-VRWD].

[89] Rahill, *supra* note 31.

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

about the intersection of privacy, equity, and civil rights.[90] Additionally, NTIA intends to solicit related comments through a forthcoming, formal RFC.[91] President Biden also issued an Executive Order in July 2021 "Promoting Competition in the American Economy" with potential implications for privacy use and FTC oversight of data accumulation.[92]

Meanwhile, nearly half of the states are poised to pass their own laws in the next few years, further exacerbating the inconsistencies in data privacy regulation.[93] International factors may also encourage the Biden Administration to push for a comprehensive data privacy plan. The EU and the United States are still in negotiations after the European Court of Justice dissolved the EU-U.S. data sharing agreement, known as the Data Privacy Shield, in 2020.[94] The easiest way for the United States to fix this valuable transatlantic trade relationship would be to implement a uniform, federal data privacy law.[95] Another relevant factor impacting the Biden Administration's pending action on data privacy is Vice President Kamala Harris. During her time as Attorney General of California, Vice President Harris gained experience and familiarity with the technology industry, and she was involved in the development of the CCPA.[96] Responding to a question about reducing the size of giant technology companies during her own presidential run, Vice President

[90] Privacy, Equity, and Civil Rights Listening Sessions, 86 Fed. Reg. 67,925 (Nov. 30, 2021), https://www.ntia.doc.gov/files/ntia/publications/fr-ntia-listening-sessions-11302021.pdf [https://perma.cc/EYT5-6E6W].

[91] Press Release, NTIA, NTIA Virtual Listening Sessions on Personal Data: Privacy, Equity, and Civil Rights (Jan. 3, 2022), https://www.ntia.doc.gov/other-publication/2022/ntia-virtual-listening-sessions-personal-data-privacy-equity-and-civil-rights [https://perma.cc/8KDP-AZ4W].

[92] Press Release, The White House, Executive Order on Promoting Competition in the American Economy (July 9, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/ [https://perma.cc/G6LG-CJ3P]. *See* Press Release, Fact Sheet: Executive Order on Promoting Competition in the American Economy (July 9, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/09/fact-sheet-executive-order-on-promoting-competition-in-the-american-economy/ [https://perma.cc/62TE-5MEN].

[93] Rahill, *supra* note 31.

[94] Adam Satariano, *E.U. Court Strikes Down Trans-Atlantic Data Transfer Pact*, N.Y. TIMES (July 16, 2020), https://www.nytimes.com/2020/07/16/business/eu-data-transfer-pact-rejected.html [https://perma.cc/Z8YE-W7Z9].

[95] Rahill, *supra* note 31 ("Biden's responsibility will be to achieve uniformity in privacy law by enacting federal legislation.").

[96] *Id. See* Daisuke Wakabayashi et al., *How Kamala Harris Forged Close Ties with Big Tech*, N.Y. TIMES (Jan. 20, 2021), https://www.nytimes.com/2020/08/20/technology/kamala-harris-ties-to-big-tech.html [https://perma.cc/52LN-PEFP].

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

Harris stated instead that, if elected, her "first priority is going to be that we ensure that privacy is something that is intact, and that consumers have the power to make decisions about what happens with their personal information, and that it is not being made for them."[97]

Although the Biden Administration's primary focus is on controlling the spread of COVID-19 and addressing America's crumbling infrastructure, the Administration will likely put forth a plan on data privacy and protection this term.[98]

II. CONSUMER DATA PRIVACY AND PROTECTION LEGISLATION IS NECESSARY AND TIMELY

The use of social media, online shopping, banking, and digital healthcare continues to increase, and the "amount of personal information that is being exchanged each day is staggering and growing."[99] Simultaneously, there is mounting concern about the collection, storage, and use of personal data.[100] The current personal data protection and privacy framework is insufficient for three main stakeholders: the federal government, businesses, and consumers.[101] In a February 2020 speech, FTC Commissioner Wilson described the current environment as a "tipping point" for consumer data privacy, adding that "all eyes are on Congress during this defining moment."[102] This section examines the momentum for seeking legislative change from each stakeholder.

Section II.A's discussion argues that the federal government lacks regulatory efficiency with regard to consumer data. Currently, there is an uneven approach with information-specific and sector-specific laws because various federal agencies, with overlapping jurisdictions, regulate these laws.[103] This strategy does not reflect the ubiquity of data.[104] It is inefficient and compromises the security of Americans'

[97] Alexander Burns et al., *Meet the Candidates: Kamala Harris*, N.Y. TIMES, https://www.nytimes.com/interactive/2019/us/politics/kamala-harris-2020-campaign.html#tech [https://perma.cc/8WTN-VBB3].

[98] Rahill, *supra* note 31.

[99] Piovesan, *supra* note 1.

[100] *See Americans and Privacy*, *supra* note 2.

[101] *See* O'Connor, *supra* note 32.

[102] Wilson, *supra* note 9; *see* Hartzog & Richards, *supra* note 6, at 1705 ("Congress, it seems, is finally feeling the heat to act decisively on privacy.").

[103] O'Connor, *supra* note 32.

[104] *See* MULLIGAN & LINEBAUGH, *supra* note 12.

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

consumer data.[105] Section II.B then discusses the economic and business concerns within the current federal regulatory framework. The rapid growth of the data-driven economy has led to costly compliance, and the lack of regulation is anti-competitive and disincentivizes innovation.[106]

Finally, Section II.C considers contemporary personal data issues through a consumer protection framework. The classic principles of consumer protection in the United States—to protect consumers and maintain competition—should inform federal regulation of consumer data. When considering the related goals of security, fairness, and equity, American consumers should be reasonably informed users.[107] However, American consumers face information asymmetry;[108] they do not fully understand or consent to how their data is being collected or understand privacy characteristics of digital products and services.[109] Through ballot initiatives, lobbying, and consumer advocacy for new regulation and protection, consumers and consumer privacy issues are finally generating considerable momentum.[110]

A. Federal Government Inefficiency

Rather than a single, comprehensive data privacy law, current U.S. laws are information-specific or sector-specific.[111] Moreover, a handful of federal agencies share overlapping jurisdiction for enforcement or additional rulemaking.[112] The result is a complex, technical, regulatory scheme that lacks uniformity at the federal

---

[105] Maya Villasenor, *Consumer-Facing Companies Still Have Few Incentives to Stop Data Breaches, and That's a National Security Concern*, COUNCIL ON FOREIGN RELS. (Oct. 26, 2021), https://www.cfr.org/blog/consumer-facing-companies-still-have-few-incentives-stop-data-breaches-and-thats-national [https://perma.cc/Z27U-STQF] (explaining there is a confusing patchwork of disclosure laws, and a lack of coherence disadvantages consumers and U.S. cybersecurity strategy).

[106] *See* Robert Walters, Bruno Zeller & Leon Trakman, *Personal Data Law and Competition Law—Where Is It Heading?*, 39 EUR. COMPETITION L. REV. 505, 505 (2018).

[107] *See generally* Timothy Morey, Theodore Forbath & Allison Schoop, *Consumer Data: Designing for Transparency and Trust*, HARV. BUS. REV. (May 2015), https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust [https://perma.cc/3F7N-DUCT] ("In a future in which customer data will be a growing source of competitive advantage, gaining consumers' confidence will be key.").

[108] Wilson, *supra* note 9.

[109] *Id.*

[110] *See, e.g.*, Kerry & Chin, *supra* note 21.

[111] MULLIGAN & LINEBAUGH, *supra* note 12, at 7–34.

[112] *Id.* at 57 ("As discussed, under the current patchwork of federal data protection laws, there are multiple federal agencies responsible for enforcing the myriad federal statutory protections, such as the FTC, CFBP, FCC, and HHS.").

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

level.[113] This lack of uniformity is problematic because data is ubiquitous;[114] there is frequent overlap between information- and sector-specific laws, which implicates multiple agencies for enforcement.[115] Many are calling for a comprehensive data privacy and protection regulation, similar to the General Data Protection Regulation ("GDPR") in the EU, the CCPA in California,[116] or the model used in Colorado and Virginia.[117] Moreover, if Congress continues to stall, "states are likely to follow the CCPA's lead and pass mini-GDPRs at the state level."[118]

It is in the federal government's interest to improve its data privacy regulatory framework for two reasons. First, the current patchwork of laws and regulations is an inefficient form of digital governance. Second, they are not meeting the needs of constituents, both consumers and businesses alike.

Because there is no comprehensive federal law in this field, there are hundreds of disparate legal requirements related to consumer data and privacy.[119] The lack of uniformity complicates compliance and security and leaves consumers without any real understanding of their personal data rights.[120]

One example of this uneven approach is health data. Many consumers "reveal detailed, sensitive health information online. Through wearable devices, social media posts, traceable web searches, and online patient communities, users generate

[113] *Id.* at 2.

[114] Wilson, *supra* note 9, at 8.

[115] MULLIGAN & LINEBAUGH, *supra* note 12, at 57.

[116] *Id.* at 62–63; *see generally* Kerry & Chin, *supra* note 21.

[117] *See generally* Mark Brennan & Ryan Woo, *10 Key Differences Between the 2023 California, Virginia, and Colorado Privacy Laws*, JD SUPRA (July 1, 2021), https://www.jdsupra.com/legalnews/10-key-differences-between-the-2023-5939867/ [https://perma.cc/CUF2-AMFP].

[118] Hartzog & Richards, *supra* note 6, at 1713.

[119] Yaki Faitelson, *Data Privacy Disruption in the U.S.*, FORBES (Dec. 12, 2018, 9:30 AM), https://www.forbes.com/sites/forbestechcouncil/2018/12/12/data-privacy-disruption-in-the-u-s/#73c6f87715cc [https://perma.cc/22NV-V89Q].

[120] *See* Elvy, *supra* note 16, at 1140–41 ("Research on consumers' understanding of privacy policies has also consistently found that a significant number of consumers do not understand the meaning of the term 'privacy policy,' and many mistakenly believe that the existence of a privacy policy means that their data will not be disclosed or shared with third parties.").

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

large volumes of health data."[121] However, HIPAA only applies to "covered entities" "holding protected health information,"[122] and only covers identifiable health data.[123] Not only are sites such as Google, Facebook, and Twitter not covered entities under the law, but also the health information that is deidentified or anonymized is not protected by HIPAA.[124] Firms can therefore "use health data for various purposes targeting consumers and patients based on profiles assembled from tracked user behavior, data purchased from other sources, and predictive analytics."[125] The major regulatory gaps and inconsistencies in health data privacy is just one example of how the current regulatory scheme is not conducive to effective oversight or protecting personal data.

The patchwork of federal laws and regulations also has consequences for the security of personal data. Many businesses provide services and products to consumers across multiple industries and states—consequently, they are subject to the governance of various regulations and agencies.[126] Without clear, comprehensive regulations for security, companies are not effectively "put on notice that they need to prioritize data security";[127] the most prevalent data security laws and regulations have developed in response to—and not in prevention of—security breaches.[128] This framework is not particularly helpful to consumers because "by the time a breach is disclosed, harm could already have befallen hundreds of thousands, if not millions of individuals."[129] To complicate matters further, there are fifty unique state data breach laws in addition to the federal data breach laws based on industry or type of

[121] Lawrence O. Gostin et al., *Health Data and Privacy in the Digital Era*, GEORGETOWN LAW FACULTY PUBLICATIONS AND OTHER WORKS 233 (July 17, 2018), https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3099&context=facpub [https://perma.cc/8M63-DQLA].

[122] O'Connor, *supra* note 32.

[123] Gostin et al., *supra* note 121.

[124] *Id.*

[125] *Id.*

[126] O'Connor, *supra* note 32 ("Meaningful federal laws and regulations should seek to resolve the differences among the existing federal and state legal rights and responsibilities. This would not only simplify compliance for U.S. companies, but would also strengthen and bring the United States in line with emerging data-protection norms.").

[127] *Id.*

[128] *Id.* ("Yet record-shattering data breaches and inadequate data-protection practices have produced only piecemeal legislative responses at the federal level, competing state laws, and a myriad of enforcement regimes.").

[129] *Id.*

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

information.[130] Compliance with these various data breach notification laws is expensive, burdensome, and exceedingly complex.[131] The regulatory focus on data breach responses is insufficient to secure consumer data, and the volume of unique laws and regulations addressing the same issue is inefficient for compliance and enforcement.

Finally, the federal law should change to prepare for an increasingly digital future. Other advanced economies, like the European Union, Israel, Japan, and Canada, have developed comprehensive approaches to personal data privacy and protection and provided users with a set of privacy rights.[132] The U.S. federal government is ill-equipped to regulate emerging technology issues without a comprehensive data privacy law or a uniform agency to control enforcement.[133]

B. Market Concerns

Personal data will increasingly fuel the twenty-first-century economy.[134] Not only is personal data a seemingly inexhaustible resource, but the data-driven economy is also largely unregulated in the United States.[135] Although this may seem like a free-market dream, America's current federal regulatory scheme raises major concerns for companies of all sizes operating with American personal data. There are two distinct areas of concern: first, the difficulty and cost of compliance with various state and federal laws, and second, the lack of comprehensive personal data privacy and protection legislation has an anti-competitive impact on the market.

There are compliance challenges for companies of all sizes. Certain products or companies may deal with personal data across states, information types, and business areas.[136] In addition to complying with various sector and information-

[130] FED. TRADE COMM'N, DATA BREACH RESPONSE: A GUIDE FOR BUSINESS, https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business [https://perma.cc/7X29-D4MZ].

[131] Faitelson, *supra* note 119.

[132] O'Connor, *supra* note 32.

[133] *See* Julie Brill, *GDPR's First Anniversary: A Year of Progress in Privacy Protection*, MICROSOFT: ON THE ISSUES (May 20, 2019), https://blogs.microsoft.com/on-the-issues/2019/05/20/gdprs-first-anniversary-a-year-of-progress-in-privacy-protection/ [https://perma.cc/YS5B-23MU].

[134] O'Connor, *supra* note 32.

[135] *Grading on a Curve: Privacy Legislation in the 116th Congress*, ELEC. PRIV. INFO CTR. 1, 2 (Apr. 2020), https://archive.epic.org/GradingOnACurve/EPIC-GradingOnACurve-Apr2020.pdf [https://perma.cc/E5X6-95KT] ("U.S. privacy law is considered out of date and ineffective.") [hereinafter EPIC].

[136] Kerry, *supra* note 7 ("Today, our checkerboard of privacy and data security laws covers data that concerns people the most. These include health data, genetic information, student records and information

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

specific laws for personal data privacy, companies must also comply with laws that govern security breach responses.[137] Identifying and ultimately complying with these laws or regulations is costly and burdensome.[138]

Additionally, international compliance is increasingly difficult. The European Union, and other advanced economies, have pivoted towards more comprehensive data privacy regimes, leaving the United States as a global outlier.[139] In the global economy, compliance with numerous laws and regulations in the United States and entirely different privacy approaches abroad is an expensive burden.[140] Advocates for federal reform argue that "consistency among regulatory frameworks reduces company costs, promotes international competitiveness, and increases compliance with privacy standards."[141]

In July 2020, companies operating in the United States with personal data from the European Union saw harsh effects from the inconsistent regulatory frameworks.[142] The European Court of Justice invalidated the EU-U.S. Privacy Shield, which was the most recent data-sharing agreement.[143] The Court held that the Privacy Shield did not provide adequate protection for EU citizens' data.[144] This decision created a tremendous amount of compliance work for corporate legal departments and threatened to interrupt the data flow between the United States and the European Union that underpins a $7.1 trillion transatlantic economic relationship.[145]

---

pertaining to children in general, financial information, and electronic communications (with differing rules for telecommunications carriers, cable providers, and emails).").

[137] *Id.* ("[A]ll 50 states now have laws requiring notification of data breaches (with variations in who has to be notified, how quickly, and in what circumstances).").

[138] *See* Wilson, *supra* note 9, at 7.

[139] O'Connor, *supra* note 32.

[140] *See* Yaki Faitelson, *Why U.S. GDPR-Style Privacy Laws Are Good For Business*, FORBES (Dec. 19, 2019), https://www.forbes.com/sites/forbestechcouncil/2019/12/19/why-u-s-gdpr-style-privacy-laws-are-good-for-business/?sh=625272d48756 [https://perma.cc/93M9-DPVX] (arguing that a comprehensive data privacy law would lower compliance costs).

[141] *See* Wilson, *supra* note 9, at 9.

[142] *See, e.g.*, Satariano, *supra* note 94.

[143] *Id.*

[144] *Id.*

[145] *Id.*

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

Business leaders have been vocal about the high cost of compliance and ineffectiveness of fragmented data privacy laws.[146] In 2019, CEOs of 51 companies such as Target, Amazon, and IBM signed a letter to congressional leaders encouraging the creation of a consumer data privacy law.[147] The letter indicated a "widespread agreement among companies across all sectors of the economy . . . about the need for a comprehensive federal consumer data privacy law . . . ."[148] Their reasoning balanced both the need for consumer confidence that their personal data is being treated responsibly, and continued the growth and competition in the digital economy.[149]

The patchwork of data privacy and protection laws and regulations is anti-competitive in many ways.[150] First, the high costs of compliance with a fragmented regulatory landscape "naturally disincentivizes innovation by increasing regulatory costs for products that require scale."[151] Second, personal data increases in value as it accumulates, so firms amassing large amounts of personal data sets often have an insurmountable advantage over newer entrants to an industry.[152] In contemporary, data-driven capitalism, various industries from business to "technology, infrastructure, finance, manufacturing and energy are now treating data as a form of capital."[153] The accumulation of data informs decision-making in business and corporate governance. They use the data to profile and target consumers; grow the value of assets; model probabilities; and build, manage, control, and optimize systems and services.[154]

---

[146] Cillian Kieran, *Divided We Fall: Why Fragmented Global Privacy Regulation Won't Work*, VENTUREBEAT (May 2, 2021), https://venturebeat.com/2021/05/02/divided-we-fall-why-fragmented-global-privacy-regulation-wont-work/ [https://perma.cc/6ENB-W3FV].

[147] Lauren Feiner, *CEOs from Amazon, IBM, Salesforce and More Ask Congress to Pass A Consumer Data Privacy Law*, CNBC (Sept. 10, 2019), https://www.cnbc.com/2019/09/10/business-roundtable-urges-congress-to-pass-consumer-data-privacy-law.html [https://perma.cc/6GW7-JYAX].

[148] *Id.*

[149] *Id.*

[150] Hartzog & Richards, *supra* note 6, at 1743 ("Competition law has been underutilized as a privacy regulatory tool, but there is a groundswell of support to change that.").

[151] RFC, *supra* note 14, at 48,600.

[152] Jathan Sadowski, *When Data is Capital: Datafication, Accumulation and Extraction*, BIG DATA & SOC'Y 1,1 (Jan. 7, 2019).

[153] *Id.* at 1.

[154] *Id.* at 5–6.

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

Finally, a consequence of the current reliance on opt-in consent for use of personal information "may be the entrenching monopolies."[155] The status quo is an opt-in consent where consumers theoretically read small-print privacy policies and agree to the terms and conditions of the website or product.[156] Realistically, consumers rarely read the entire terms and conditions before exercising opt-in consent and "are more likely to grant their opt-in consent to large networks with a broad scope rather than to less established firms."[157] As a result, users are less likely to use services from less established firms or newer entrants to a market—potentially leading to an uneven playing field and barriers to entry.[158]

C. Extending a Consumer Protection Framework

Consumers are at the heart of personal data issues ranging from security to privacy and ownership. American consumers "transmit their personal data on the internet at an exponentially higher rate than in the past."[159] Consumer information is increasingly collected and analyzed through a mixture of consumer-facing websites and implicit actors like data brokers and advertising companies.[160] There is momentum from consumer advocacy groups, ballot initiatives, and other lobbying efforts to improve the current regulatory landscape for personal data.[161] This section will consider consumers' issues and the efforts for change within a consumer protection framework.

The modern consumer protection framework of the Consumer Bill of Rights evolved from President Kennedy's 1962 speech, which outlined four basic consumer rights: the right to safety, the right to be informed, the right to choose, and the right

[155] Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LITERATURE 442, 456 (2016).

[156] *Americans and Privacy*, *supra* note 2 ("Among adults who say they ever read privacy policies before agreeing to their terms and conditions, only a minority—22%—say they read them all the way through before agreeing to their terms and conditions.").

[157] Acquisti, Taylor & Wagman, *supra* note 155.

[158] *See id.*

[159] MULLIGAN & LINEBAUGH, *supra* note 12, at 1.

[160] *Id.* at 1–2.

[161] *See, e.g.*, Wilson, *supra* note 9, at 2.

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

to be heard.[162] Historically, the FTC was the principal federal agency to enforce consumer protection regulations, but it was not the only such regulator.[163] Created in 1914, FTC, has two broad goals: "protect consumers by preventing fraud, deception and unfair business practices in the marketplace," and "to maintain competition by preventing anticompetitive business practices."[164] More recently, the CFPB has taken over regulating consumer protection of financial services and products and is also responsible for providing financial literacy and education to promote the informed financial consumer.[165]

Although the FTC and CFPB have overlapping jurisdiction in certain areas to ensure consumer protection online, there is insufficient coverage. The classic consumer protection principles should extend to include consumer personal data protection. Consumers overwhelmingly do not understand how their personal data is collected and stored.[166] Without comprehensive personal data legislation or a federal agency with wide enough jurisdiction to enforce all types of personal data regulation, consumers have ongoing privacy, security, and equity concerns.[167]

Applying consumer protection principles to personal data would inform consumers of their right to know and understand the collection of their data, the right to choose what happens with personal data, and the right to safety and privacy. Currently, there is no federal oversight requiring transparency to consumers' or security standards.[168] Given the pervasiveness of the digital economy, it is alarming

[162] President John F. Kennedy, Special Message to the Congress on Protecting Consumer Interest (Mar. 15, 1962), https://www.jfklibrary.org/asset-viewer/archives/JFKPOF/037/JFKPOF-037-028 [https://perma.cc/X7A4-6QGB].

[163] Spencer Weber Waller, Jillian G. Brady, R.J. Acosta, Jennifer Fair & Jacob Morse & Emily Binger, *Consumer Protection in the United States: An Overview*, EUR. J. OF CONSUMER LAW 1, 1 (2011) [hereinafter *Consumer Protection*].

[164] *Id.* at 3.

[165] *Building the CFPB: A Progress Report*, CFPB 1, 19–20 (July 18, 2011), https://files.consumerfinance.gov/f/2011/07/Report_BuildingTheCfpb1.pdf [https://perma.cc/X3VL-82S6] [hereinafter CFPB].

[166] *Americans and Privacy*, *supra* note 2.

[167] Kerry, *supra* note 7 ("Our current laws were designed to address collection and storage of structured data by government, business, and other organizations and are busting at the seams in a world where we are all connected and constantly sharing. It is time for a more comprehensive and ambitious approach. We need to think bigger, or we will continue to play a losing game.").

[168] *Id.*

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

that "consumers' data is collected, maintained, shared, and monetized in a way that consumers cannot see and cannot avoid."[169]

Companies that collect and profit from consumer data have a moral responsibility to the consumer and should be accountable for privacy and data security: "simply put, companies should own the risks they create for others."[170] However, the security and privacy risks for American consumers rest squarely on their shoulders,[171] and companies profit off of personal data collection and storage through targeted advertising, data brokers, and more.[172] Across various industries, "consumer data is the raw material driving the businesses of the largest digital platforms."[173] In addition to a lack of federal oversight, two mechanisms maintain this problematic relationship between consumers and data collectors: information asymmetry between the company and consumer, and uninformed consumer consent.[174]

Consumers face information asymmetries because there is little transparency about privacy or how their data is collected, used, or shared.[175] Without this information, consumers frequently make uninformed decisions about the quality and value of products and services.[176] The prevailing opt-in/opt-out consent model in the United States "forces consumers to make a decision on every website and online service they visit. This places an unreasonable—and unworkable—burden on individuals."[177] Companies remain unaccountable for the personal data they collect and store while also having the upper hand in the transaction with a consumer.[178] Moreover, there are findings that companies use deceptive online sales tactics, like

---

[169] Wilson, *supra* note 9, at 7.

[170] *Id.* at 12.

[171] Kerry, *supra* note 7 ("Our existing laws also rely heavily on notice and consent—the privacy notices and privacy policies that we encounter online or receive from credit card companies and medical providers, and the boxes we check or forms we sign.").

[172] *See, e.g.*, MULLIGAN & LINEBAUGH, *supra* note 12, at 5–6.

[173] Erika Douglas, *Monopolization Remedies and Data Privacy*, 24 VA. J.L. & TECH. 1, 43 (2020).

[174] Wilson, *supra* note 9, at 4–7.

[175] *Id.*

[176] *Id.* at 5–6.

[177] Brill, *supra* note 133.

[178] Kerry, *supra* note 7 ("[B]usinesses that use the data know far more than we do about what our data consists of and what their algorithms say about us.").

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

"misleading wording, take-it-or-leave-it choices, and hidden privacy options (often referred to as 'dark patterns') to nudge users towards desired outcomes."[179] The lack of transparency, and ultimately, the information asymmetry between the company and consumer enables such deceptive practices.[180]

Another effect of the information asymmetry is that consumers are rarely completely informed about privacy threats or other security consequences.[181] Online interactions often occur without the individuals' full informed consent,[182] introducing a "privacy paradox" in which there seems to be an "inconsistency between consumers' expressed preferences and their actual behavior when it comes to privacy."[183] Some argue that while consumers claim that they value privacy, it seems that they also easily give it away.[184] However, research indicates that the information asymmetry itself explains this privacy paradox.[185] Either consumers do not know enough to make informed decisions about their privacy preferences, or the information is too sparse or difficult to comprehend—in lengthy, small print terms and conditions agreements—to really understand their privacy rights.[186] The latter phenomenon is known as "privacy resignation," where "consumers chose to forego expending significant time and energy to protect their online information."[187]

[179] Wilson, *supra* note 9, at 6.

[180] *Id.* at 6–7.

[181] *See id.* at 5–6.

[182] *Id.* at 5.

[183] *Id.* at 6.

[184] *See id.*

[185] *Id.*

[186] Kerry, *supra* note 7 ("In a constant stream of online interactions, especially on the small screens that now account for the majority of usage, it is unrealistic to read through privacy policies. And people simply don't.").

[187] Wilson, *supra* note 9, at 6.

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

III. PROPOSED LEGISLATION TO PROVIDE CONSUMER DATA RIGHTS AND PROTECTIONS, AND CREATE AN INDEPENDENT CONSUMER DATA PRIVACY AND PROTECTION AGENCY

It has been nearly twenty years since Congress enacted meaningful privacy legislation.[188] Technology is outpacing the law, and consumers are paying the price. While most modern countries have updated their laws to reflect changes in technology and the digital economy, "U.S. privacy law is considered out of date and ineffective."[189] This proposal will address personal data rights, privacy, and security by formally extending a consumer protection framework to data privacy. The proposed federal legislation is two-fold: first, a baseline, comprehensive regulatory scheme referred to as CDPPA, and second, the creation of an independent agency called the CDPPB.

Section III.A explains why federal legislation is realistic and pragmatic. There is political capital and willingness to legislate from both sides of the aisle and in both chambers of Congress.[190] The current federal laws related to data privacy are a series of distinct laws and regulations enforced by various agencies with different jurisdictions.[191] Perhaps due to this inefficiency, over two dozen states have begun independently legislating on the issue, and three states have already implemented comprehensive consumer data privacy and protection laws.[192] Moreover, there is palpable energy from outside of government supporting new legislation: businesspeople, academics, and consumer advocates have introduced a range of creative solutions to address personal data issues.[193]

---

[188] EPIC, *supra* note 135.

[189] *Id.*

[190] *See id.* at 1.

[191] O'Connor, *supra* note 32.

[192] Lively, *supra* note 25.

[193] *See, e.g.*, Andrew Yang, *Op Ed: Make Tech Companies Pay You For Your Data*, L.A. TIMES: OPINION (June 23, 2020), https://www.latimes.com/opinion/story/2020-06-23/andrew-yang-data-dividend-tech-privacy [https://perma.cc/F5ZL-KLKP] (arguing in support of personal data dividends); Jessica Leber, *MIT Wants You to Own Your Own Data, Not Give It Away*, FAST CO. (July 23, 2014), https://www.fastcompany.com/3033414/mit-wants-you-to-own-your-own-data-not-give-it-away [https://perma.cc/CAA5-P7C7] (describing a mechanism for data ownership); Vincent Mitchell, *What if the Companies That Profit From Your Data Had to Pay You?*, THE CONVERSATION (July 29, 2018), https://theconversation.com/what-if-the-companies-that-profit-from-your-data-had-to-pay-you-100380 [https://perma.cc/LG35-SD94] (discussing value and fairness of personal data collection).

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

Sections III.B and III.C explore the two main goals of the proposed, comprehensive CDPPA: the creation of the CDPPB and the extension of a consumer protection framework within the CDPPA. The CDPPB would act as a consumer protection agency for all issues related to consumer data. It would consolidate or share jurisdiction with the various federal agencies that currently enforce personal data privacy regulations. Centralizing the existing data security and privacy regulations would make their enforcement leaner and more efficient. It would also make the CDPPB well-placed to enact new regulations. Structurally, the CDPPB would share qualities similar to the FTC and CFPB in their consumer protection efforts and organizational aspects.

Within the comprehensive CDPPA, there would be a reciprocal scheme for consumers and entities that store, collect, or sell consumer data. CDPPA would provide consumers with basic individual rights to access, control, and delete their personal data. Under CDPPA, data controllers would be obligated to practice transparency, data minimization and deletion, accountability, and security. Like the FCRA, CDPPA would serve as a baseline regulatory scheme that will not preempt state laws unless there is a regulatory inconsistency. With its broad, straightforward application to all types of personal data and sectors that involve consumer data, CDPPA would ease compliance and increase competition within the U.S. market and abroad.

A. Reform is Realistic

There is a growing concern in the United States for its inadequate legal protection for consumer data.[194] Specifically, there is a call for a comprehensive data privacy and protection law.[195] The current information- and sector-specific regulatory scheme, enforced by many federal agencies with overlapping jurisdiction, is inefficient and ineffective. A 2018 poll by Pew Research found that "two-thirds of Americans said current laws are not good enough in protecting people's privacy, and 64% support more regulation of advertisers."[196]

[194] EPIC, *supra* note 135, at 1.

[195] Wilson, *supra* note 9, at 8.

[196] EPIC, *supra* note 135, at 2.

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

As a response to public opinion and in the face of sophisticated regulations abroad, many in Congress are pushing for comprehensive privacy protection,[197] and U.S. Representatives and Senators from both parties have introduced legislation in consecutive sessions of Congress.[198] Although there seems to be a consensus that the "federal government should assume a larger role in data protection policy,"[199] there is a wide variation of ideas to address the issue legislatively.[200] In the 116th Congress, Senator Marco Rubio introduced the American Data Dissemination Act, which seeks to increase privacy rights and preempt stronger state laws.[201] Senators Amy Klobuchar (D-MN) and John Kennedy (R-LA) also introduced a bipartisan bill called the Social Media Protection and Consumer Rights Act.[202] It has bipartisan cosponsors and aims to provide consumers a right to access their data and improve the "notice and consent" process to require affirmative consent in the event that a change would impact the user's privacy settings.[203] Other leaders on this issue are Senators Mark Warner (D-VA), Josh Hawley (R-MO) and Kirsten Gillibrand (D-NY).[204]

In the House of Representatives, Representatives Anna Eshoo (D-CA) and Zoe Lofgren (D-CA) introduced the Online Privacy Act.[205] Their legislation would establish an independent data protection agency and focus on antidiscrimination in automated decision-making.[206] Similar to CDPPA, the Online Privacy Act would grant rights to individuals over their data while also enacting clear obligations for data controllers.[207] Even though there is variation in legislators' proposed

[197] *See, e.g.*, MULLIGAN & LINEBAUGH, *supra* note 12, at 6; JOHNATHAN M. GAFFNEY, CONG. RSCH. SERV., LSB10441, WATCHING THE WATCHERS: A COMPARISON OF PRIVACY BILLS IN THE 116TH CONGRESS (2020).

[198] EPIC, *supra* note 135, at 1.

[199] *Id.* at 7.

[200] *See generally id.* at 12–16 (listing proposed and related legislation).

[201] *Id.* at 8.

[202] *Id.* at 5–6.

[203] *Id.*

[204] *Id.* at 12–16.

[205] *Id.* at 5.

[206] *Id.*

[207] *Id.*

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

approaches, there is clearly bipartisan momentum to enact new federal legislation for consumer data protection and privacy.

Creative ideas and approaches to protect consumer data are also forming outside the federal government and perhaps even inspired by its inaction. For example, Andrew Yang founded the Data Dividend Project after his presidential run.[208] His goal is to create a union to bargain collectively as an authorized agent for individuals' data rights.[209] Through this process, individual users could have a seat at the table with large technology companies ("big tech") to negotiate transparency, personal data rights, and potential compensation.[210] Relatedly, there is a movement for users to be paid for their personal data proportionately to what it is worth for big tech or data brokers.[211] There is also a movement to consider personal data property, such that ownership rights and licensing would attach at its use.[212] These ideas reveal broad momentum and support for change, and their chorus increases pressure on legislators to act.[213]

B. Consumer Data Privacy and Protection Bureau

The United States is one of the only democratic countries in the world without an independent federal data protection agency.[214] Currently, multiple agencies enforce various privacy laws with overlapping jurisdictions.[215] This situation leads to inconsistent enforcement and complicated compliance structures.[216] Moreover, the current security mechanisms are spread over various agencies, and "many now believe that the failure to establish a data protection agency in the U.S. has

[208] *Take Control of Your Data*, DATA DIVIDEND PROJECT, https://www.datadividendproject.com/ [https://perma.cc/Z66M-YS4M].

[209] *Id.*

[210] *Id.*

[211] Mitchell, *supra* note 193.

[212] *See* Leber, *supra* note 193.

[213] *See* Hartzog & Richards, *supra* note 6, at 1690 ("The modern data industrial complex is facing a tidal wave of public support for a privacy law revolution.").

[214] EPIC, *supra* note 135, at 3.

[215] O'Connor, *supra* note 32.

[216] Kerry, *supra* note 7 ("As the data universe keeps expanding, more and more of it falls outside the various specific laws on the books.").

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

contributed to the growing incidents of data breach and identity theft."[217] This section will outline the goals and functions of the CDPPB and the ways in which it would be similar to the FTC and CFPB.

1. Purpose and Goals of CDPPB

The purpose of the CDPPB is to provide a centralized agency dedicated to consumer data privacy and protection. Much like the principles of the FTC,[218] the CDPPB would protect consumers by increasing transparency, enforcing privacy and security regulations, and preventing deceptive or unfair personal data practices. Simultaneously, the CDPPB would maintain competition by improving compliance and enforcement, lowering barriers so that competitors can realistically enter the market. In doing so, the CDPPB would extend the consumer protection framework to facilitate a reasonably informed consumer, empowered to make informed decisions about their personal data and provide fully informed consent when sharing their personal data.

A major initiative of the CDPPB would be negotiating to consolidate jurisdiction from various agencies. The federal agencies that currently have jurisdiction over varying data privacy and protection issues include the Department of Commerce, the Securities and Exchange Commission, the Federal Communications Commission, the Department of Health and Human Services, the Consumer Finance Protection Bureau, and the Federal Trade Commission.[219] Because personal data issues can span information or sector-specific regulations, enforcement and compliance are currently very difficult and expensive.[220] Although it may be pertinent to share jurisdiction with other agencies on certain issues like HIPAA, centralizing most of the enforcement of existing personal data privacy and protection laws would make governance and enforcement leaner and more efficient. It could also decrease compliance costs for companies by making regulations simpler and centralized.

The CDPPB framework would be similar to the CFPB in a few ways, partly because of comparable information asymmetries that exist with personal data and financial products and services. The CFPB has tried to address the information

[217] EPIC, *supra* note 135, at 3.

[218] *Consumer Protection*, *supra* note 163, at 3.

[219] MULLIGAN & LINEBAUGH, *supra* note 12, at 1.

[220] Faitelson, *supra* note 140 (arguing that a comprehensive data privacy law would lower compliance costs).

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

asymmetry in the financial sector by making it easier for consumers to understand financial services and products enough to make informed financial decisions.[221] Generally, "a fair, efficient, and transparent market depends on consumers' ability to compare the costs, benefits, and risks of different products effectively and to use that information to choose the product that is best for them."[222] The CFPB also invests in consumer financial literacy and education to encourage reasonably informed financial consumers.[223] Correspondingly, the CDPPB will emphasize personal data literacy and education to decrease information asymmetries. By centralizing enforcement, easing compliance, and promoting transparency, the CDPPB would make the digital economy, fueled by personal data, fairer and more competitive.

The CDPPB would equip consumers with the ability to make informed decisions about their personal data that is in their control. However, the onus to protect the privacy and security of personal data cannot realistically rest on the consumers' shoulders. Therefore, the CDPPB would consistently enforce existing security and privacy regulations for companies that collect, store, and sell personal data. It would also serve as the dedicated agency to implement future federal regulations for the privacy and protection of personal data.

2. Structure and Funding

The leadership structure of the CDPPB would be similar to the FTC with five commissioners nominated by the President and confirmed by the Senate, with no more than three Commissioners from the same political party.[224] Given the bipartisan support of consumer data protection, Congress would likely support commissioners that plan to further their goals accordingly.[225] Much like the CFPB,[226] the CDPPB would be subject to congressional oversight and report to Congress twice yearly to provide testimony. Additionally, it would be subject to the notice and comment

[221] CFPB, *supra* note 165.

[222] *Id.*

[223] *Id.* at 19–20.

[224] *Consumer Protection*, *supra* note 163, at 2–3. *But see* Selia Law v. CFPB, 140 S. Ct. 2183, 2210-11 (2020) (holding single director structure unconstitutional).

[225] EPIC, *supra* note 135 (bipartisan momentum for data privacy regulation).

[226] CFPB, *supra* note 165, at 32.

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

requirements of rulemaking under the Administrative Procedure Act so that non-governmental actors could also participate in forming regulation.[227]

Conceptually, the funding for the new agency would come from the private industry. Personal data is a resource fueling the digital economy. Some believe that the enormous profits from personal data should be taxed and redistributed in the form of a dividend.[228] This structure would theoretically function similarly to how the State of Alaska taxes oil companies drilling in the state and uses that tax revenue to pay its citizens a dividend each year.[229] However, instead of providing consumers a dividend for the value of their data, the tax would fund the CDPPB to facilitate consumer protection and oversight. Big technology companies, as well as other organizations that profit from personal data would be taxed proportionally to their profit from utilizing or selling consumer data. This tax revenue would ideally fund most, if not all, of the CDPPB. Until that complicated mechanism is developed and implemented, congressional appropriations would fund the CDPPB .

3. An Independent Agency

A new, independent agency for consumer data protection is needed because the FTC, CFPB, and other agencies have failed to facilitate consumer data protection. While the FTC "held itself out as the privacy agency for the U.S. . . . over time it became clear that the FTC lacked the authority, competence, and political will to safeguard American consumers."[230] There has been little actual change in the business practices and privacy policies of technology giants like Google and Microsoft despite the significant judgments and fines placed against them by these various regulatory agencies.[231]

For example, the 2019 FTC settlement with Facebook over its privacy practices resulted in a $5 billion penalty.[232] The investigation was triggered by "allegations

[227] 5 U.S.C. § 553.

[228] *See* Yang, *supra* note 193.

[229] *State Revenue*, ALASKA OIL AND GAS ASS'N, https://www.aoga.org/state-revenue/ [https://perma.cc/QL2S-D6PG].

[230] EPIC, *supra* note 135, at 2.

[231] *See, e.g.*, David Shepardson, *Facebook to Pay Record $5 Billion U.S. Fine Over Privacy; Faces Antitrust Probe*, REUTERS (July 24, 2019, 8:35 AM), https://www.reuters.com/article/us-facebook-ftc/facebook-to-pay-record-5-billion-us-fine-over-privacy-faces-antitrust-probe-idUSKCN1UJ1L9 [https://perma.cc/77PZ-FGMQ] (criticizing the FTC settlement with Facebook for not being impactful enough).

[232] *Id.*

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

that Facebook violated a 2012 consent decree by inappropriately sharing information belonging to 87 million users with the now-defunct British political consulting firm Cambridge Analytica."[233] A well-known client of the firm was Donald Trump's 2016 presidential campaign.[234] The FTC settlement instructed Facebook to create an independent privacy committee, but there was arguably no legal obligation for Facebook to take accountability for its data-sharing aside from paying the hefty fine.[235] Furthermore, the settlement did nothing to address the underlying privacy issues at Facebook that led to the lawsuit. There was bipartisan outrage from Republican senators like Josh Hawley and Democratic FTC Commissioner Slaughter that the "FTC failed 'to impose substantive restrictions on Facebook's collection of use and data from or about users.'"[236]

The only other agency with similar jurisdiction over consumer data is the CFPB.[237] Although it technically has the ability to expand its scope of jurisdiction, the CFPB has been reluctant to regulate consumer privacy outside of financial products and services.[238]

4. Alternate Option: Cabinet-Level Office to Unify Jurisdiction

Although a new, independent agency is preferable, there is an alternate option to accomplish the same goals if that the political climate would not support the creation of the CDPPB. This position, the Director of Privacy and Protection ("DPP"), would be modeled after the Director of National Intelligence ("DNI"). The Office of the DNI unifies the intelligence community, which is composed of eighteen unique organizations.[239] The Senate-confirmed position and office were created in 2004 as part of the Intelligence Reform and Terrorism Prevention Act.[240] In the same

[233] EPIC, *supra* note 135, at 2.

[234] Shepardson, *supra* note 231 ("The consultancy's clients included President Donald Trump's 2016 election campaign.").

[235] *Id.*

[236] *Id.*

[237] *Consumer Protection*, *supra* note 163, at 15.

[238] *Id.* at 113.

[239] *What We Do: Members of the IC*, OFF. OF THE DIR. OF NAT'L INTEL., https://www.dni.gov/index.php/what-we-do/members-of-the-ic [https://perma.cc/8J2Q-29PC].

[240] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3643 (2004).

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

way that establishing the DNI created a coalition of intelligence agencies to more efficiently share information,[241] the DPP would consolidate efforts across agencies to enforce various privacy laws. In that way, the DPP could effectively and efficiently point the various agencies that regulate data privacy in the same direction, moving forward cohesively. Passing the CDPPA would create the office of DPP.

C. Consumer Data Privacy and Protection Act

The CDPPA would grant the CDPPB authority to regulate consumer data privacy and protection. Additionally, it would have two reciprocal aims to enable consumer data protection: providing basic individual rights to the consumer while also regulating obligations for companies that store, collect, and sell personal data. The CDPPB would consistently and fairly enforce the CDPPA. The rights to access, control, and delete personal data would give individuals meaningful insight and control over their data.[242] "Notice and consent" for personal data privacy and security purposes is entirely unhelpful to consumers. It "allows companies to diminish the rights of consumers, and use personal data for purposes to benefit the company but not the individual."[243] Only a very small number of users read these notice and consent policies.[244] By providing consumers with more control and information about where and how their personal data is collected, the CDPPA would enable reasonably informed consumers to be "empowered to meaningfully express privacy preferences."[245]

Under the CDPPA, the burden for assuring consumer data privacy and protection would not rest solely with the informed consumer. The law will regulate data controller obligations—transparency, data minimization and deletion, increased security, and confidentiality practices. These straightforward obligations are not sector- or information-specific. Moreover, they would decrease the information asymmetry between consumers and companies that collect and store personal data. Enforced by a single agency, the CDPPB, the data controller obligations would increase accountability and compliance.

---

[241] Gordon Liu, *The Role of the Director of National Intelligence as 'Head' of the Intelligence Community*, FOREIGN POL'Y RSCH. INST. (Sept. 13, 2019), https://www.fpri.org/article/2019/09/the-role-of-the-director-of-national-intelligence-as-head-of-the-intelligence-community/ [https://perma.cc/C9JZ-RT9P].

[242] EPIC, *supra* note 135, at 4.

[243] *Id.*

[244] RFC, *supra* note 14.

[245] *Id.*

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

While the CDPPA has broad application, it would serve as a baseline by setting a minimum consumer data privacy and protection standard. Moreover, in a similar manner to the FCRA,[246] it would not preempt stronger state laws, many of which are currently in the throes of the legislative process. This would allow for "individual states to develop and innovate approaches to privacy protection."[247]

Finally, a comprehensive data privacy and protection law would ease international compliance and benefit international trade. The United States is a global outlier.[248] Other advanced economies like Canada, Israel, and Japan have adopted comprehensive privacy regulations similar to and compatible with the European Union's GDPR.[249] Unfortunately, this has put "U.S. companies at a disadvantage globally as emerging economies adopt simpler, and often more EU-style, comprehensive approaches."[250] International compliance is burdensome and expensive for U.S. companies dealing with personal data.[251] Moreover, the recent suspension of the U.S.-European Union Data Privacy Shield data sharing agreement due to insufficient data-privacy protections in the United States will likely make GDPR compliance and transatlantic trade more complicated and expensive.

The CDPPB and the CDPPA would equip the U.S. government with the tools to approach future data privacy and protection issues. From big tech and social media, to the breakdown of the U.S.-European Union Data Privacy Shield agreement and the impending 5G framework, there is urgent need for federal reform.

CONCLUSION

Consumer data regulation is realistic, necessary, and timely. The volume of American consumer data will increase as social media, digital healthcare, and other online services continue to pervade everyday life. Congress should act to address the uneven scheme of privacy and personal data regulations. Specifically, as fundamental consumer protection principles continue to evolve in America, Congress should pass legislation to extend the consumer protection framework to

[246] 15 U.S.C. § 1681t.

[247] EPIC, *supra* note 135, at 5.

[248] O'Connor, *supra* note 32.

[249] *Id.*

[250] *Id.*

[251] *How to Prepare for Global Data Compliance*, ERNST & YOUNG (May 4, 2021), https://www.ey.com/en_us/consulting/how-to-prepare-for-global-data-compliance ("Now, over 100 jurisdictions—countries, states and cities—are enacting their own data privacy laws. . . . It is like a second set of tax codes—high costs, high risk, complex execution, and where absolute non-compliance is not an option.").

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu

include consumer data. In addition to ensuring privacy and protection for consumer data, it would incentivize a competitive market to enable reasonably informed users to insightfully compare products and make informed decisions about their privacy preferences online.

The proposed CDPPA would create an independent agency, the CDPPB, to consolidate jurisdiction of existing privacy laws and enforce new laws, like the CDPPA itself. It is the best step Congress can take to ensure consumer safety and market competition as the digital and global economy continues to expand.

ISSN 1942-8405 (online) ● DOI 10.5195/lawreview.2022.839
http://lawreview.law.pitt.edu