PRIVACY PURGATORY: WHY THE UNITED STATES NEEDS A COMPREHENSIVE FEDERAL DATA PRIVACY LAW

Emily Stackhouse Taetzsch[*]

CONTENTS

© 2024 Emily Stackhouse Taetzsch. Individuals and educational institutions may reproduce and distribute copies of this Article in any format at or below cost, for educational purposes, so long as each copy identifies the author, provides a citation to the *Journal of Legislation*, and includes this provision and proper notice of copyright ownership.

[*] J.D. Candidate, University of Notre Dame Law School, 2024; B.A. in Philosophy with English literature integration, Wheaton College, 2018. Many thanks to Hon. Margaret A. Ryan of Notre Dame Law School, Jena M. Valdetero of Greenberg Traurig, LLP, and the editors of the *Journal of Legislation* for their guidance with this Note.

INTRODUCTION

When asked how they felt about the state of data privacy and its future, a sample of Americans surveyed by the Pew Research Center in 2016 expressed feelings of general powerlessness.[1] Their answers ranged from "hopeless" and "resigned" to, vaguely, "I don't think things are hopeless, some genius will figure out how to get around all this."[2] By "all this," they referred to the ever-growing volumes of data being aggregated by and exchanged between private companies for numerous purposes,[3] including website enhancement,[4] precision marketing,[5] and the generation of profit from user data.[6] By 2019, about six in ten American adults did not think it possible to live each day without their data being collected by companies or the government.[7] By 2023, a majority of Americans now say they are "concerned, lack control and have a limited understanding about how the data collected about them is used."[8]

While one popular argument in favor of such data collection is that it enables companies to provide free or reduced-price services,[9] widespread and rapidly evolving methods of data collection combined with myriad loopholes in the legal regime have created something of a "wild west" environment in the world of data privacy.[10] There is no federal law dictating when a company must notify consumers that it is selling or sharing their data—in fact, there is no comprehensive

---

1 Lee Rainie & Maeve Duggan, *Privacy and Information Sharing*, PEW RSCH. CTR. (Jan. 14, 2016), https://www.pewresearch.org/internet/2016/01/14/privacy-and-information-sharing [https://perma.cc/L8HB-JQVU].

2 *Id.*

3 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/D2MW-6PU2].

4 *What is a Cookie? How it Works and Ways to Stay Safe*, KASPERSKY: RES. CTR., https://www.kaspersky.com/resource-center/definitions/cookies [https://perma.cc/6FWA-SG8P] (last visited Oct. 8, 2022) [hereinafter *What is a Cookie?*].

5 *See* Max Eddy, *How Companies Turn Your Data Into Money*, PC MAG. (Oct. 10, 2018), https://www.pcmag.com/news/how-companies-turn-your-data-into-money [https://perma.cc/8AHT-HQ9Y].

6 *Id.*; For a general overview of the regulations and issues concerning the practices of cookies and privacy as elaborated further in this Note, see *Cookie Benchmark Study*, DELOITTE RISK ADVISORY B.V. (Apr. 2020) (U.K.), https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-risk-cookie-benchmark-study.pdf [https://perma.cc/FK9K-GUJN].

7 Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling 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/SLP4-ECKN].

8 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/UZW7-QRRW].

9 Eddy, *supra* note 5; Kassandra Polanco, Note, *Trimming the Fat: The GDPR as a Model for Cleaning up Our Data Usage*, 36 TOURO L. REV. 603, 603 (2020); Louise Matsakis, *The WIRED Guide to Your Personal Data (and Who Is Using It)*, WIRED MAG. (Feb. 15, 2019, 7:00 AM), https://www.wired.com/story/wired-guide-personal-data-collection/ [https://perma.cc/MZZ4-5DLL].

10 Casey Rentmeester, *Kant's Ethics in the Age of Online Surveillance: An Appeal to Autonomy*, *in* EVERYDAY LIFE IN THE CULTURE OF SURVEILLANCE 200 (Lars Samuelsson et al. eds., 2023).

federal privacy law at all.[11] Outside the federal realm, minimal laws exist requiring companies to notify users of precisely how their data is being used, but meanwhile the world of data brokerage has grown exponentially over the past decade.[12] For data breach notification, the problem is inverted. Every state has its own requirement dictating the number of consumers and, more obscurely, the type of data that should trigger the dispersion of a notice, resulting in a complex maze of requirements companies must adhere to on top of the many stressors of a breach.[13]

While it is no simple matter to vindicate privacy rights as a "data subject"[14] anywhere in the world, this is particularly true in the United States, where lack of data privacy regulation provides companies all kinds of opportunities to misuse people's data. For example, there is a now-common practice, that of using "dark patterns," for obtaining user consent, in which companies present information in a way that subtly coaxes users toward a particular response.[15] Companies use the strategy to design the notifications that ask users to give consent for "cookies."[16] Dark patterns make the cookie-accepting process "as opaque, unpractical and time-consuming as possible—just to make you click 'accept.'"[17] In 2021, the Federal Trade Commission—the executive body in charge of enforcing data privacy regulations—reiterated its commitment to treat dark patterns as unfair

---

[11] Klosowski, *supra* note 3.

[12] *See generally* Kalev Leetaru, *What Does it Mean for Social Media Platforms to "Sell" Our Data?*, FORBES (Dec. 15, 2018, 3:56 PM), https://www.forbes.com/sites/kalevleetaru/2018/12/15/what-does-it-mean-for-social-media-platforms-to-sell-our-data/?sh=4d86a602d6c4 [https://perma.cc/XVU5-9TV2] (illuminating the expansive industry that is data brokerage).

[13] *See* Security Breach Notification Chart, PERKINS COIE, https://www.perkinscoie.com/images/content/2/4/246420/Security-Breach-Notification-Law-Chart-Sept-2021.pdf (Sept. 2021) [https://perma.cc/JLU4-PS62]. The variation in type of data that triggers notification can be problematic when residents of many states are affected. For example, some states count passwords as personal information (often in combination with a financial account number). If a breach of only usernames and passwords affected residents of all fifty states, a company must gauge the wisdom of notifying residents of all states, including those that do not require notification in such a case.

[14] 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 (General Data Protection Regulation), art. 4(1), 2016 O.J. (L 119) 1 (EC) [hereinafter GDPR] (defining data subject as "an identified or identifiable natural person.").

[15] *See* Isha Marathe, *Proposed CPRA Rules Show 'Dark Patterns' a Growing Focus for State Privacy Laws*, LEGALTECH NEWS (June 13, 2022, 10:30 AM), https://www.law.com/legaltechnews/2022/06/13/proposed-cpra-rules-show-dark-patterns-a-growing-focus-for-state-privacy-laws/ [https://perma.cc/LS7K-5VFV].

[16] "Cookies" are those infamous files with small pieces of data that can be deposited onto a user's computer in response to a single click. They allow companies to track a user's online presence, collect their data, and sell it. For more information, see *What Is a Cookie?*, *supra* note 4.

[17] *Most Cookie Banners Are Annoying and Deceptive. This Is Not Consent.*, PRIVACY INT'L (May 21, 2019), https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent [https://perma.cc/5MH8-2GYU] [hereinafter *Most Cookie Banners Are Annoying*]; *Cookie Benchmark Study*, *supra* note 6, at 6 (finding that 43% of all websites investigated "nudged" users to provide consent for all cookies, including by graphically designing cookie notifications to indicate that users should accept).

business practices in violation of the FTC Act.[18] Despite its admirable stance, the agency released a report in 2022 showing that the use of dark patterns is actually increasing.[19] Additionally, the lack of comprehensive data privacy legislation in the United States means that companies can safely interpret a user's consent to the placement of cookies by third parties like Meta or Google on one website as "global consent,"—or an agreement to be tracked across the web by such third parties for advertising purposes.[20] Where consent management platforms are used,[21] consent to third party cookies on one site with a global consent request may be interpreted as consent on all other sites with similar requests.[22] In short, "this means that users accept tracking on hundreds of websites in a single click, often obtained out of users' frustration."[23] *The New York Times* called this understandable frustration "notification fatigue."[24] There are a few meager ways data subjects can take back a modicum of control: apps have been made to block the ever-prevalent cookie notices, though some of them "block" by automatically providing consent.[25]

Many Americans say they wish they could do more to protect their privacy but do not know how to do so,[26] and technology experts predict few citizens will have the "energy or resources to protect themselves from 'dataveillance' in the coming years."[27] A hard look at the reality of being a data subject in the United States makes it clear that there is a real need for protection via regulation.

Just as the life of a data subject can be burdensome, organizations that process data face difficulties too.[28] Between January 2020 and December 2023,

---

18 Press Release, Fed. Trade Comm'n, FTC to Ramp Up Enforcement against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions, (Oct. 29, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap-consumers-subscriptions [https://perma.cc/NDF8-7KMC]; Federal Trade Commission Act, ch. 311, §1, 38 Stat. 717 (1914) (codified as amended at 15 U.S.C. §§ 41–58, 57(a) (2018)).

19 *See* FTC REPORT SHOWS RISE IN SOPHISTICATED DARK PATTERNS DESIGNED TO TRICK OR TRAP CONSUMERS, FED. TRADE COMM'N (Sept. 15, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers [https://perma.cc/2TMK-3H3R].

20 *See Most Cookie Banners Are Annoying*, *supra* note 17.

21 *See* Kaya Ismail, *What is a Consent Management Platform?*, CMSWIRE (Mar. 14, 2019), https://www.cmswire.com/information-management/what-is-a-consent-management-platform/ [https://perma.cc/4CYL-7BV4].

22 *See Most Cookie Banners Are Annoying*, *supra* note 17.

23 *Id.*

24 Klosowski, *supra* note 3.

25 *See* Nelson Aguilar, *How to Block Those Annoying Cookie Consent Notices from Appearing on Websites in Safari*, GADGET HACKS (Jan. 28, 2021, 3:52 PM), at 1–2, https://ios.gadgethacks.com/how-to/block-those-annoying-cookie-consent-notices-from-appearing-websites-safari-0384278/ [https://perma.cc/C4M7-FQ9S].

26 *See* PEW RSCH. CTR., *The State of Privacy in Post-Snowden America*, (Sept. 21, 2016), https://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ [https://perma.cc/FM2T-BXH6].

27 *Id.*

28 *See* GDPR, *supra* note 14, art. 4(2) ("'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage . . .").

five different comprehensive state privacy laws went into effect, all with slightly different requirements for the treatment of data and all with substantial impacts on business compliance.[29] Similar laws from other states are set to take effect after 2023.[30] Organizations will need to assess whether the laws apply to them and subsequently determine compliance measures. Remaining in compliance with the patchwork of state and federal laws may be difficult for a new company but could be extremely resource-draining for established businesses. Even for businesses that can afford to hire an outside firm to ensure compliance, the process of establishing and maintaining compliance is highly complex and can be cost-intensive.[31] Some law firms and other companies have published guidance on how to reach compliance with the new comprehensive laws; the process involves an extremely detailed review of how all data is used and secured, from whom it is collected, and to whom it is sent, as applied to each state in question.[32] Having one primary set of rules would provide clarity and stability to the legal landscape, giving companies a better chance of complying and decreasing the opportunity for error in handling individuals' data. Despite these benefits, the realization of a federal privacy law remains in a purgatory-like state of inertia even as Americans' sense of powerlessness grows.

This Note presents an overview of the leading models of privacy regulation most relevant for the United States: beginning with the General Data Protection Regulation (GDPR) and its data protection principles, moving to the current patchwork of federal and state laws in the United States, and analyzing a proposed comprehensive federal privacy law. Next, it establishes why the United States ought to adopt the model of a comprehensive federal law rather than leaving states to create an ever-increasing web of regulation. Finally, it briefly engages with arguments surrounding privacy regulation and First Amendment free speech concerns, for any federal law must clear constitutional hurdles.

I. OVERVIEW OF PRIVACY LAW IN UNITED STATES AND EUROPE

A. Europe's Omnibus Approach: The General Data Protection Regulation

---

[29] *See Key Dates from US Comprehensive State Privacy Laws*, INT'L ASS'N OF PRIV. PROS., https://iapp.org/media/pdf/resource_center/key_dates_us_comprehensive_state_privacy_laws.pdf [https://perma.cc/9S92-25RP] (Sept. 2022).

[30] For a compilation of up-to-date coverage of national legislation concerning individual data privacy rights, see Andrew Folks, *US State Privacy Legislation Tracker*, IAPP, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/#enacted-laws [https://perma.cc/SL5F-ZVUF] (Oct. 20, 2023).

[31] *See Cookie Benchmark Study*, *supra* note 6, at 23–25. Of note, these comprehensive state laws largely apply only to companies that collect large amounts of data or derive a threshold percentage of revenue from data sales. *See e.g.*, COLO. REV. STAT. § 6-1-1304 (2022).

[32] *See, e.g.*, Gretchen A. Ramos & Michael Wertheim, *Is it Secret, Is it Safe? What Employers Need to Know About the California Privacy Rights Act*, GREENBERG TRAURIG: DATA PRIV. DISH (Aug. 18, 2021), https://www.gtlaw-dataprivacydish.com/2021/08/is-it-secret-is-it-safe-what-employers-need-to-know-about-the-california-privacy-rights-act/ [https://perma.cc/HAM9-H7M9]; Abi Tyas Tunggal, *9 Ways to Prevent Third-Party Data Breaches in 2022*, UPGUARD (Aug. 8, 2022), https://www.upguard.com/blog/prevent-third-party-data-breaches [https://perma.cc/DXH9-9MQN].

As the capacity for widespread collection of data has ballooned, Europe has consistently set the universal tone for the vindication of individual data privacy rights. The right to privacy was recognized worldwide in the United Nations' Universal Declaration of Human Rights of 1948,[33] reinforced in 1950 by the European Convention on Human Rights.[34] The world's first comprehensive data privacy statute was passed in Germany in 1970,[35] and the GDPR (passed in 2016)[36] and its predecessor statutes have created a legislative domino effect across the globe. A brief look at European history illuminates why it is a world leader in this area: in Nazi Germany, personal data was aggregated and weaponized for horrific purposes.[37] In the 1930s, census workers gathered data from citizens that they then used to identify Jews and other groups the government wished to destroy.[38] When Germany was partitioned into East and West after World War II, the East German secret police continued to use the data to intimidate and control citizens.[39] In 1970, the West German state of Hesse passed the world's inaugural comprehensive privacy law,[40] followed by Germany's 1977 Federal Data Protection Act.[41] Upon reunification, all German citizens were able to claim the rights within the federal law, which included the right of "self-determination over personal data."[42]

The GDPR, Europe's current trend-setting data privacy regulation, followed the European Union's 1995 Data Protection Directive, which was less comprehensive and allowed individual nations to decide how to achieve the listed goals.[43] At its core, the GDPR is centered on foundational principles of data privacy and its requirements are oriented toward enforcing those principles, which include "lawfulness, fairness, and transparency; purpose limitation; data minimiza-

---

[33] *See* G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 12 (Dec. 10, 1948).

[34] *See* Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4 1950, E.T.S. No. 5, 213 U.N.T.S. 221.

[35] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 7 (6th ed. 2022); Datenschutzgesetz [Data Protection Act], Oct. 7, 1970, GESETZ-UND VERORDNUNGSBLATT [GVBL.] II 300-10 (Hesse) (Ger.).

[36] GDPR, *supra* note 14.

[37] Olivia B. Waxman, *The GDPR Is Just the Latest Example of Europe's Caution on Privacy Rights. That Outlook Has a Disturbing History*, TIME (May 24, 2018, 7:12 PM), https://time.com/5290043/nazi-history-eu-data-privacy-gdpr/ [https://perma.cc/45DX-U5MB].

[38] *Id.*

[39] *Id.*

[40] *See* Datenschutzgesetz [Data Protection Act], Oct. 7, 1970, GESETZ-UND VERORDNUNGSBLATT [GVBL.] II 300-10 (Hesse) (Ger.).

[41] Bundesdatenschutzgesetz [Federal Data Protection Act], Feb. 1, 1977, BGBl I at 201 (Ger.); Waxman, *supra* note 37.

[42] Waxman, *supra* note 37.

[43] Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, repealed by GDPR, *supra* note 14, art. 94; Stefan Ducich & Jordan L. Fischer, *The General Data Protection Regulation: What U.S.-Based Companies Need to Know*, 74 BUS. LAW. 205, 206 (2019).

tion; accuracy; storage limitation; and integrity and confidentiality."[44] The law divides those who handle data into controllers[45] and processors,[46] with the main difference being that controllers, appropriately, have full control over how data is used and why, shouldering the burden of legal responsibility by default.[47] The data in question, or "personal data," is broadly defined to include "'any information relating to an identified or identifiable natural person,' whether directly or indirectly."[48] Among other things, the GDPR requires controllers to notify data subjects of their data collection and processing activities;[49] provide certain rights to access;[50] delete,[51] correct,[52] and object to the processing of data subjects' personal data;[53] implement data security measures;[54] and report data breaches.[55] Controllers must bind organizations that process personal data on their behalf to use data only for purposes covered by the parties' contract.[56] The GDPR mandates that controllers report certain data security incidents to regulators within seventy-two hours of discovery and requires highly detailed post-breach assessments that include reasoning behind any decision not to report a breach.[57] Lack of compliance is enforced by a tier-system of fines, with the lower tier comprising two percent of an entity's worldwide annual revenue (or ten million euros, whichever is greater).[58]

While the above requirements may sound daunting, arguably the most formidable and controversial aspect of the GDPR is its extraterritorial impact. Article 3 of the GDPR applies the regulation even to controllers or processors "not established in the Union" when the processing of data relates to "(a) the offeri-

---

[44] Ducich & Fischer, *supra* note 43, at 209 (quoting GDPR, *supra* note 14, art. 5(1), at 35–36). The GDPR also has recitals that act as advisory notes, written to clarify the Regulation. *Id. at* 206; Leonard Wills, *A Very Brief Introduction to the GDPR Recitals*, A.B.A. (July 1, 2019), https://www.americanbar.org/groups/litigation/committees/minority-trial-lawyer/practice/2019/a-very-brief-introduction-to-the-gdpr-recitals/ [https://perma.cc/Z4DF-5X4H].

[45] Ducich & Fischer, *supra* note 43, at 208 (quoting GDPR, *supra* note 14, art. 4(7)) (defining "controller" as "an entity that 'determines the purposes and means of the processing of personal data.'").

[46] *Id.* (quoting GDPR, *supra* note 14, art. 4(8)) (defining "processor" as "'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.'").

[47] *Id.* (noting that while controllers are liable for processors' compliance, "processors are liable only for their compliance and for the compliance of any sub-processors they bring into the data transaction.").

[48] *Id.* at 206 (quoting GDPR, *supra* note 14, art. 4(1)). Note that the analogous American term, "personally identifiable information," is defined similarly but the information is protected sector by sector.

[49] GDPR, *supra* note 14, art. 13–14.

[50] *Id.* at art. 15.

[51] *Id.* at art. 17.

[52] *Id.* at art. 16.

[53] *Id.* at art. 18.

[54] *Id.* at art. 32.

[55] *Id.* at art. 34.

[56] *Id.* at art. 28(3).

[57] Ducich & Fischer, *supra* note 43, at 212.

[58] *Id.* at 213.

ng of goods or services . . . to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union."[59] In simplified terms, US-based companies must comply with the GDPR if the data they process relates to advertising to EU residents or the monitoring of residents' behavior. In our global economy, in which the vast majority of business is conducted online and websites are accessible to almost anyone, even small US businesses that collect consumer data could risk "targeting" EU residents for sales[60] or monitoring residents (because any data about consumer preferences could conceivably fall under the latter category).[61] Thus, the bottom line is that as soon as the GDPR was passed, it has been wise for US organizations to evaluate whether their practices arguably could come within the coverage of the GDPR and, if so, collect and process individuals' data in compliance with the regulation to avoid the hefty fines. The European Union recognizes certain rights of privacy that are more specific than those in the United States,[62] so the stringent requirements of the GDPR may be unfamiliar, but the extraterritorial language of the GDPR nonetheless makes the law broadly applicable.

Domestic law in the United States has occasionally clashed with the GDPR. *United States v. Microsoft Corp.*[63] highlighted the extreme tension between the United States' typical stance toward international law and the real need for coordination among nations in dealing with data privacy. In *Microsoft*, the corporation (no doubt wary of fines) received a search warrant from the US government, but argued that the GDPR prevented it from turning over the data stored in its data center in Dublin, Ireland.[64] The Supreme Court dismissed the case as moot under the Clarifying Lawful Overseas Use of Data (CLOUD) Act,[65] but the European Commission—the executive cabinet of the European Union—filed an amicus brief strongly asserting the primacy of the GDPR and pointing to Article 48, which states that a domestic judgment arising from a country outside the European Union requiring disclosure of personal data is enforceable only if based on a formal international agreement.[66] In short, even when trying to comp-

---

[59] GDPR, *supra* note 14, art. 3(2).

[60] *See* GUIDELINES 3/2018 ON THE TERRITORIAL SCOPE OF THE GDPR (ARTICLE 3), VERSION 2.1, EUROPEAN DATA PROTECTION BOARD 13–18 (Jan. 7, 2020) (including a list of factors to determine intent to target, such as use of currency "other than that generally used in the trader's country" or the use of "a top-level domain name other than that of the third country in which the controller or processor is established," such as ".fr" or ".eu." However, the report qualifies that any one of those factors taken alone may not be enough to clearly indicate intent to target.).

[61] *See id.* at 19–20.

[62] *See* Charter of the Fundamental Rights of the European Union, art. 8, 2012 O.J. (C 326) 397.

[63] 138 S. Ct. 1186 (2018) (per curiam).

[64] *See* Ducich & Fischer, *supra* note 43, at 214.

[65] 18 U.S.C. § 2713 (2018) (requiring organizations to produce information in their "possession, custody, or control, regardless of whether such . . . information is located within or outside of the United States.").

[66] GDPR, *supra* note 14, art. 48. Notably, the United States and European Union attempted to broker such an agreement, the E.U.-U.S. Privacy Shield Framework, but the agreement was invalidated by the Court of Justice of the European Union in 2020 (*see* Case C-311/18, Data Prot. Comm'r v. Facebook Ireland (Schrems II), ECLI:EU:C:2020:559 (July 16, 2020)).

ly with the GDPR, a US-based company could find itself in violation of domestic law as it currently stands.[67]

B. The United States' Sectoral Approach: A Federal and State Law Patchwork

While many other western countries have facilitated transactions with residents of the European Union by adopting comprehensive laws similar to the GDPR, the United States is ambling along with the sectoral approach, protecting privacy rights in certain sectors or industries rather than holistically.[68] The United States has some federal and state laws regulating data collection and processing, but no single overarching law to fill the inevitable gaps.[69] The framework is (with the exception of the recent comprehensive state laws) a patchwork of regulations covering "'specific types of data, like credit data or health information, or . . . specific populations like children, and regulat[ing] within those realms.'"[70] Because only certain sectors are regulated, this has created overlapping and sometimes contradictory protections.[71] The FTC is the executive body charged with enforcing privacy regulations under its ability to penalize companies for unfair business practices, but its powers are limited.[72]

Unlike Europe, the development of the United States' data privacy framework has been more reactionary than preventative and is not rooted in the fear of gruesome history repeating itself. In the United States, privacy as a legal right began with the Fourth Amendment to the Constitution,[73] but the privacy framework pertaining to data began in earnest with the Fair Information Practices of 1973, a report containing a set of regulatory goals proposed by the Department of Health, Education, and Welfare.[74] The report was motivated by the realization that a societal shift from the family to the individual (for tax and social security purposes) combined with rapidly developing computer technology could lead to

---

67 *See generally* Diane D. Reynolds et al., *Is a Company Permitted to Transfer PI From Europe to the US for a Discovery Request?*, GREENBERG TRAURIG (Nov. 8, 2022), https://www.gtlaw.com/en/insights/2022/11/published-articles/is-a-company-permitted-to-transfer-pi-from-europe-to-the-us-for-a-discovery-request [https://perma.cc/62B4-5XMC] (outlining the requirements of transferring personal information from Europe to the United States).

68 *See Reforming the US Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/Q5YC-3NQX] [hereinafter *Reforming the US Approach*]; SOLOVE & SCHWARTZ, *supra* note 35, at 7–8.

69 Klosowski, *supra* note 3.

70 *Id.* (quoting Amie Stepanovich, executive director at the Silicon Flatirons Center at Colorado Law).

71 *See Reforming the US Approach*, *supra* note 68 (discussing the tangle of federal regulations regarding health information).

72 *See id.*

73 *See* U.S. CONST. amend. IV.

74 *See* U.S. DEP'T OF HEALTH, EDUC., & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS, at xxxii (1973); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 510 (2006).

enormous potential for centralization, and thus compromise, of individuals' data.[75] In 1974, the Federal Privacy Act was passed,[76] requiring federal agencies retaining personal data to establish appropriate safeguards and inform citizens of their purpose for collecting data.[77] The Act also provided citizens with the right to access data stored by the agencies.[78] From there, regulatory statutes multiplied, covering sectors deemed at particular risk of compromising the personal data they collect. For example, the Fair Credit Reporting Act of 1970 "provides citizens with rights regarding the use and disclosure of their personal information by consumer reporting agencies."[79] The Family Educational Rights and Privacy Act of 1974 protects school records.[80] The Health Insurance Portability and Accountability Act of 1996 "gives the Department of Health and Human Services . . . the authority to promulgate regulations governing the privacy of medical records."[81] The Gramm-Leach-Bliley Act of 1999 "requires privacy notices and provides opt-out rights when financial institutions seek to disclose personal data to other companies."[82] These and many more make up the United States' privacy landscape at the federal level.

When focusing on this list of positive law, it may appear that solid limits have been placed upon data collection and processing. But in comparison with the GDPR, the gaps are obvious and glaring. In states that do not have explicit laws against the practice, organizations not covered by the federal laws can still use, share, or sell any data without notifying individuals.[83] On the cybersecurity side, there is no national standard for when a company must notify consumers if their data has been breached.[84] And if a company shares consumer data with third parties, those parties can share or sell it without notifying the consumer.[85]

There are also sectoral laws at the state level, though they have historically focused on cybersecurity rather than data privacy. The most common are "breach notification laws," which require companies to notify individuals if their informat-

---

[75] Solove, *supra* note 74, at 510; *see* U.S. DEP'T OF HEALTH, EDUC., & WELFARE, *supra* note 74. For a more detailed discussion of these goals, which also underpinned the United States' Privacy Act of 1974 (5 U.S.C. § 552a), see CHAPTER 7—PRIVACY AND CONFIDENTIALITY, POLICY MANUAL, U.S. CITIZENSHIP AND IMMIGRATION SERVICES (2023), https://www.uscis.gov/policy-manual/volume-1-part-a-chapter-7 [https://perma.cc/CUP8-VW9T]. Solove, *supra* note 74, at 517–19.

[76] Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a).

[77] Solove, *supra* note 74, at 517–19.

[78] *Id.* at 523.

[79] SOLOVE & SCHWARTZ, *supra* note 35, at 4; Fair Credit Reporting Act (FCRA), Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified as amended at 15 U.S.C. § 1681).

[80] *See* Family Educational Rights and Privacy Act (FERPA), Pub. L. No. 93-380, 88 Stat. 571 (1974) (codified at 20 U.S.C. § 1232g).

[81] SOLOVE & SCHWARTZ, *supra* note 35, at 5; Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 42 U.S.C.).

[82] SOLOVE & SCHWARTZ, *supra* note 35, at 5; Gramm-Leach-Bliley Act of 1999 (GLBA), Pub. L. No. 106-102, 113 Stat. 338 (codified in scattered sections of 15 U.S.C. and 12 U.S.C.).

[83] *See* Klosowski, *supra* note 3.

[84] *Id.*

[85] *Id.*

ion is compromised, whether due to a cyberattack, a corporate error, or other incident.[86] All states have breach notification laws, but each state differs in its specific requirements.[87] Therefore, organizations must be able to ascertain how many residents of that state could be affected in a breach. State breach notification laws vary substantially regarding the precise method of notification to residents,[88] the type of data that triggers notification,[89] and next steps if sensitive data is exposed.[90] As an example of the tangled web of requirements companies must keep track of, consider the following three states: Arizona requires that 1,000 residents be affected before notification must be made to the state attorney general;[91] Georgia does not require notification to state authorities, but does mandate that if over 10,000 residents are affected, the breached entity must notify all consumer reporting agencies;[92] New Jersey requires that any breaches whatsoever must be reported to the Division of State Police within the New Jersey Department of Law and Public Safety, and the notification must occur *prior* to the notice to the affected residents.[93] These requirements are a mere snapshot of the full body of mandates within each state's breach notification law.[94] With the extraordinary level of minute variation between states, it is no wonder companies are lobbying Congress to simplify matters on the data privacy side with a comprehensive federal framework.[95]

With respect to data privacy, some state legislatures have responded even more strongly to the lack of federal initiative, taking it upon themselves to create comprehensive laws that remedy the gaps left by the federal government. The

---

86 Ian C. Ballon, *Cybersecurity: Information, Network and Data Security*, *in* 4 E-COMMERCE AND INTERNET LAW: LEGAL TREATISE WITH FORMS 274–81 (2d ed. Thomson/West Pub., 2009), *reprinted as Complying with U.S. State and Territorial Security Breach Notification Laws*, *in* DAILY J. CYBERFORUM (2019) (explaining the purpose and breach application of state breach notification laws).

87 *See Security Breach Notification Chart*, PERKINS COIE (Oct. 2022), https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart.html [https://perma.cc/Y78G-KHYP].

88 *See id.* Compare Minnesota's options for notification to state residents (written or electronic notice) with New Hampshire's (written; telephonic with log of all notifications; electronic if that is the entity's primary means of communication with customers; or any method pursuant to entity's internal notification procedures).

89 *See id.* Compare Alabama's definition of personal information pertaining to medical history ("[a]ny information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional") with Alaska's (nothing about medical information), Illinois's (includes health insurance information and related identifiers), and Delaware's (includes "deoxyribonucleic acid profile").

90 *See id.* Connecticut, Delaware, the District of Columbia, and Massachusetts each require organizations to provide free access to credit monitoring if residents' social security numbers are exposed.

91 ARIZ. REV. STAT. ANN. § 18-552 (2022).

92 GA. CODE ANN. § 10-1-912(d) (2022).

93 N.J. STAT. ANN. § 56:8-163 (2023).

94 For a full summary of these laws, see *Security Breach Notification Chart*, *supra* note 87.

95 *See* Letter from Chief Executives of Leading Companies across industries to Congressional and Committee Leadership (Sept. 10, 2019), https://s3.amazonaws.com/brt.org/BRT-CEOLetteronPrivacy-Finalv2.pdf [https://perma.cc/U8XK-DSBL] (letter from various chief executives advocating for the passage of a federal privacy law to US Congressional leaders).

approach has its positive points. Until very recently, the prospect of the passage of a comprehensive federal law was slim to none, so states aiming to protect their residents had few other options. The strategy even seemed reasonable when California, the first state to pass a breach notification law,[96] became the first state with a comprehensive privacy law, enacting the California Consumer Privacy Act in 2018.[97] Because so many companies transact business with California residents and collect their data, the effect of the CCPA on the whole nation was similar to that of the GDPR. Companies nationwide simply adopted California's requirements, creating policies that would align them with the CCPA.[98]

California did not retain its position of domination over the legal landscape for long, though, and the influx of comprehensive laws has begun to raise red flags. In 2021, Virginia enacted its Consumer Data Protection Act which went into effect on January 1, 2023.[99] This law is similar to the CCPA,[100] but differs in material ways similar to the manner in which state notification laws differ and some experts have noted its relative weakness compared to the CCPA.[101] California's law remains the strongest protection for its residents, requiring companies that sell personal information to offer a global opt-out option, giving California residents control over the extent to which their data is resold.[102] California also offers its residents a private right of action where certain types of their sensitive personal information are disclosed in a data breach.[103] Moreover, California's law extends to residents in their capacity as employees or when their personal information is collected as part of a business transaction.[104] Virginia's law, on the other hand, contains no private right of action and requires residents to affirmatively object to certain types of processing for each individual instance.[105]

After Virginia, more threads of the state data privacy law patchwork began to weave together. In July 2021, Colorado enacted its own comprehensive law,

---

96 2002 Cal. Stat. 5778 (codified as amended at CAL. CIV. CODE § 1798.29 (West 2023)); *Reforming the US Approach*, *supra* note 68;

97 California Consumer Privacy Act (CCPA), 2018 Cal. Stat. 1807, *amended by* California Privacy Rights Act (CPRA), 2020 Cal. Stat. A-84 (current version at CAL. CIV. CODE § 1798.100 (West 2023)); David Harrington, *US Privacy Laws: The Complete Guide*, VARONIS (Sept. 2, 2022), https://www.varonis.com/blog/us-privacy-laws [https://perma.cc/N8WE-7BLR]; *see* F. Paul Pittman, *U.S. Data Privacy Guide*, WHITE & CASE (Aug. 31, 2022), https://www.whitecase.com/insight-our-thinking/us-data-privacy-guide [https://perma.cc/BT78-C6ZH].

98 *See* Natasha Singer, *What Does California's New Data Privacy Law Mean? Nobody Agrees*, N.Y. TIMES (Dec. 29, 2019), https://www.nytimes.com/2019/12/29/technology/california-privacy-law.html [https://perma.cc/97XH-CGKN].

99 Virginia Consumer Data Protection Act (VCDPA), 2021 Va. Acts 74 (codified at VA. CODE ANN. §59.1-575 (2022)).

100 As amended ineffective January 1, 2023 by the CPRA, 2020 Cal. Stat. A-84 (codified at CAL. CIV. CODE § 1798.100).

101 Klosowski, *supra* note 3 (quoting Kate Ruane, senior legislative counsel for the First Amendment and consumer privacy at the ACLU).

102 *Id.*

103 *Id.*

104 *Id.*

105 *Id.*

the Colorado Privacy Act;[106] in 2022, Utah passed the Utah Consumer Privacy Act,[107] and Connecticut enacted the Connecticut Data Privacy Act.[108] More states have passed comprehensive laws since these ones, all with their own variations.

Each of the aforementioned statutes are legislative attempts to do for state residents what the CCPA did for Californians and what the GDPR did for Europeans: respond to concerns about lack of visibility and control over how companies are using their data and try to solve the problem. These comprehensive laws and their sectoral counterparts have been useful for raising standards of privacy across the nation,[109] but the recent proliferation of statutory schemes has created a real problem for organizations. The tangled web of breach notification statutes is one matter; a whole body of privacy legislation that differs in minute ways for each state is a logistical nightmare. Experts also note the real possibility of burnout among privacy professionals. Law firms and other organizations charged with helping companies stay compliant are overwhelmed with the rapidly changing statutory landscape.[110] When the law changes substantially almost every month in a manner affecting the entire nation, it is a clear sign that standardization is needed.

C. A Federal Bill with Promise: The American Data Privacy Protection Act

To solve the mess of data privacy laws in the United States, the House Committee on Energy and Commerce has been diligently working toward compromise on a bill known as the American Data Privacy Protection Act (ADPPA) aimed to serve as a GDPR analog for the entire country and bring the United States up to speed with peer nations.[111] The bill has garnered rare bipartisan support and in July 2022 was even on track to head to the House floor for a vote, a first in the history of such bills advocating for comprehensive data privacy reform.[112] With the transition to a new congressional session, ADPPA appears to

---

106 *See* Colorado Privacy Act (CPA), 2021 Colo. Sess. Laws 3445 (codified at COLO. REV. STAT. § 6-1-1301 (2022)).

107 *See* Utah Consumer Privacy Act (UCPA), 2022 Utah Laws 3799 (codified at UTAH CODE ANN. § 13-61-101 (West 2022)).

108 Connecticut Data Privacy Act (CTDPA), 2022 Conn. Pub. Act No. 22-15; *Key Dates from US Comprehensive State Privacy Laws*, INT'L ASS'N OF PRIV. PROS. (Sept. 2022), https://iapp.org/resources/article/key-dates-from-us-comprehensive-state-privacy-laws/ [https://perma.cc/C4TN-ZGLB] (also see accompanying infographic); Anokhy Desai, *U.S. State Privacy Legislation Tracker*, INT'L ASS'N OF PRIV. PROS. (Oct. 7, 2022), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ [https://perma.cc/2AAU-25LT].

109 *See* Klosowski, *supra* note 3.

110 *See id.*

111 American Data Privacy Protection Act (ADPPA), H.R. 8152, 117th Cong. (2022); *see* Anne Toomey McKenna, *Bill Would Increase Data Privacy Protections—and Make Businesses Change How They Handle Data*, N.H. BULL. (Aug. 29, 2022, 5:30 AM), https://newhampshirebulletin.com/2022/08/29/a-new-us-data-privacy-bill-aims-to-give-you-more-control-over-information-collected-about-you-and-make-businesses-change-how-they-handle-data/ [https://perma.cc/5UC2-24TR].

112 *See* Cameron F. Kerry, *Federal Privacy Negotiators Should Accept Victory Gracefully*, THE BROOKINGS INST. (Aug. 12, 2022), https://www.brookings.edu/blog/techtank/2022/08/12/federal-privacy-negotiators-should-accept-victory-gracefully/ [https://perma.cc/6WU2-A6WP].

have lost steam; on December 30, 2022, it was placed on the House's Union Calendar at number 488 where it has stayed ever since.[113] Regardless, ADPPA marks a promising shift toward helpful federal regulation of data collection and processing, and ought to be given serious consideration.

The move toward a comprehensive federal privacy law began during the Obama administration with the Consumer Privacy Bill of Rights,[114] based on the Fair Information Practice Principles identified back in the 1970s.[115] The bill lost momentum, though, and data privacy retreated from the forefront of the national consciousness for several years, especially because the Trump administration was not inclined to pass sweeping federal regulation of any kind.[116] Public attention is now turned toward privacy once more, in part because of the influx of comprehensive state laws in the last few years. There are, of course, intense debates over the content of a potential federal law: the loudest voices resistant to compromise due to concern over weak protections are those among the California Privacy Protection Agency, which enforces the state's privacy act, and Democratic congressmembers like Washington Senator Maria Cantwell, chair of the Senate Committee on Commerce, Science, & Transportation (through which ADPPA would need to pass) and the primary voice of congressional opposition to ADPPA.[117] In 2018, Senator Cantwell and Senator Roger Wicker, a Republican from Mississippi who remains a member of Senator Cantwell's committee, kicked off privacy progress in earnest with separate draft bills.[118] The bills were materially different, sharply diverging on the issue of whether to preempt comprehensive state laws, and to what extent.[119] Senator Cantwell was a particularly prominent voice of caution, pointing out loopholes and suggesting improvements for ADPPA.[120] Recently, though, the latest drafts of Senator Cantwell's bill and the finalized version of ADPPA converged to become, as the Brookings Institution puts it, "virtually identical," marking a dramatic trend toward resolution.[121] ADPPA now includes specific provisions that it does not preempt California citizens' rights to private action after a breach, nor Illinois laws

---

113 H.R. 8152, 2022 Sess. (Dec. 30, 2022), *All Actions*, CONGRESS.GOV, https://www.congress.gov/bill/117th-congress/house-bill/8152/all-actions?q=%7B%22search%22%3A%22H.R.+8152+american+data+privacy%22%7D&s=2&r=1&overview=closed#tabs [https://perma.cc/6K4J-VPY7] (last visited Nov. 29, 2023). As of November 29, 2023, this remains the latest action on ADPPA.

114 *See* THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL ECONOMY (Feb. 2012), https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf [https://perma.cc/7Z5X-2XV5] (containing the Consumer Privacy Bill of Rights).

115 *Reforming the US Approach*, *supra* note 68; U.S. DEP'T OF HEALTH, EDUC., & WELFARE, *supra* note 74.

116 *See Reforming the US Approach*, *supra* note 68.

117 Kerry, *supra* note 112; Editorial Board, Opinion, *Democrats and Republicans Agree on this Tech Privacy Bill. But Can it Pass?*, WASH. POST (Dec. 8, 2022, 2:38 PM), https://www.washingtonpost.com/opinions/2022/12/08/tech-privacy-bill-bipartisan-congress/ [https://perma.cc/AH82-TNN7].

118 Kerry, *supra* note 112.

119 *Id.*

120 *Id.*

121 *Id.*

related to biometric and genetic information.[122] If reintroduced and passed, it would create a Bureau of Privacy within the FTC for enforcement, and violations would be treated as unfair or deceptive acts under the FTC Act.[123]

Experts and commentators have analyzed ADPPA's content, predicting what the bill might achieve for the US privacy field. ADPPA applies to "covered" entities, meaning any entity that collects, processes, or transfers covered data to another entity.[124] Nonprofits and some common carriers are included within this definition.[125] Data covered under the statute is any information or device that can be reasonably linked to a natural person.[126] ADPPA carves out a special category of sensitive data, such as biometric, health, financial, and geologic information, all which is subject to heightened requirements.[127] There is also a special category of entities, called "large data holders," which are organizations that meet certain thresholds of revenue or data processing.[128] Those entities are subject to stricter requirements.[129] Likewise, smaller entities that fall under a specified threshold of revenue derived from data transfers are exempt from certain requirements of ADPPA.[130]

For the most part, the framework of laws in the United States has been what leading privacy scholar Daniel J. Solove calls "rights-based,"[131] where the legislature provides individuals with laws they can use to assert privacy rights in case of violation.[132] The ball is in the data subjects' court; they must act as guardians of their own freedom and point to the law as an enforcement mechanism.[133] A purely rights-based model is rooted in the provision and withdrawal of user consent, but ADPPA incorporates some elements of what Solove calls a "structural" model, where the law places restrictions upon data collection regardless of consent.[134] As currently written, ADPPA mandates that "covered entities may

---

[122] Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. ANN. 14/1 (West 2023); Genetic Information Privacy Act (GIPA), 410 ILL. COMP. STAT. ANN. 513/1 (West 2023).

[123] *See* Niketa K. Patel et. al., *The American Data Privacy and Protection Act: Is Federal Regulation of AI Finally on the Horizon?*, MAYER BROWN (Oct. 21, 2022), https://www.mayerbrown.com/en/perspectives-events/publications/2022/10/the-american-data-privacy-and-protection-act-is-federal-regulation-of-ai-finally-on-the-horizon [https://perma.cc/C7P2-DZ4P]; *see also* 15 U.S.C. § 57(a) (2018).

[124] *See* McKenna, *supra* note 111.

[125] *Id.*

[126] *Id.*

[127] STAFF OF COMM. ON ENERGY & COM., 117TH CONG., JUNE 10, 2022 MEMORANDUM 3–5 (Comm. Print 2022).

[128] *Id.* at 4.

[129] *Id.*

[130] *Id.*

[131] *See* Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. 975 (2023).

[132] *Id.* at 983. Solove notes that a rights-based model of privacy protection is less effective than a structural approach, which would focus on placing the burden on organizations collecting data. Given that the rights-based approach currently dominates the legal landscape, my paper will focus on considerations of rights-based legislation.

[133] *Id.*; *Reforming the US Approach*, *supra* note 68 (discussing the United States' practice of placing the burden upon individuals to be vigilant about their own privacy rights).

[134] *See* Solove, *supra* note 131, at 993.

not collect, process, or transfer covered data beyond what is reasonably necessary, proportionate, and limited to provide specifically requested products and services or communicate with individuals in a manner they reasonably anticipate."[135] Covered data must also be permanently deleted once no longer necessary for its original purpose.[136] The Act also includes a civil rights component, containing "broad anti-discrimination protections to protect consumers irrespective of consent."[137] In comparison with the current landscape of privacy in the United States in which almost anything goes, incorporating the structural model of regulation could mark a drastic change in the status quo, especially if enforcement is effective.

Preemption has been a hotly contested issue, and ADPPA leans directly into the matter. The bill states that it should not be construed to preempt state laws regarding general consumer protection, civil rights laws, employee privacy laws, and many other specific areas.[138] Given the construction of the statute, it will preempt some aspects of the CCPA and CPRA, which is why some Californians in state government are skeptical.[139] But states are free to legislate more strictly in specific areas, so the Illinois Biometric Information Privacy Act[140] will not be affected.[141]

In summary, ADPPA requires that data collection be as minimal as possible, allowing covered entities to collect and share data only when reasonably necessary.[142] For the most part, ADPPA is a rights-based law, granting users nationwide an avenue to correct inaccuracies and delete data, but it sets up a framework of structural guardrails as a less flexible system to rein in misuse of data.[143]

D. First Amendment Considerations Inherent in a Comprehensive Federal Privacy Law

Like so much legislative change, ADPPA's development has been far from a unanimous process, with constitutional concerns underpinning many debates about the bill. The drive to pass ADPPA or a bill like it is derived from concern over individuals' privacy; on the other side, some companies desiring to collect, process, and use data have relied on the argument that regulation would infringe upon their freedom of speech.[144] Boiled down, the main tensions of ADPPA could

---

135 *See* STAFF OF COMM. ON ENERGY AND COMMERCE, 117TH CONG., *supra* note 127, at 4.

136 *Id.*

137 *Id.*

138 American Data Privacy Protection Act (ADPPA), H.R. 8152, 117th Cong. §§ 404–06 (2022).

139 McKenna, *supra* note 111.

140 Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. ANN. 14/1 (West 2023).

141 McKenna, *supra* note 111.

142 *Id.*

143 *See id.*

144 *See* Margot E. Kaminski & Scott Skinner-Thompson, *Free Speech Isn't a Free Pass for Privacy Violations*, SLATE (Mar. 9, 2020, 2:53 PM), https://slate.com/technology/2020/03/free-speech-privacy-clearview-ai-maine-isps.html [https://perma.cc/DHE9-9MJW].

be characterized as a Fourth[145] and First Amendment[146] standoff. At first glance it may seem as though compromise cannot be reached: how can a right to privacy in one's personal data be reconciled with a company's purported right to "speak" by using or sharing data? There is a strong line of American legal precedent recognizing that speech and privacy are interdependent and exist on a spectrum.[147] In particular, responding to the argument that using and sharing data is protected speech, scholars have noted that there is a recognized concept of privacy in public that outweighs freedom of speech.[148] The interplay of privacy and free speech was demonstrated recently when a company called Clearview AI argued in 2020 that it is protected free speech to "scrape" photographs of people's faces posted on public social media platforms for compilation in a gigantic facial recognition database.[149] However, when Clearview moved to dismiss the case, the ACLU argued that scraping these "faceprints" is not speech,[150] but regulatable conduct, as defined by *United States v. O'Brien*.[151] In Clearview's case, privacy won the day over a warped understanding of free speech. The case reached a settlement permanently restricting Clearview AI from making its faceprint database available to most private entities nationwide.[152]

The fate most likely for ADPPA, should it once again gain momentum, is that lawmakers will need to ensure it can pass a balancing test, something akin to the one recognized by the Supreme Court in *Sorrell v. IMS Health, Inc.*[153] In that case, the Court held that for commercial speech (which may turn out to be the correct category for the majority of data processing and sharing)[154], the burden is on the lawmaker to show that the statute "directly advances a substantial governmental interest and that the measure is drawn to achieve that interest."[155] On the other side of this kind of test, the inquiry is about harm to the data subject, so the balance is between government interest and harm to the individual. An increasing

---

145 *See* U.S. CONST. amend. IV.

146 *See* U.S. CONST. amend. I.

147 Kaminski & Skinner-Thompson, *supra* note 144.

148 *See id.*

149 Defendant's Motion to Dismiss at 3, ACLU v. Clearwater AI, Inc., No. 2020-CH-04353 (Ill. Cir. Ct. 2020).

150 Plaintiffs' Response to Defendant's Motion to Dismiss at 14–15, ACLU v. Clearwater AI, Inc., No. 2020-CH-04353 (Ill. Cir. Ct. 2020).

151 391 U.S. 367, 377 (1968).

152 ACLU v. Clearview AI, Inc., No. 2020-CH-04353 (Ill. Cir. Ct. 2020); *ACLU v. Clearview AI*, ACLU (May 11, 2022), https://www.aclu.org/cases/aclu-v-clearview-ai [https://perma.cc/C6AY-4RYJ]. For a general discussion of this dispute, see Vera Eidelman, *Clearview's Dangerous Misreading of the First Amendment Could Spell the End of Privacy Laws*, ACLU, NEWS & COMMENT. (Jan. 7, 2021), https://www.aclu.org/news/privacy-technology/clearviews-dangerous-misreading-of-the-first-amendment-could-spell-the-end-of-privacy-laws [https://perma.cc/7P32-MZCN].

153 564 U.S. 552 (2011).

154 Because, according to leading privacy scholar Eugene Volokh, "the Court's most common definition of commercial speech is 'speech that explicitly or implicitly propose[s] a commercial transaction.'" Eugene Volokh, *Freedom of Speech, Information Privacy, and the Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1081 (2000) (quoting Virginia State Bd. Of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 761 (1976)).

155 Sorrell v. IMS Health, Inc., 564 U.S. 552, 553–54 (2011).

number of courts have explored this "harm" aspect of the test. For example, in *Patel v. Facebook*, the Ninth Circuit Court of Appeals, concluded "that an invasion of an individual's biometric privacy rights 'has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts.'"[156] For ADPPA, legislators will need to establish that the legislation is warranted because the harm to individual privacy without ADPPA is greater than the interest of covered entities in unrestricted collecting and processing.[157]

II. THE UNITED STATES NEEDS A COMPREHENSIVE FEDERAL DATA PRIVACY LAW

A. The Patchwork Model is Unsatisfactory

Perhaps the most obvious reason Congress ought to give ADPPA serious consideration is the breadth and number of parties in favor of a federal law—and this law in particular. Countless parties have articulated why a federal law would be beneficial for the United States, citing concerns for individual privacy rights and the confusion and expense for businesses if the patchwork of laws was allowed to continue. For example, unlikely though it may seem, the head executives of major companies including Amazon, AT&T, Accenture, American Express, and Bank of America signed a joint letter to Congress in 2019 pleading for a federal privacy law.[158]

Without a federal law, there are several options to move forward, but none are satisfactory. The states could continue to pass a mix of sectoral and comprehensive laws. There has been a trend among many states authoring data privacy bills to base the text of their laws on the Washington Privacy Act, a bill that has not yet passed, but has nonetheless gained significant traction as a model template.[159] Nevertheless, whether states were to use the Washington Privacy Act or ADPPA, the material differences among the five most recent comprehensive state laws are a good indicator that the gaps of the patchwork approach wou-

---

[156] 932 F.3d 1264, 1273 (9th Cir. 2019) (quoting Spokeo Inc, v. Robins, 578 U.S. 330, 341 (2016)).

[157] Eidelman, *supra* note 152. For another example of a balancing test that could be relevant for ADPPA, see United States v. O'Brien, 391 U.S. 367 (1968) (finding that for regulations of conduct with an incidental effect on speech [which could be another fitting category for data collection]).

[158] Letter from Chief Executives of Leading Companies across industries, *supra* note 95 (writing "We urgently need a comprehensive federal consumer data privacy law to strengthen consumer trust and establish a stable policy environment in which new services and technologies can flourish within a well-understood legal and regulatory framework. Innovation thrives under clearly defined and consistently applied rules.").

[159] Washington Privacy Act, S.B. 6281, 66th Leg., Reg. Sess. (Wash. 2020); David Stauss, *State Data Privacy Legislation: Takeaways from 2022 and What to Expect in 2023*, INT'L ASS'N PRIV. PROS. (Aug. 23, 2022), https://iapp.org/news/a/state-data-privacy-legislation-takeaways-from-2022-and-what-to-expect-in-2023/ [https://perma.cc/3DUF-4C54].

ld not be eliminated.[160] Another option for state lawmakers is simply to wait for Congress to pass a law, whether ADPPA or not, and do nothing in the meantime. This is not likely, nor is it wise. Until recently, the only rules requiring companies to dispose of their massive stockpiles of old consumer data were the comprehensive state laws, meaning years of data has been at risk of exposure in a breach. The FTC recently updated its Safeguard Rule to mandate that companies dispose of customer information "two years after the last time the information is used in connection with providing a product or service to the customer unless the information is required for a legitimate business purpose," effective December 9, 2022.[161] State lawmakers are taking action as well: in the 2022 legislative cycle alone, the legislative bodies of twenty-nine states and the District of Columbia either introduced or carried over data privacy bills. Experts watching this legislative activity have remarked upon the unusually high level of attention to data privacy among states, an encouraging trend that will hopefully incentivize federal action.[162]

Reviewing the differences among the comprehensive state laws, one may wonder whether there could be a good reason for the differences—would a federal law do more harm than good, taking away states' ability to customize provisions like applicability thresholds, private rights of action, and amounts of fines? Interestingly, it is rare to find a practice-oriented article that even reaches the question of why the laws have material differences; they focus instead on how to keep track of the differences (a reality that may be due to the sheer struggle to keep up with the ever-changing legal landscape).[163] Likewise, scholarly articles on data privacy are generally oriented toward more theoretical questions about the legality and constitutional underpinnings of privacy and free speech.[164] But examining the laws themselves for trends is helpful, and yields further support for the passage of a federal law. The reason for the differences is likely more policy-oriented than anything; for example, Utah's act is the most business-friendly of the laws, allowing organizations considerable latitude to collect, process, and use data.[165] Connecticut's and Colorado's privacy acts are among the most consumer friendly (exceeded, of course, by the CCPA's strong consumer protections), with

---

160 *See Data Privacy Laws by State: Comparison Charts*, BLOOMBERG LAW (Feb. 2, 2022), https://pro.bloomberglaw.com/brief/data-privacy-laws-in-the-u-s/ [https://perma.cc/4L6H-J8W2].

161 *See* Standards for Safeguarding Customer Information, 16 C.F.R. § 314 (2022).

162 *E.g.*, *Data Privacy Laws by State*, *supra* note 160; Mark Smith, *Five Subtle Ambiguities in Virginia's New Privacy Law*, BLOOMBERG L. ANALYSIS (June 9, 2021, 4:01 AM), https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-five-subtle-ambiguities-in-virginias-new-privacy-law [https://perma.cc/8KAZ-G4T7]; *Comparing the 5 Comprehensive Privacy Laws Passed by U.S. States*, CLIENT ALERTS, KRAMER LEVIN NAFTALIS & FRANKEL (June 10, 2022), https://www.kramerlevin.com/en/perspectives-search/comparing-the-5-comprehensive-privacy-laws-passed-by-us-states.html [https://perma.cc/9QMH-CQMV]; Sheila A. Millar & Tracy P. Marshall, *The State of U.S. State Privacy Laws: a Comparison*, NAT'L L. REV. (Dec. 23, 2022), https://www.natlawreview.com/article/state-us-state-privacy-laws-comparison [https://perma.cc/U9TM-VYMD].

163 *See* Stauss, *supra* note 159.

164 *E.g.*, Volokh, *supra* note 154; Solove, *supra* note 131; Paul M. Schwartz, *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STAN. L. REV. 1559 (2000).

165 *See* Stauss, *supra* note 159.

requirements for opting out and prohibitions against dark patterns.[166] The tension between freedom for businesses and protection for consumers will always be at the heart of the privacy debate, but the benefits of a federal law will far outweigh the benefits of allowing states to diversify.

B. Addressing Arguments Against the Passage of a Federal Law

Scholars arguing against the GDPR and the passage of a federal law modeled after it tend to focus on the costs of compliance and the potential curtailing of technological progress. The below arguments represent the most prominent ones that could be brought against the passage of ADPPA, but they do not outweigh the benefits of passing the federal bill.

Matthew R. A. Heiman, Director of Planning at George Mason University's National Security Institute, wrote an article summarizing many of the main arguments against the GDPR which can be and have been levied at ADPPA as well.[167] He argues first that the key terms in the GDPR are either vaguely defined (such as "collect" and "store") or too expansive (such as "personal data," which is defined as "any information relating to an individual, whether it relates to his or her private, professional, or public life.").[168] Heiman highlights that vagueness in terminology is especially unforgivable in light of the significant penalties the GDPR includes for noncompliance.[169] But by virtue of the GDPR being passed first, the House Energy and Commerce Committee has been given the opportunity to cure major vagueness present in the GDPR when drafting ADPPA, and any leftover vague or overbroad terms must either be construed as intentional or a necessary evil of drafting a comprehensive statute. ADPPA's drafters seem to have been careful to minimize vagueness, defining covered entities to include nonprofits and specific groups of common carriers, defining sensitive data, and defining large data holders via thresholds.[170] And even if some key terms in ADPPA do remain ambiguous after its passage, covered entities and those charged with keeping them compliant can use the same interpretive strategies and doctrines used for every ambiguous legal provision.[171]

Heiman, like others,[172] notes that small businesses could struggle to meet the requirements of a sweeping law like the GDPR, citing a report saying that to

---

166 *See id.*

167 *See* Matthew R. A. Heiman, *The GDPR and the Consequences of Big Regulation*, 47 PEPP. L. REV. 945 (2020).

168 *Id.* at 949.

169 *Id.* at 950.

170 *See supra* section I.C.

171 For example, if plain meaning is ambiguous, practitioners can look to legislative history or similar guidance, as Europeans have done with the GDPR. The Article 29 Working Party was an advisory body charged with issuing guidelines for the interpretation of the GDPR, and their writings have provided much clarity when it came to ambiguous provisions. *See* WORKING PARTY GUIDELINES, EUR. COMM'N, NEWSROOM, https://ec.europa.eu/newsroom/article29/items [https://perma.cc/AL97-R8M9] (last visited Oct. 30, 2023).

172 *See e.g.*, *Hearing on the General Data Protection Regulation and California Consumer Privacy Act: Opt-Ins, Consumer Control, and the Impact on Competition and Innovation Before S. Comm. On the*

comply with the GDPR, a company will need to spend $1 million on the necessary technology.[173] However, while the GDPR does not contain exceptions for small businesses,[174] ADPPA does.[175] Moreover, experts have shown that GDPR-compliant businesses save money in the long run, because, when breaches do occur, the precautions put in place, like data security measures and data minimization, limit damage.[176]

Heiman argues that the GDPR threatens the internet's business model (referring to the practice of offering free services) and poses risks to emerging technologies like blockchain and the development of artificial intelligence (AI).[177] His arguments could be applied to ADPPA: if the majority of consumers withhold consent to tracking, companies will have to charge for services that were once offered for free, meaning platforms like Facebook, LinkedIn, and even some news sources could begin to charge fees.[178] And if consumers exercise their right to deletion, blockchain—which depends on the permanent retainment of information—will be unable to function.[179] Such a bleak picture, if applied to the United States, misses the bottom line: things cannot stay as they are in this country. As American law currently stands, the most helpful aspects of the law kick in after a breach has already occurred. There is a massive gap in the law that does not protect against the "sloppy mass data mining" that proves so disastrous when breaches inevitably occur.[180] A federal law modeled in the GDPR's image would be proactive, targeting data collection and use, rather than reactive. If that means free services and blockchain must change how they operate, that may be the necessary price to pay. "People lend their information to businesses, and those businesses have a responsibility to look after that information with care."[181]

Lastly, Heiman emphasizes that, in some circumstances, databases of information linkable to people can be very helpful to law enforcement, and is so

---

Judiciary, 116th Cong. (2019) (statement of Roslyn Layton, American Enterprise Institute); *see also* Oliver Smith, *The GDPR Racket: Who's Making Money from This $9 Billion Business Shakedown*, FORBES (May 2, 2018), https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/ [https://perma.cc/2NNP-XN7M].

173 Heiman, *supra* note 167 at 950 (citing George P. Slefo, *Got $1 Million? You're That Much Closer to Being GDPR Compliant*, ADAGE (Dec. 11, 2017), https://adage.com/article/digital/gdrp-privacy-costing-media-companies/311582) [https://perma.cc/V9GM-A67P].

174 *See GDPR for Small Businesses Under 250 Employees*, CLARIP, https://www.clarip.com/blog/gdpr-under-250-employees/ [https://perma.cc/G8NV-U3X9] (last visited Oct. 17, 2023).

175 American Data Privacy Protection Act (ADPPA), H.R. 8152, 117th Cong. § 209 (2022).

176 *See* Polanco, *supra* note 9, at 634 (citing Dan Swinhoe, *Does GDPR Compliance Reduce Breach Risk?*, CSO ONLINE (Mar. 29, 2019), https://www.csoonline.com/article/3369461/does-gdpr-compliance-reduce-breach-risk.html [https://perma.cc/TKR4-SASW]).

177 Heiman, *supra* note 167 at 950–51 (citing Anisha Mirchandani, *The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR*, 20 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1201, 1224 (2019)); A blockchain is a "distributed database or ledger that is shared among the nodes of a computer network" and collects information in groups known as blocks. Adam Hayes, *Blockchain Facts: What Is It, How It Works, and How It Can Be Used*, INVESTOPEDIA (Sept. 27, 2022), https://www.investopedia.com/terms/b/blockchain.asp [https://perma.cc/84FV-586Y].

178 Heiman, *supra* note 167, at 950–52.

179 *Id.*

180 Polanco, *supra* note 9, at 620.

181 *Id.* at 630.

crucial in some cases that enforcement would be significantly hindered without such information.[182] Privacy expert Michael Lamb agrees with Heiman, discussing how ADPPA in particular contains "unlimited rights for any person to opt out of data held by any firm that acquired the data indirectly" (such as anti-crime services that do not get their data directly from consumers) but "contains no exceptions for data used to prevent or investigate fraud or other crimes."[183] In other words, as Lamb points out, efforts to identify sexual predators or potential terrorists could be frustrated if such persons are able to request that third party data brokers not use their information.[184]

The best answer to Heiman and Lamb's arguments at this point may be that while enforcing the law may become more difficult, ensuring ADPPA's passage is more important than ironing out every kink, especially if alternative routes are available to law enforcement. Heiman discusses how the GDPR reduced access to WHOIS, a popular third-party database that was used by law enforcement, owners of intellectual property, security experts, domain name owners, and many others to identify infringers of intellectual property rights.[185] Practitioners have commented on the situation as it stands now that the GDPR is in place, saying the situation is not as dire as some predicted, and there are still strategies firms and government officials can use to enforce the law.[186] The situation may be the same for ADPPA if it passes; law enforcement will need to find other sources of the same information, or concerned groups could lobby for an amendment. Moreover, Lamb's complaint that even potential sexual predators or potential terrorists could opt out of data processing contains a hidden assumption that such people should not be eligible for privacy rights despite not yet having committed any crime. If this understanding of Lamb's argument is correct, his is a disturbing assertion that goes against the values of constitutional and criminal law.[187] Perhaps some carve-out for convicted criminals could be contemplated, in which criminals forfeit data privacy rights for a period of time. The fact remains that the need for a comprehensive federal law to protect individ-

---

182 Heiman, *supra* note 167, at 952.

183 Michael Lamb, *What's Needed to Improve the ADPPA*, INT'L ASS'N OF PRIV. PROS. (Oct. 20, 2022), https://iapp.org/news/a/whats-needed-to-improve-the-adppa/ [https://perma.cc/YXT5-NAF2].

184 *Id.*

185 Heiman, *supra* note 167, at 952 (discussing the WHOIS database, a registry of website ownership that was formerly open to the public); David E. Weslow et al., *Preparing for Drastic Changes to Availability of "WHOIS" Information About Domain Names*, WILEY LAW (Apr. 18, 2018), https://www.wiley.law/alert-IPAlert-PreparingforDrasticChangestoAvailabilityofWHOISInformationAboutDomainNames [https://perma.cc/WE9G-GPJD] (listing the various parties who have relied upon WHOIS for information).

186 David Cooper et al., *Enforcement in an Era of Data Privacy and Redacted WHOIS*, WORLD TRADEMARK REV. 2–3 (Oct. 1, 2019), https://www.worldtrademarkreview.com/article/enforcement-in-era-of-data-privacy-and-redacted-whois [https://perma.cc/2ZSD-8Q7R] (noting that "archived WHOIS information is still widely available" and that "monitoring tools can still be used to detect potential and actual infringements" as well as "online relay system[s]" that allow enforcers to "contain domain name registrants without having access to their personal data.").

187 *See Presumption of Innocence*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/presumption_of_innocence [https://perma.cc/N68C-PS4Q] (last visited Oct. 17, 2023).

ual privacy rights is greater than the inconvenience to law enforcement's search for suspects.

Roslyn Layton, visiting scholar at the American Enterprise Institute, and former law student Julian Mclendon raise other noteworthy arguments against the GDPR, contending that a similar model should not be used in the United States and implying that the patchwork functions smoothly.[188] First, Layton and Mclendon claim in a questionable twist that the GDPR does not protect data privacy, it is instead oriented only toward data protection.[189] They differentiate privacy from protection, first citing the International Association of Privacy Professionals' definition of information privacy as the "claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others."[190] They then explain that "data protection . . . is the safeguarding of information from corruption, compromise, or loss."[191] They are not the only people to make such a distinction: an article by IPSwitch states that "data protection is essentially a technical issue, whereas data privacy is a legal one."[192] But Layton and Mclendon's claim that the GDPR does not protect data privacy is simply incorrect. The one real measure of support they give their claim is that the word "privacy" does not appear in the final text of the GDPR other than in a footnote and that the "P" of "GDPR" stands for processing rather than privacy.[193] In fact, the GDPR was created precisely to protect an individual's right to determine "when, how and to what extent" their information is communicated to others, a goal which perfectly corresponds with data privacy.[194] ADPPA is constructed to do the same. Like the GDPR, ADPPA "allows individuals to access, correct, delete, and export covered data and opt out of data transfers and targeted advertising."[195] It is understandable why Layton and Mclendon interpreted these rights to be consistent with data protection, but that does not mean data privacy is not also protected. Both statutes empower individuals to determine how their information is collected and used.

Layton and Mclendon make it seem as though it would be a gross exaggeration to characterize the US data privacy landscape as the "wild west." They argue that there are "hundreds of laws relating to privacy and data protection in the

---

188 *See* Roslyn Layton & Julian Mclendon, *The GDPR: What it Really Does and How the U.S. Can Chart a Better Course*, 19 FEDERALIST SOC'Y REV. 234 (2018).

189 *Id.*

190 *Id.* at 235 (citing *Glossary of Privacy Terms*, IAPP, https://iapp.org/resources/glossary/#information-privacy [https://perma.cc/4HTM-FCUR] (last visited Nov. 14, 2023)).

191 *Id.*

192 Rick Robinson, *Data Privacy vs. Data Protection*, IPSWITCH (Jan. 30, 2020), https://blog.ipswitch.com/data-privacy-vs-data-protection [https://perma.cc/2SMW-DLWL].

193 Layton & Mclendon, *supra* note 188, at 235 (citing GDPR, *supra* note 14, n.18).

194 *Id.* (quoting *Information Privacy*, INT'L ASS'N OF PRIV. PROS: GLOSSARY, https://iapp.org/resources/glossary/#information-privacy [https://perma.cc/ZA75-6B2B] (last visited Oct. 17, 2023)); *What is GDPR, the EU's New Data Protection Law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr/ [https://perma.cc/JU8W-HTEL] (last visited Oct. 17, 2023).

195 Qiuyang Zhao, *American Data Privacy and Protection Act: Latest, Closest, Yet Still Fragile Attempt Toward Comprehensive Federal Privacy Legislation*, HARV. J. L. & TECH.: JOLT DIGEST (Oct. 19, 2022), https://jolt.law.harvard.edu/digest/american-data-privacy-and-protection-act-latest-closest-yet-still-fragile-attempt-toward-comprehensive-federal-privacy-legislation [https://perma.cc/7J8C-52NZ].

US—including common law torts, criminal laws, evidentiary privileges, federal statutes, and state laws."[196] Their argument proves too much. There may be hundreds of laws that relate in some way to privacy and data, but that does not fix the undeniable problems that those very laws present: American companies and individuals have been left vulnerable to cyberattacks due to complex and transient patchworks; all parties are confused about their rights and duties; and ultimately, the nation is left generally disadvantaged in a rapidly evolving digital world. Layton and Mclendon point to the Federal Trade Commission Act as the shining example of American privacy law; they point out that the FTC enforces privacy promises made only upon being broken and, presumably in contrast to the GDPR, "does not assume that every entity wants to harm online users."[197] The FTC presides over deceptive and unfair practices.[198] While the FTC has determined that claims of inadequate data security can legitimately fuel a deceptive practices claim, the lack of comprehensive regulations have resulted in lengthy, costly proceedings for those making data security claims.[199] Ambiguity in the FTC's current policies leads to gaps that can be filled by a comprehensive law. Even if Layton and Mclendon's characterization of the GDPR is correct, that simply means any similarities in ADPPA exist to further protection of data subjects. Even if ADPPA does err on the side of assuming the worst of entities, data subjects need the protection and the power ADPPA can provide.

Layton and Mclendon's final significant argument is the problematic assertion that the United States would not benefit from a GDPR-like privacy model because Americans simply care less about giving out their private data. They cite one study as proof of their argument and conclude that "this could explain why Americans are more comfortable with sharing information."[200] While their supporting claim that a GDPR-like model may not perfectly fit every country is sound, their generalization about American attitudes toward privacy has been undermined by numerous surveys and studies.

The reality of the American attitude toward data privacy sharply contradicts Layton and Mclendon's claims, signifying a real, abiding need for clarity and regulation. The Pew Research Center has a treasure trove of data, all pointing to a deep sense of confusion among average citizens and an increasing lack of trust toward data collectors. The Center identifies the 2013 leak by former National Security Agency contractor Edward Snowden as the beginning of America's suspicions about data collection and processing.[201] At the close of 2019, a clear majority of Americans expressed concern over the amount of data collected

---

196 Layton & Mclendon, *supra* note 188, at 236.

197 *Id.*

198 15 U.S.C. §§ 41-58 (2018).

199 *See* Polanco, *supra* note 9, at 623–26 (referencing F.T.C. v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015)).

200 *Id. at* 237; *see also Frequently Asked Questions*, HOFSTEDE INSIGHTS, https://hi.hofstede-insights.com/faq [https://perma.cc/M6S4-78NU] (last visited Oct. 17, 2023).

201 Brooke Auxier et al., *10 Tech-Related Trends That Shaped the Decade*, PEW RSCH. CTR. (Dec. 20, 2019), https://www.pewresearch.org/fact-tank/2019/12/20/10-tech-related-trends-that-shaped-the-decade/ [https://perma.cc/4FF3-M7AQ].

about them by companies and the government.[202] Most Americans "do not think it is possible to go about daily life without corporate and government entities collecting data about them."[203] Crucially, most Americans believe the risks of data collection outweigh the benefits.[204] It is true that about half of American adults are comfortable with the government collecting mass data to assess potential terrorist threats.[205] But most citizens who say they understand little to nothing about data protection laws are in favor of more governmental regulation.[206] In fact, half of American citizens are so concerned about privacy, they have been dissuaded from using a product or service.[207] In short, Americans emphatically *do* care about whether their information is collected and how it is used, regardless of the fact that their attitudes have changed dramatically over a short period of time. Americans deserve a regulatory scheme that they feel protects them adequately, and ADPPA shows great promise.

C. The American Data Privacy Protection Act's Consistence with the First Amendment

While the primary object of this Note is to argue that a federal law regulating data privacy is needed and that ADPPA appears to be a solid solution, it is important to briefly address ADPPA's fitness for withstanding First Amendment challenges; for no law can be a solution without passing constitutional muster. As mentioned above in section I.D, legislators wishing to pass ADPPA will need to be able to demonstrate why the harm to American citizens without ADPPA is greater than the interest of potential collectors and processers in unfettered data mining. Given that ADPPA does not apply to government entities,[208] leaving only private entities and nonprofits within ADPPA's restrictions, convincing a court that ADPPA is worth passing may prove to be straightforward. The government arguably has the most interest in collecting and processing data for the sake of national security and other important goals and will be exempt. Without ADPPA, the situation for citizens (who lack protection) and potential covered entities (which lack direction) is dire.

---

202 *See* Brooke Auxier & Lee Rainie, *Key Takeaways on Americans' Views About Privacy, Surveillance and Data-Sharing*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/ [https://perma.cc/VFP6-JGT2].

203 *Id.* *See* Brooke Auxier, *How Americans See Digital Privacy Issues Amid the COVID-19 Outbreak*, PEW RSCH. CTR. (May 4, 2020), https://www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/ [https://perma.cc/9GWK-AAU2]; *see also* Brooke Auxier, *How Americans See US Tech Companies as Government Scrutiny Increases*, PEW RSCH. CTR. (Oct. 27, 2020), https://www.pewresearch.org/fact-tank/2020/10/27/how-americans-see-u-s-tech-companies-as-government-scrutiny-increases/ [https://perma.cc/QJ6C-VKS8].

204 Auxier & Rainie, *supra* note 202.

205 *Id.*

206 *Id.*

207 *See* Andrew Perrin, *Half of Americans Have Decided Not to Use a Product or Service Because of Privacy Concerns*, PEW RSCH. CTR. (Apr. 14, 2020), https://www.pewresearch.org/fact-tank/2020/10/27/how-americans-see-u-s-tech-companies-as-government-scrutiny-increases/ [https://perma.cc/PGK2-9LB4].

208 *See* McKenna, *supra* note 111.

Leading privacy scholar Eugene Volokh once expressed doubt that sharing individuals' data between companies can be regulated as speech.[209] He acknowledges that the commercial speech doctrine has been held out as a promising category for data sharing but argues that data sharing does not meet the criteria for commercial speech.[210] "Under the 'speech that proposes a commercial transaction' analysis, communication of information about customers by one business to another is not commercial speech. It doesn't advertise anything, or ask the receiving business to buy anything from the communicating business."[211] Today, though, "collecting and selling data about people is estimated to be a $200 billion business, and all signs point to continued growth of the data-brokerage business."[212] Marketers, whether social media companies, grocery stores, or clothing retailers, can pay to license databases compiled by data brokers, who have gathered information about consumers through many different sources: "through loyalty cards, public records, social media posts, and most often by tracking their browsing behavior across different websites."[213] Marketers then target certain audiences using this data.[214] If this highly popular practice of data sharing for money is not commercial speech, hardly any other transactional speech would fit the bill; categorizing it as commercial would not stretch the definition.[215] Thus, legislators hoping to pass ADPPA can at least argue that this kind of speech passes First Amendment tests, and they can likely extend the definition to free data sharing without fear of putting many other kinds of speech at risk.[216]

Michael Lamb points out another First Amendment challenge ADPPA might face; ADPPA, as well as all five state comprehensive data privacy laws, exempts publicly available information about individuals from legal regulation.[217] It does so because "the Supreme Court has never upheld restricting speech when the content of the speech consists of true, publicly available information that was

---

209 *See* Volokh, *supra* note 154.

210 *See id.*, at 1075–76.

211 Volokh, *supra* note 154, at 1082.

212 Catherine Tucker & Nico Neumann, *Buying Consumer Data? Tread Carefully.*, HARV. BUS. REV. (May 1, 2020), https://hbr.org/2020/05/buying-consumer-data-tread-carefully [https://perma.cc/B7HM-LW36]. *See* Kalev Leetaru, *What Does It Mean for Social Media Platforms to "Sell" Our Data?*, FORBES (Dec. 15, 2018, 3:56 PM), https://www.forbes.com/sites/kalevleetaru/2018/12/15/what-does-it-mean-for-social-media-platforms-to-sell-our-data/?sh=51a4cd022d6c [https://perma.cc/6XXE-QUMW]; Kalev Leetaru, *The Data Brokers So Powerful Even Facebook Bought Their Data—But They Got Me Wildly Wrong*, FORBES (Apr. 5, 2018), https://www.forbes.com/sites/kalevleetaru/2018/12/15/what-does-it-mean-for-social-media-platforms-to-sell-our-data/?sh=51a4cd022d6c [https://perma.cc/WK5S-5KPF].

213 Tucker & Neumann, *supra* note 212.

214 *See id.*

215 Volokh, *supra* note 154, at 1084 (articulating a concern about stretching the definition of "commercial speech"). For another defense of data sharing as commercial speech, see Kathryn Peyton, *The First Amendment and Data Privacy: Securing Data Privacy Laws That Withstand Constitutional Muster*, 2019 PEPP. L. REV. 51, 75–76 (2020).

216 Volokh, *supra* note 154, at 1122 ("All the proposals for such expansion—whether based on an intellectual property theory, a commercial speech theory . . . would, if accepted, become strong precedent for other speech restrictions . . . [and] may shift courts and the public to an attitude that is more accepting of government policing of speech generally.").

217 Lamb, *supra* note 183.

lawfully made public."[218] Lamb predicts that ADPPA will face scrutiny because it allows for restriction of publicly available information if combined with covered data.[219] According to Lamb, databases used by law enforcement and identity authentication services routinely combine public data with covered data. While a deep dive into First Amendment precedent is outside the scope of this Note's analysis, it is conceivable that, if given the opportunity, the Court, taking all circumstances of the current data privacy landscape into account, would decide that data covered under ADPPA must take precedence over public data so that any combinations must give priority to covered data. The lack of protection for data addressed by ADPPA is so stark that it is time for federal regulation to be given serious consideration. Of course, any downsides of this relatively expansive approach should be thoughtfully considered as well, and Lamb even suggests adding a provision to ADPPA exempting public interest data uses (although one would imagine the exemption for government entities could be sufficient).[220] Ultimately, avenues around Volokh's and Lamb's objections are possible, leaving room for hope about ADPPA's viability.

CONCLUSION

The nature of privacy is difficult to pin down and challenging to regulate,[221] but the problems created by a lack of regulation in the United States far outweigh the costs of passing legislative solutions. The patchwork of laws currently comprising the United States' approach toward data privacy is confusing, outdated, and poses risks to individuals and companies alike. The federal government should take seriously the possibilities ADPPA poses for national (and international) harmony. Congress can iron out defects as needed but ought to keep passage of a federal law the main goal, as partisan arguing has too often killed efforts at regulating data collection.[222]

A comprehensive privacy law would change data subjects' daily lives for the better. People would be able to buy products and explore websites without concerns over how much of their data could be compromised from a single click.[223] Privacy policies would be easy to understand, and a baseline level of privacy would allow consumers to feel more comfortable clicking "I accept" in response to a boilerplate list of terms and conditions.[224] Consumers who know that companies will be held accountable for protecting against and responding to breaches will have higher levels of trust in their choices. On the other side, companies that have previously spent resources keeping breach notification laws and data privacy laws

---

218 *Id.*

219 *Id.*; *see* American Data Privacy Protection Act (ADPPA), H.R. 8152, 117th Cong. § 2(27) (2022).

220 Lamb, *supra* note 183.

221 *See generally* Solove, *supra* note 74 (laying out a framework to help scholars organize leading theories of privacy as a concept, but acknowledging that privacy is nebulous).

222 *See* Editorial Board, Opinion, *Enough Failures. We Need a Federal Privacy Law.*, WASH. POST (Mar. 30, 2022, 3:53 PM), https://www.washingtonpost.com/opinions/2022/03/30/congress-must-pass-federal-privacy-law/ [https://perma.cc/TRD8-8AM2].

223 Klosowski, *supra* note 3.

224 *Id.*

straight will enjoy the benefits of clarity about the exact limits of data collection, processing, and sharing.

Laying down rules and regulations is crucial when there is a lack of legal clarity, as there so clearly is with the United States' data privacy regime. A legal vacuum such as this cries out for what jurisprudence scholar Larry Alexander calls "authoritative settlement," or a set of rules to which all actors can point as the final authority.[225] A federal law would solve the problems of coordination among organizations and states; enable efficiency when it comes to everyday user experience; prevent greater injury when breaches occur; and allow for greater expertise in the privacy community, reducing burnout and leading to greater trust among consumers.

Naturally, a federal privacy law subject to legislative compromise will never fix every issue, but at least it could encourage the development of a technological world less hostile to people's privacy and provide protection against careless data mining.[226] After all, "'[p]rivacy isn't about not using tech, it's about being able to participate in society and knowing your data isn't going to be abused. . . .'"[227] Given the level of bipartisan agreement about the state of American data privacy, the time is right for a federal law to protect Americans' personal information from misuse.

---

[225] For a broad discussion of legal clarity for better efficiency, see Larry Alexander, *"With Me, It's All er Nuthin'": Formalism in Law and Morality*, 66 U. CHI. L. REV. 530, 533–36 (1999).

[226] *See* Klosowski, *supra* note 3.

[227] *Id.* (quoting Amie Stephanovich, executive director at the Silicon Flatirons Center at Colorado Law).