Volume 68 | Issue 3 Article 4

9-8-2023

Accept All Cookies: Opting-in to a Comprehensive Federal Data Privacy Framework and Opting-out of a Disparate State Regulatory Regime

Lauren A. Di Lella

Comments

ACCEPT ALL COOKIES: OPTING-IN TO A COMPREHENSIVE FEDERAL DATA PRIVACY FRAMEWORK AND OPTING-OUT OF A DISPARATE STATE REGULATORY REGIME

Lauren A. Di Lella*

I. Unlocking the Algorithm: Data Privacy in the United States

Sheri Cullens lost hundreds of dollars when hackers compromised her government-issued debit card during the 2013 Target data breach—one of the largest security breaches to date.[1] Cullens was a single mother and relied on this income to support her family each month; she realized the money was missing just days before her rent was due.[2] Target never informed Cullens that the card had been compromised nor that her money was stolen.[3]

Cullens' story serves as just one example of those who have fallen victim to data breach and suffered financial loss as a result.[4] Some victims may eventually obtain relief from the breached company or by pursuing

* J.D. Candidate, 2024, Villanova University Charles Widger School of Law; B.A., 2021, Occidental College. This Comment is dedicated to my parents, Nancy and Paul Di Lella, whose impressive legal careers inspired me to attend law school and become an advocate for others, and to my brothers and grandparents, who support me in all things. Many thanks to the members of the *Villanova Law Review* for their editorial feedback.

1. *See* Beth Pinsker, *Consumers Vent Frustration and Anger at Target Data Breach*, Reuters (Jan. 13, 2014, 7:30 PM), https://www.reuters.com/article/us-target-consumers/consumers-vent-frustration-and-anger-at-target-data-breach-idUSBREA0D01Z20140114 [https://perma.cc/9R69-HJHN] (sharing the stories of consumers who suffered following the 2013 Target data breach, where "tens of millions of Target customer credit and debit card data was hacked"). Cullens' debit card was compromised after she purchased prescription medicine at Target in late December right before the breach occurred around the holidays. *Id. See also* Jim Finkle & Dhanya Skariachan, *Target Cyber Breach Hits 40 Million Payment Cards at Holiday Peak*, Reuters (Dec. 18, 2013, 7:05 PM), https://www.reuters.com/article/us-target-breach/target-cyber-breach-hits-40-million-payment-cards-at-holiday-peak-idUSBRE9BH1GX20131219 [https://perma.cc/N66V-DVHQ] (reporting that in 2013, this was the "second-largest . . . breach reported by a U.S. retailer").

2. *See* Pinsker, *supra* note 1 (sharing Cullens' story and experience with Target).

3. *See id.* (claiming no one from Target contacted her to tell her the card had been compromised or answered her phone calls or emails once she found out). Following the breach, Cullens "worked out the issue with Florida state officials," but said she would never shop at Target again. *Id.*

4. *See id.*; *see also New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021*, Fed. Trade Comm'n (Feb. 22, 2022), https://www.ftc.gov/news-

limited claims under state or federal law, but these instances of recovery are few and far between, and there is currently no comprehensive federal remedy for such devastating privacy violations.[5]

In 2022 alone, hackers compromised the personal data of over 422 million Americans.[6] Seventy-nine percent of Americans express concern about the way companies use and share their data, and sixty-four percent express the same concern with respect to the United States government; yet sixty-three percent do not understand what laws protect their data privacy rights, and seventy-five percent are not confident that perpetrators are held accountable for misusing data.[7] Thus, while most Americans do not trust companies or the government to protect their data privacy, they inevitably do not understand how to protect their own personal information.[8]

---

events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0 [https://perma.cc/8BLS-S6BC] (reporting that in 2021 alone, the FTC received 2.8 million fraud reports, which caused consumers to suffer $5.8 billion worth of loss); Ido Kilovaty, *Psychological Data Breach Harms*, 23 N.C. J.L. & TECH. 1, 9 (2021) (noting how data breach harms can manifest in non-financial, psychological ways as well). In particular, the author discusses depression, anxiety, post-traumatic stress disorder (PTSD), and other related conditions that commonly result when individuals suffer from a data breach. *Id.*

5. For further discussion of the challenges consumers face in trying to obtain relief for data privacy violations under the current statutory regime, see *infra* Section II.B.1. *See also* Rachel Abrams, *Target to Pay $18.5 Million to 47 States in Security Breach Settlement*, N.Y. TIMES (May 23, 2017), https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html [https://perma.cc/CS8Q-DPYV] (reporting the Target data breach settlement statistics); Rob Sobers, *64% of Americans Don't Know What to do After a Data Breach—Do You? (Survey)*, VARONIS (Oct. 14, 2022), https://www.varonis.com/blog/data-breach-literacy-survey [https://perma.cc/BSV5-RZ5Q] (identifying an additional problem that precludes consumers from proper redress—namely, that fifty-six percent of Americans would not even know how to remedy a data breach).

6. *See* Ani Petrosyan, *Cyber Crime: Number of Compromises and Impacted Individuals in U.S. 2005–2022*, STATISTA (Apr. 1, 2023), https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed [https://perma.cc/WV8V-XGLD] (explaining how data compromise may occur in the form of data breach, data leakage, or data exposure—all of which often result in an unauthorized threat actor gaining access to consumers' sensitive data).

7. *See* Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, *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/DS7Q-EDU5] (conveying Americans' beliefs about data privacy). Pew's study reveals that Americans feel their personal data is less secure now than it ever has been before, that data collection poses more risks than benefits to individuals, and that it is not possible to go through life without being tracked by companies or the United States government. *Id.* Nevertheless, most Americans "are not confident about the way companies [and the United States government] will behave when it comes to using and protecting their personal data." *Id.*

8. *See id.* (discussing Americans' overall lack of confidence regarding the protection of their data privacy). Sixty-three percent of Americans say they under-

Data privacy is the right to retain control and knowledge about any personally identifiable information (PII) that is collected from or about an individual.[9] As technology continues to advance and the world becomes increasingly digitized, consumer data becomes a more valuable commodity.[10] Businesses use consumer data to modify their marketing strategies and generate additional cash flow, and cybercriminals sell it to earn a profit on the black market.[11] Consumers do care about their privacy when they fall victim to data breach and find themselves in Sheri Cullens' position experiencing financial loss—or worse, identity theft.[12] Nevertheless,

---

stand very little or nothing about the laws and regulations in place to protect their data privacy rights. *Id.*

9. *See* Shaun G. Jamison, *Creating a National Data Privacy Law for the United States*, 10 CYBARIS INTELL. PROP. L. REV. 1, 5 (2019) (defining "data privacy" and explaining different forms of "personally identifiable information," including one's name, social security number, or bank account number); *see also* William Newhouse, Michael Ekstrom, Jeff Finke & Marisa Harriston, *Securing Property Management Systems*, NAT. INST. STANDARDS & TECH. 1, 58 (2021) (defining PII as "[i]nformation that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual").

10. *See* Max Freedman, *How Businesses are Collecting Data (And What They're Doing With It)*, BUS. NEWS DAILY (May 30, 2023), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html [https://perma.cc/79D2-PR96] (discussing the proliferation of technologies that capture and analyze consumer data). Freedman notes how some companies have used such technologies to improve their marketing intelligence. *Id.* In fact, "[s]ome companies have built an entire business model around consumer data, whether they sell personal information to a third party or create targeted ads to promote their products and services." *Id.*

11. *See id.* (explaining why businesses collect data). One reason is to "improve the customer experience," by modifying a company's digital presence based on consumers' individualized preferences. *Id.* This helps the company understand how consumers engage with and respond to their marketing campaigns and allows them to adjust their operating models accordingly. *Id.* Companies also "transform the data into cash flow" by selling it to data brokers or data service providers, who then sell it to third-party advertisers. *Id. See also* A. Dominick Romeo, *Hidden Threat: The Dark Web Surrounding Cyber Security*, 43 N. KY. L. REV. 73, 77–78 (2016) (reporting that stolen data, including healthcare information and credit card and social security information, are often available for purchase on the dark web). Buyers typically use bitcoins or other cryptocurrencies to purchase the data, which allows users and transactions to remain completely anonymous. *Id.* at 78.

12. For a discussion of Sheri Cullens' financial loss following the 2013 Target breach, see Pinsker, *supra* notes 1–3 and accompanying text. *See also* Robert L. Rabin, *Perspectives on Privacy, Data Security and Tort Law*, 66 DEPAUL L. REV. 313, 315 (2017) (highlighting the number of Americans who have become victims of identity theft due to hackers stealing their data). Data breaches have tangible effects and are felt widely among the American public, as they often result in monetary loss and a decrease in one's credit score. *Id.* For a discussion of the psychological side effects consumers may experience following identity theft, see Kilovaty, *supra* note 4.

many Americans consent to the collection of their data by readily agreeing to privacy policies on websites or apps they interact with, and take no action to protect their data beyond routinely changing passwords.[13]

In response to growing concerns over the collection, storage, and use of consumer data, several states have enacted data privacy laws.[14] In 2022, state lawmakers introduced over one hundred bills, albeit with divergent regulatory requirements.[15] This has led to a "patchwork of state laws," which makes it difficult for consumers to understand their rights and creates challenges for organizations operating across state borders that must comply with fifty-plus differing and changing data privacy frameworks.[16]

Politicians and privacy experts largely agree that the solution to this complex issue, at least in part, is a comprehensive federal data privacy law with preemptive power over the disparate state data privacy laws.[17] The

13. *See* Auxier, Rainie, Anderson, Perrin, Kumar & Turner, *supra* note 7 (reporting only nine percent of adults always read privacy policies before agreeing to them). *But see* Geoffrey A. Fowler, *I Tried to Read All My App Privacy Policies. It Was 1 Million Words.*, WASH. POST (May 31, 2022, 7:00 AM), https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/ [https://perma.cc/4SZV-LQ4C] (explaining most adults do not read privacy policies because of their length, convoluted language, and lack of a meaningful opportunity to negotiate); *see also* Rob Sobers, *Do Americans Ever Change Their Passwords?*, VARONIS (Oct. 14, 2022), https://www.varonis.com/blog/america-password-security [https://perma.cc/FL8L-8ELL] (stating Americans do not seem to change their digital habits despite expressing concern over cyberattacks and data breach).

14. *See* Fara Soubouti, *Data Privacy and the Financial Services Industry: A Federal Approach to Consumer Protection*, 24 N.C. BANKING INST. 527, 531 (2020) (noting several states introduced comprehensive data privacy bills to "enhance consumer data protections of their residents"). Many of these bills grant consumers the right to access personal information collected and shared with third parties, inquire about the deletion of their data, understand data portability, and opt out of the sale of their personal information. *Id.* For further discussion of these state laws, see *infra* Section II.B.2.

15. *See* Kristin L. Bryan, *Congress Proposes Federal Privacy Legislation to Preempt Certain State Privacy Laws, Hearing Scheduled for Next Week*, NAT'L L. REV. (June 9, 2022), https://www.natlawreview.com/article/congress-proposes-federal-privacy-legislation-to-preempt-certain-state-privacy-laws [https://perma.cc/67GY-JTPZ] (highlighting the recent increase in the number of states introducing data privacy legislation). Some states, such as Florida, have sought "to adopt broad privacy regimes" while other states have focused on drafting privacy bills that are "narrowly tailored to specific areas such as biometric privacy, AI [artificial intelligence], and facial recognition." *Id.*

16. *See* Telephone Interview with Kim Gold, Chief Privacy Officer, Genentech (Oct. 28, 2022) (notes on file with author) (identifying the current system as a "patchwork" of state data privacy laws and discussing the challenges this presents); *see also* Jason Hirsch, Comment, *A New Digital Age: Why COVID-19 Necessitates Preemptive Federal Action to Regulate Data Privacy*, 94 TEMP. L. REV. ONLINE *1, *2–3 (2022) (discussing the downfalls of the "increasing patchwork of data privacy laws that vary state to state," and calling for uniform federal legislation to "eliminate the potential of inequitable protections between Americans residing in different states").

17. *See, e.g.*, House Energy and Commerce Committee Chair Cathy McMorris Rodgers, *Energy and Commerce Leaders Announce Hearing on Enhancing Privacy Protections for Americans*, H. COMM. ENERGY & COM. (Feb. 22, 2023), https://energycom-

question has now shifted to how such a law will operate in practice.[18] After a longstanding partisan divide, the House Energy and Commerce Committee introduced the American Data Privacy and Protection Act (ADPPA) on June 21, 2022.[19] If enacted, the ADPPA would be the first comprehensive data privacy law in the United States.[20]

This Comment argues that the ADPPA will be effective in practice because it makes notable progress towards improving data privacy protections and strikes the appropriate federalism balance necessary to withstand preemption-based constitutional challenges.[21] While it is imperative

---

merce.house.gov/posts/energy-and-commerce-leaders-announce-hearing-on-enhancing-privacy-protections-for-americans [https://perma.cc/R4BS-2LUT] ("The Energy and Commerce Committee is continuing to lead on creating a national data privacy standard that will minimize the amount of Americans' information companies are allowed to collect, process, and transfer. It is the strongest way to promote innovation, put individuals in charge of their data, and protect children online."); Gold, *supra* note 16 ("The United States would be better served by a comprehensive privacy law."); Letter from Tim Cook, Chief Exec. Officer at Apple, to Rep. Maria Cantwell, Chair of U.S. Senate Comm. Com., Sci., & Transp., Rep. Roger Wicker, Ranking Member of U.S. Senate Comm. Com., Sci., & Transp., Rep. Frank Pallone, Jr., Chair of U.S. House Comm. Energy & Com. & Rep. Cathy McMorris Rodgers, Ranking Member of U.S. House Comm. Energy & Com., (June 10, 2022, 9:42 AM), https://9to5mac.com/2022/06/10/tim-cook-privacy-letter/ [https://perma.cc/35UX-VDKM] ("Apple continues to support efforts at the federal level to establish strong privacy protections for consumers, and we are encouraged by the draft proposals your offices have produced.").

18. *See* Soubouti, *supra* note 14, at 527 ("Industry leaders are no longer asking *if* a comprehensive federal data privacy law should be implemented; instead, the question has shifted to *how* it should be implemented.").

19. *See generally* American Data Privacy and Protection Act, H.R. 8152, 117th Cong., 2d Sess. (2022) (outlining the provisions of the bill); *see also* Hirsch, *supra* note 16, at *2 (acknowledging the "deep partisan divides in Congress," which have "prevented meaningful action toward adopting a federal data privacy law" in the past).

20. For a discussion of why previous efforts to enact comprehensive federal data privacy legislation have been unsuccessful, see *infra* notes 25–28 and accompanying text. *See also The American Data Privacy and Protection Act*, ABA (Aug. 30, 2022), https://www.americanbar.org/advocacy/governmental_legislative_work/publications/washingtonletter/august-22-wl/data-privacy-0822wl/ [https://perma.cc/84TF-LXV8] ("[T]he American Data Privacy and Protection Act (ADPPA) represents a major step forward by Congress in its two-decade effort to develop a national data security and digital privacy framework that would establish new protections for all Americans.").

21. For further development of this argument, see *infra* Part IV. For the direct text of the ADPPA's preemption provision, see H.R. 8152 §§ 404(b)(1)–(2). The provision states:

> No State or political subdivision of a State may adopt, maintain, enforce, prescribe, or continue in effect any law, regulation, rule, standard, requirement, or other provision having the force and effect of law of any State, or political subdivision of a State, *covered* by the provisions of this Act, or a rule, regulation, or requirement promulgated under this Act.

Id. § 404(b)(1) (emphasis added). Explicit carve outs (i.e., non-preempted laws) include:

> (A) Consumer protection laws of general applicability such as laws regulating deceptive, unfair, or unconscionable practices, except that the fact

that any federal statute leaves room for states to exercise their constitutionally granted police powers, an effective data privacy law must be preemptive enough to override disparate state regulations and provide the robust protections that are currently lacking.[22] The ADDPA is the first

> of a violation of this Act or a regulation promulgated under this Act may not be pleaded as an element of any violation of such a law. (B) Civil rights laws. (C) Provisions of laws, in so far as, that govern the privacy rights or other protections of employees, employee information, students, or student information. (D) Laws that address notification requirements in the event of a data breach. (E) Contract or tort law. (F) Criminal laws. (G) Civil laws governing fraud, theft (including identity theft), unauthorized access to information or electronic devices, unauthorized use of information, malicious behavior, or similar provisions of law. (H) Civil laws regarding cyberstalking, cyberbullying, nonconsensual pornography, sexual harassment, child abuse material, child pornography, child abduction or attempted child abduction, coercion or enticement of a child for sexual activity, or child sex trafficking. (I) Public safety or sector specific laws unrelated to privacy or security. (J) Provisions of law, insofar as such provisions address public records, criminal justice information systems, arrest records, mug shots, conviction records, or non-conviction records. (K) Provisions of law, insofar as such provisions address banking records, financial records, tax records, Social Security numbers, credit cards, consumer and credit reporting and investigations, credit repair, credit clinics, or check-cashing services. (L) Provisions of law, insofar as such provisions address facial recognition or facial recognition technologies, electronic surveillance, wiretapping, or telephone monitoring. (M) The Biometric Information Privacy Act (740 ICLS 14 et seq.) and the Genetic Information Privacy Act (410 ILCS 513 et seq.). (N) Provisions of laws, in so far as, such provisions to address unsolicited email or text messages, telephone solicitation, or caller identification. (O) Provisions of laws, in so far as, such provisions address health information, medical information, medical records, HIV status, or HIV testing. (P) Provisions of laws, in so far as, such provisions pertain to public health activities, reporting, data, or services. (Q) Provisions of law, insofar as such provisions address the confidentiality of library records. (R) Section 1798.150 of the California Civil Code (as amended on November 3, 2020 by initiative Proposition 24, Section 16). (S) Laws pertaining to the use of encryption as a means of providing data security.

Id. §§ 404(b)(2)(A)–(S).

22. *See* Hearing on Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security Before the H. Subcomm. Consumer Prot. & Com., 117th Cong. 85 (2022) [hereinafter *Hearing on Protecting America's Consumers*] (statement of Rep. Bob Latta) ("A *preemptive* national privacy and data security bill clearly is a priority for consumers, for economy, and to maintain U.S. competitiveness." (emphasis added)); *see also* U.S. CONST. amend. X ("The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people."). *But see* Tatyana Bolton, Brandon Pugh, Sofia Lesmes, Lauren Zabierek & Cory Simpson, *Preemption in Federal Data Security and Privacy Legislation*, R ST. INST. (May 31, 2022), https://www.rstreet.org/commentary/preemption-in-federal-data-security-and-privacy-legislation/ [https://perma.cc/CUN6-QEFA] (questioning whether a preemptive federal comprehensive data privacy law will displace traditional state authority to enact legislation in this area). The authors urge the importance of a preemption provision that includes "[s]elect carve-outs" because "they respect and uphold the long history of states having control over unique issues that affect their area, they account for areas that are best addressed by having a local approach instead of a

significant step in the United States' federal data privacy framework, so lawmakers should take the opportunity to understand where the bill falls short and continue to work together to improve protections for all stakeholders.[23]

Part II of this Comment discusses Congress's past efforts to enact comprehensive data privacy legislation and explains why there is now bipartisan support for such a law. Next, Part III examines the ADPPA as Congress's most recent attempt to implement a uniform data privacy standard. Part IV critically analyzes whether the ADPPA will be successful in practice notwithstanding its shortcomings, and explains why it will likely withstand constitutional scrutiny. Finally, Part V discusses the potential implications of passing the ADPPA as it currently stands.

II. DECRYPTING KEY ISSUES IN THE UNITED STATES' DATA PRIVACY FRAMEWORK

The Federal Trade Commission (FTC) first called on Congress to enact comprehensive data privacy legislation in May of 2000.[24] Since then, partisan politics has largely prevented Congress from passing such a law.[25] In 2012, for example, the Obama administration introduced the Consumer Privacy Bill of Rights (CPBR), which Republicans voted against due to concerns that it would "stifle industry innovation."[26] For years, compa-

national one, and they can help fill gaps not covered by federal law." *Id.* For further development of this argument, see *infra* Part IV.

23. *See* The American Data Privacy and Protection Act, Hearing on H.R. 8152 Before the H. Comm. on Energy & Com., 117th Cong. 13 (2022) [hereinafter *Hearing on ADPPA*] (statement of Rep. Gus Bilirakis, Subcomm. Consumer Prot. & Com.) (recognizing the "bipartisan efforts" representatives have undertaken to get the ADPPA to this point but acknowledging that "our work is still not done"). Rep. Bilirakis stated: "I am glad that every member on this committee will be able to consider this legislation and weigh in as we continue to tweak this product further. . . . This is the best opportunity we have had in years to give the American people and businesses something that has been long needed." *Id.* at 13–14. *See also The American Data Privacy and Protection Act*, *supra* note 20 (predicting the ADPPA could become a priority issue once the 118th Congress convenes).

24. *See* Jessica Rich, *After 20 Years of Debate, It's Time for Congress to Finally Pass a Baseline Privacy Law*, BROOKINGS INST. (Jan. 14, 2021), https://www.brookings.edu/blog/techtank/2021/01/14/after-20-years-of-debate-its-time-for-congress-to-finally-pass-a-baseline-privacy-law/ [https://perma.cc/YD7T-4MLN] (explaining how very few companies disclosed their data collection and usage practices when the FTC and leading privacy groups turned to Congress in 2000 to pass a federal law to protect Americans' basic data privacy rights).

25. *See* Tiffany Light, *Data Privacy: One Universal Regulation Eliminating the Many States of Legal Uncertainty*, 65 ST. LOUIS U. L.J. 873, 893 (2021) (noting there have been "numerous attempts within the last decade to pass federal privacy regulations, but none have been successful"). Although some may not expect data privacy to be a highly partisan issue, finding a solution has very partisan undertones and has garnered pushback from Republicans and Democrats alike. *Id.* at 893–94.

26. *See id.* at 894 (indicating that Republicans proposed "self-regulation" as an alternative means to regulate industry under the CPBR); *see also Administration Discussion Draft: Consumer Privacy Bill of Rights Act* (2015), https://

nies across different industries have advocated for a federal law to ease their compliance burden and override disparate state regulations.[27] Opponents pushed back, explaining they do not want a federal standard that will diminish the laws states have worked tirelessly to implement.[28]

In September 2020, commentators believed Republicans and Democrats took steps towards compromise when both parties introduced comprehensive data privacy legislation.[29] Senator Roger F. Wicker (R-MS) introduced the Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act (SAFE DATA) and Senator Maria Cantwell (D-WA) introduced the Consumer Online Privacy Rights Act (COPRA), the latter of which is similar to the ADPPA.[30] Neither bill

---

obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf [https://perma.cc/PU7K-GSRY] (outlining the provisions of the CPBR).

27. *See* Gold, *supra* note 16 (stating the United States might be better served by a comprehensive privacy law based on a common set of principles that regulates across all industries). According to Ms. Gold, this would be "more efficient, and effective in protecting individual rights, as opposed to a complex web of disparate state and federal data privacy laws." *Id.* For further discussion about why businesses support federal privacy legislation, see *infra* Section II.A.2.

28. *See, e.g.*, Hayley Tsukayama, *Federal Preemption of State Privacy Law Hurts Everyone*, ELEC. FRONTIER FOUND. (July 28, 2022), https://www.eff.org/deeplinks/2022/07/federal-preemption-state-privacy-law-hurts-everyone [https://perma.cc/YAB5-74E4] (identifying the Electronic Frontier Foundation (EFF) as a major opponent to the ADPPA because of how the bill would undercut state data privacy laws). EFF opposes the ADPPA because of its broad preemptive power and believes "the ability to pass bills at the state and local level is one of the strongest points of leverage that people have in the fight for data privacy." *Id. See also* Press Release, Rep. Anna Eshoo, *Rep. Eshoo Introduces Amendment to Protect California Privacy Law in ADPPA* (July 20, 2022), https://eshoo.house.gov/media/press-releases/rep-eshoo-introduces-amendment-protect-california-privacy-law-adppa [https://perma.cc/ZMG7-RFQ2] (introducing an amendment that would protect California's ability to strengthen its own privacy protections in the future).

29. *See* Cameron F. Kerry & Caitlin Chin, *How the 2020 Elections Will Shape the Federal Privacy Debate*, BROOKINGS INST. (Oct. 26, 2020), https://www.brookings.edu/blog/techtank/2020/10/26/how-the-2020-elections-will-shape-the-federal-privacy-debate/ [https://perma.cc/Y4VK-DZ59] ("The 116th Congress opened with great energy and promise for federal privacy legislation across both houses and parties [as exemplified by the introduction of COPRA and the SAFE DATA Act]."). For the direct text of the SAFE DATA Act, see Setting an American Framework to Ensure Data Access, Transparency and Accountability Act, S. 2499, 117th Cong., 1st Sess. (2021). For the direct text of COPRA, see Consumer Online Privacy Rights Act, S. 3195, 117th Cong., 1st Sess. (2021).

30. *See* S. 2499; S. 3195. COPRA preempts state laws that "directly conflict" with it and specifies that a state law providing greater protection is not in conflict, whereas the ADPPA preempts state laws covered by its provisions (even those that grant broader privacy rights). *See* Hunton Andrews Kurth, *House and Senate Release a Bipartisan U.S. Federal Privacy Bill*, NAT'L L. REV. (June 15, 2022), https://www.natlawreview.com/article/house-and-senate-release-bipartisan-us-federal-privacy-bill [https://perma.cc/5HN6-DCMN] (summarizing the similarities and differences between COPRA and the ADPPA).

passed in the Senate or the House of Representatives due to lawmakers' inability to agree on key provisions, and this reflects the general trend of Congress's inaction in the area of data privacy over the past two decades.[31]

After twenty years of partisan stalemate, lawmakers are particularly optimistic about the ADPPA because it compromises on two points that have historically precluded progress in the past: a private right of action and federal preemption.[32] The ADPPA provides a private right of action for individuals with limited rights to sue for monetary damages if a company violates the provisions of the statute.[33] The ADPPA also provides for federal preemption,[34] so it would control over all of the state privacy laws covered by its provisions, albeit with exceptions.[35]

---

31. *See* Rich, *supra* note 24 (noting twenty years have passed since the FTC initially called upon Congress to enact comprehensive data privacy legislation and Congress still has yet to do so). According to the author, the United States was once a leader on privacy due to its passage of the Privacy Act in the 1970s and certain "sector-specific privacy laws." *Id.* Recently, however, the United States "relinquished its leadership to Europe and California"—both of which have enacted robust data privacy laws in the Global Data Protection Regulation (GDPR) and the California Privacy Rights Act (CPRA). *Id. But see* Light, *supra* note 25, at 894 ("Even if these particular acts [SAFE DATA and COPRA] fail, their introduction alone suggests that hope is on the horizon that, if Congress is able to prioritize data privacy, federal legislation could be put in place during the Biden administration.").

32. *See* Johnathan M. Gaffney, Chris D. Linebaugh & Eric N. Holmes, *Overview of the American Data Privacy and Protection Act, H.R. 8152*, CONG. RSCH. SERV. 3 (Aug. 31, 2022), https://crsreports.congress.gov/product/pdf/LSB/LSB10776 [perma link unavailable] (recognizing how the ADPPA differs from other data privacy bills Congress introduced because it contains a private right of action and generally preempts state laws); *see also* Makena Kelly, *Congress Might Finally Have a Deal on Data Privacy*, THE VERGE (June 14, 2022, 1:41 PM), https://www.theverge.com/2022/6/14/23167705/data-privacy-legislation-bill-compromise-energy-commerce-cantwell-pallone [https://perma.cc/AY8P-DTPQ] (discussing the novelty of the ADPPA). Lawmakers have tried for decades to enact a comprehensive federal law to protect data privacy but "it has never survived the chaos of a deeply divided Congress." *Id.* Chairman Pallone is quoted stating: "This proposal is the first serious, bipartisan, bicameral, comprehensive national privacy bill that directly confronts the sticking points which derailed earlier efforts. . . . This legislation represents a fundamental shift in how data is collected, used, and transferred." *Id.*

33. *See* Lauren Henry Scholz, *Private Rights of Action in Privacy Law*, 63 WM. & MARY L. REV. 1639, 1653 (2022) (defining a private right of action as "one individual su[ing] another in court with a claim of right sounding in either statute or common law"). For further discussion of the ADPPA's private right of action, see *infra* Section V.B.

34. *See* Caleb Nelson, *Preemption*, 86 VA. L. REV. 225, 225–26 (2000) (defining preemption as "the extent to which a federal statute displaces (or 'preempts') state law"). Preemption is rooted in the Supremacy Clause of the United States Constitution, and "requires courts to ignore state law (but only if) state law contradicts a valid rule established by federal law, so that applying the state law would entail disregarding the valid federal rule." *Id.* at 234. For further discussion of the ADPPA's preemption provision, see *infra* Part IV.

35. *See* American Data Privacy and Protection Act, H.R. 8152, 117th Cong., 2d Sess. § 404(a) (2022). For a detailed list of the ADPPA's non-preempted laws, rules, regulations, and requirements, see *supra* note 21.

This Comment analyzes four factors that contributed to the dissolution of the longstanding partisan debate. Two factors reflect policy concerns and are discussed in Section A, and two factors reflect legislative deficiencies in the current system and are discussed in Section B.

A. *Bypassing the Firewall: Policy Considerations Behind the ADPPA*

Legislators introduced the ADPPA in June of 2022 because the lack of a comprehensive federal data privacy standard leaves American consumers and businesses vulnerable.[36] The sections discussed below reflect policy considerations that prompted lawmakers to take this significant step.[37] Section II.A.1 addresses the need to protect consumers' data privacy rights given the way businesses exploit such data for financial gain. Section II.A.2 then explains why companies are negatively impacted by the lack of comprehensive legislation.

1. *Consumers Need Data Privacy Protections*

Eighty-five percent of Americans access the internet every day, making their personal information ripe for abuse by businesses that rely on consumer data to sustain and grow their operating models.[38] In 2021

36. *See* Cristiano Lima, *House Panel Advances Major Privacy Bill, Striking a Long-Awaited Grand Bargain*, WASH. POST (July 20, 2022, 8:48 AM), https://www.washingtonpost.com/politics/2022/07/20/house-panel-set-advance-privacy-bill-striking-long-awaited-grand-bargain/ [https://perma.cc/88JL-ZT5X] (discussing policy considerations that led to the introduction of the ADPPA). Then-Ranking Member Rep. Cathy McMorris Rodgers stated: "The American Data Privacy and Protection Act's national standard is stronger than any state privacy law. . . . It prohibits Big Tech from tracking and exploiting people's sensitive information for profit without their consent, protects kids, and ensures small businesses can innovate." *Id.*

37. For further development of this argument, see *infra* Section II.A.1–2 (addressing lawmakers' rationales for prioritizing comprehensive federal data privacy legislation in 2022).

38. *See* Andrew Perrin & Sara Atske, *About Three-in-Ten U.S. Adults Say They Are 'Almost Constantly' Online*, PEW RSCH. CTR. (Mar. 26, 2021), https://www.pewresearch.org/fact-tank/2021/03/26/about-three-in-ten-u-s-adults-say-they-are-almost-constantly-online/ [https://perma.cc/TXJ9-7RT3] (reporting statistics about the frequency at which Americans use the internet on a daily basis); *see also* Freedman, *supra* note 10 (explaining why businesses collect consumer data).

alone, the FTC received 2.8 million claims of fraud, reporting $5.8 billion worth of loss by consumers.[39] This represents a seventy percent increase from the amount reported as lost in 2020.[40]

The growing rate at which individuals are losing control over their data is likely due in part to the way businesses collect it—either by directly asking consumers for information, indirectly tracking their online practices, or appending other sources of consumer data via third-party platforms.[41] When consumers are not asked for information, they are left with little control over how their data is collected and used.[42] When they are afforded some control (i.e., when they are asked for permission), it is often in the form of a dense and convoluted privacy policy that consumers seldom read.[43]

Facebook is one company that has been at the center of public scrutiny for its failure to protect consumer data.[44] In April 2021, hackers published the personal information of 533 million Facebook users, including their names, phone numbers, locations, birthdays, and email addresses.[45]

---

39. *See New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021*, *supra* note 4 (reporting more than $2.3 billion worth of losses in 2021 were due to imposter scams—up from $1.2 billion in 2020—while online shopping scams accounted for $392 million in reported losses—up from $246 million in 2020); *see also* Rabin, *supra* note 12, at 313, 315 (discussing the increasing number of Americans suffering from identity theft as a result of data breaches). Because of the threat of identity theft, many Americans are skeptical of sharing their data and consistently "replac[e] credit cards, clos[e] bank accounts, and obtain[ ] continuous credit monitoring." *Id.* at 315.

40. *See New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021*, *supra* note 4 (comparing how much money consumers lost to data fraud in 2020 versus in 2021).

41. *See* Freedman, *supra* note 10 (explaining the different ways businesses collect data). Most businesses utilize a software known as CRM (Customer Relationships Management) to manage customer interactions, which provides them with a centralized location to store, view, and organize customer information. *Id.* CRMs allow businesses to pull information from consumers and effectively hear what customers are saying about their products, services, methodologies, etc. *Id.*

42. *See* Timothy Morey, Theodore "Theo" Forbath & Allison Schoop, *Customer Data: Designing for Transparency and Trust*, HARV. BUS. REV. (May 2015), https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust [https://perma.cc/SXP3-YND9] (stating most companies are not transparent about their data practices because they "choose control over sharing," and tend to "ask for forgiveness [later] rather than permission [initially]"). In fact, many companies quietly collect personal data for which they have no immediate use, but which may be useful to them some day in the future. *Id.*

43. For a discussion of why privacy policies are often too convoluted for the layperson to understand, see Fowler, *supra* note 13 and accompanying text.

44. For a discussion of Facebook's involvement with consumer data privacy violations, see *infra* notes 45–48 and accompanying text. For a discussion of other large-scale, company-wide data breaches that have negatively impacted American consumers, see *infra* notes 52–54 and accompanying text.

45. *See* Aaron Holmes, *533 Million Facebook Users' Phone Numbers and Personal Data Have Been Leaked Online*, BUS. INSIDER (Apr. 3, 2021, 10:41 AM), https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4 [https://perma.cc/WSQ4-3G4N] (noting the Facebook breach impacted

Hackers allegedly obtained this data by breaching Facebook's contact importer in 2019.[46] Privacy experts expressed concern that cybercriminals will use the leaked data to impersonate consumers or scam them into providing login credentials.[47] Facebook also recently settled a class action lawsuit for $650 million in connection with its misuse of photo face-tagging and other biometric data without user consent.[48] Consumers accused Facebook of violating Illinois' Biometric Information Privacy Act (BIPA)—a strict liability statute requiring operators to obtain written consent before collecting, using, or storing users' biometric data.[49] Facebook reports having changed its photo face-tagging system since the incident, but the future potential harm to consumers cannot be undone.[50]

---

users from 106 countries, including over 32 million records from users in the United States, 11 million from users in the United Kingdom, and 6 million from users in India).

46. *See* Michael X. Heiligenstein, *Facebook Data Breaches: Full Timeline Through 2023*, FIREWALL TIMES (May 10, 2023), https://firewalltimes.com/facebook-data-breach-timeline/ [https://perma.cc/2K8S-XKZP] (claiming Facebook addressed the 2019 breach by fixing its contact importer, but decided not to notify the 530 million users whose information had been "scraped" by hackers).

47. *See id.*; *see also* Holmes, *supra* note 45 (explaining the implications of the Facebook breach). The author interviewed Alon Gal, the Chief Technology Officer of a cybercrime intelligence firm known as Hudson Rock, who discovered the leaked data from Facebook's breach. *Id.* Gal stated: "[a] database of that size containing the private information such as phone numbers of a lot of Facebook's users would certainly lead to bad actors taking advantage of the data to perform social-engineering attacks [or] hacking attempts." *Id.* (second alteration in original). For further discussion of why cybercriminals seek consumer data, see Romeo, *supra* note 11 and accompanying text.

48. *See* Robert Channick, *Nearly 1.3 Million Illinois Facebook Users Are Getting a Second Check from Last Year's $650 Million Biometric Privacy Settlement*, CHI. TRIB. (Mar. 6, 2023, 3:34 PM) https://www.chicagotribune.com/business/ct-biz-facebook-privacy-settlement-illinois-supplemental-payment-20230306-eku2fusjwzgx5i3w5grxai5xey-story.html [https://perma.cc/5QHS-VG6V] (stating Facebook users impacted by the company's data privacy violations will have received a total of $428 each from the two settlement fund payments).

49. *See* Patel v. Facebook, Inc., 932 F.3d 1264, 1268–69 (9th Cir. 2019) (discussing plaintiffs' claims against Facebook and explaining how Facebook violated BIPA). For the direct text of BIPA, see Illinois Biometric Information Privacy Act of 2008, 740 ILL. COMP. STAT. 14/15(a)–(b) (2022) (defining compliance obligations for operators using biometric data).

50. *See* Channick, *supra* note 48 (stating in November 2021, Facebook announced that it would "shut down its facial recognition system" and "put[ ] an end to the feature that automatically recognized if people's faces appear in memories, photos, or videos"). For a discussion of the harms consumers could face as a result of their data being exposed on the internet, see Rabin, *supra* note 12, at 315 (discussing the possibility of identity theft) and Kilovaty, *supra* note 4 (identifying the non-financial, psychological harms consumers may face after suffering a data breach).

2. *Businesses Support Federal Privacy Legislation*

Despite the role businesses play in exploiting consumer data, they too are susceptible to data privacy violations.[51] In September 2022, for example, Uber experienced a breach that compromised several of its internal systems, leading to widespread leakage of company data.[52] Crypto.com experienced a similar breach in January 2022, where perpetrators stole over $30 million in current cryptocurrency values from its consumers.[53] These large-scale breaches undoubtedly harmed the consumers whose digital assets and identities were ultimately compromised, and they also negatively impacted the businesses in terms of corporate reputation, consumer trust, and financial security.[54]

State governments responded with legislation; but with each law having its own regulatory requirements, businesses must comply with potentially fifty-plus different privacy frameworks—many of which are new and untested.[55] Companies find it challenging to apply the various state laws

51. *See* Rabin, *supra* note 12, at 314 (noting how corporations across all industries also face substantial costs from data breaches). In 2014, for example, over 85 million records were lost or stolen following data breaches, which costed companies approximately $145 per record. *Id.* *See also* Maria Henriquez, *$4.35 Million—The Average Cost of a Data Breach*, SECURITY (Oct. 17, 2022), https://www.securitymagazine.com/articles/98486-435-million-the-average-cost-of-a-data-breach [https://perma.cc/B4QW-QYAT] (highlighting the global average cost of a data breach, which "increased 2.6% from $4.24 million in 2021 to $4.35 million in 2022").

52. *See* Kate Conger & Kevin Roose, *Uber Investigating Breach of Its Computer Systems*, N.Y. TIMES (Sept. 15, 2022), https://www.nytimes.com/2022/09/15/technology/uber-hacking-breach.html [https://perma.cc/YFE5-W2KF] (reporting on the Uber data breach). Criminals hacked into Uber's network and "sent images of email, cloud storage and code repositories to cybersecurity researchers." *Id.* Importantly, this was not the first time hackers stole data from Uber. *Id.* In 2016, hackers stole information from 57 million Uber accounts and demanded $100,000 from Uber to delete copies of the data. *Id.* Uber ultimately paid the hackers but kept the breach confidential for over a year. *Id.*

53. *See* Anne Marie Lee, *Crypto.com Says Hackers Stole More Than $30 Million in Bitcoin and Ethereum*, CBS NEWS (Jan. 21, 2022, 7:37 AM), https://www.cbsnews.com/news/crypto-com-hack-bitcoin-ethereum-30-million/ [https://perma.cc/3FVC-F282] (stating hackers managed to "bypass [Crypto.com's] two-factor authentication system and withdraw the funds from 483 customer accounts").

54. *See id.* (claiming shares of Crypto.com reportedly fell more than six percent after news of the security breach became public); *see also* Conger & Roose, *supra* note 52 (examining the negative financial implications Uber faced following the 2022 data breach); Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL FOREIGN RELS. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/4ZPH-7BJQ] (identifying other large-scale data breaches that have left individuals "stymied" about how they can better protect their data). Namely, the 2017 Equifax data breach, Yahoo's admission that "billions of its email accounts were compromised," in 2013, and Deep Root Analytics' "accidental leak of personal details of nearly [200] million U.S. voters." *Id.*

55. *See* O'Connor, *supra* note 54 (explaining how state data privacy laws often have different and sometimes incompatible provisions regarding which categories

when a given data processing activity or the location of the individual could distinguish specific legal requirements.[56] This fragmented legal framework coupled with the regular addition of new and proposed legislation means that "staying up to date on the different requirements" and "updating privacy compliance activities in real time" has become a large part of privacy professionals' day-to-day work, according to Ms. Kim Gold, the Chief Privacy Officer at Genentech.[57]

Compliance is also costly.[58] The growing patchwork of state laws imposes duplicative costs on companies that have to update their operating models to comply with new requirements.[59] The aggregate cost of compliance with potentially fifty different laws could exceed $1 trillion over the next ten years, with at least $200 billion impacting small businesses.[60] Experts surmise that costs associated with compliance will serve as a determinative factor in how companies provide services and architect their systems

---

of personal information warrant protection, which entities are covered, and what warrants a data breach); *see also* Jamison, *supra* note 9, at 18 (arguing the "new and untested" nature of state data privacy laws places a substantial burden on companies by asking them to navigate different regulatory requirements and confront the potential technical errors or ambiguities they contain). Understanding "the meaning of a statute or regulation is time-consuming and one is still in some respects guessing as to how an agency or court will interpret it." *Id.* at 18–19.

56. *See* Gold, *supra* note 16 (noting that five states have comprehensive data privacy laws going into effect in 2023 which are all a bit different). Ms. Gold reported that many organizations are "finding the common threads and themes throughout the laws and applying them to all U.S. individuals." *Id.* Nevertheless, this still poses a challenge for businesses because privacy professionals must "think about whether on top of the different state laws, there are also other laws that may apply, such as sectoral laws, biometric data privacy laws, and [data] breach notification laws." *Id.*

57. *See id.* (anticipating the difficulties that will come with having to stay up to date with the different requirements and train an organization on compliance with privacy laws when the framework continues to change). Genentech is a large pharmaceutical company that is a member of the Roche Group, which reported revenues of $72 billion in 2021. *See* 2021 ANNUAL REPORT, ROCHE 134 (2021), Roche2021AnnualReport.pdf [https://perma.cc/CGY2-9X8L] (reporting 2021 revenue as $62.8 billion CHF (currency in Swiss Francs)).

58. For further discussion of the costs associated with compliance, see *infra* notes 59–61 and accompanying text.

59. *See* Daniel Castro, Luke Dascoli & Gillian Diebold, *The Looming Cost of a Patchwork of State Privacy Laws*, INFO. TECH. & INNOVATION FOUND. (Jan. 24, 2022), https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/ [https://perma.cc/Y6YG-TNXB] (highlighting extreme compliance costs as one of the primary reasons Congress needs to "move quickly" and create a national privacy framework that streamlines regulation, preempts state laws, establishes basic consumer data rights, and minimizes the impact on innovation).

60. *See id.* (estimating that in the absence of Congress passing comprehensive privacy legislation, state privacy laws could impose out-of-state costs of $98 billion annually on large businesses and $20–$30 billion annually on small businesses).

going forward.[61] It is the consumers, however, who bear the ultimate financial burden to fund corporate privacy programs since businesses may need to pass on the cost by raising prices for their products or services.[62]

Finally, the disparate state requirements and lack of a federal standard make it difficult for American companies to remain serious competitors in the global market.[63] Some commentators argue that the United States should adopt a national standard similar to that of Europe's General Data Privacy Regulation (GDPR)—the strongest privacy law in the world—because nearly all companies operating internationally already must comply with its requirements.[64] Even if American lawmakers do not exactly mirror the GDPR, a comprehensive standard of some sort is needed for the United States to maintain its dominant role in the international economy.[65]

---

61. *See* Zoom Interview with Matthew Berzok, Partner at the Rivendell Group, LLP (Oct. 18, 2022) (notes on file with author) (explaining that for many businesses, having to configure potentially fifty-plus different data privacy frameworks is expensive and often unworkable). The Rivendell Group, LLP is a law lobbying firm in Washington, D.C. that represents the 21st Century Privacy Coalition—a group of Internet Service Providers (ISPs) concerned about privacy legislation. *Id.* Members include AT&T, Comcast, Verizon, DirectTV, T-Mobile, etc. *Id.*

62. *See* Light, *supra* note 25, at 895 (predicting that consumers will bear the ultimate financial burden because businesses will likely need to raise costs so they can afford to implement new operating models that are compliant with state laws).

63. *See* Memorandum from H. Comm. on Energy & Com. Staff to Subcomm. Consumer Prot. & Com. Members & Staff (June 10, 2022), https://docs.house.gov/meetings/IF/IF17/20220614/114880/HHRG-117-IF17-20220614-SD002.pdf [https://perma.cc/ZVR2-XN34] [hereinafter *Energy & Com. Memorandum*] ("Unlike other global economic powers, such as the European Union and China, the United States does not have a comprehensive, national data privacy standard."); *see also* Jamison, *supra* note 9, at 3 (stating the United States must update its laws to avoid the risk of "limiting its access to markets where countries have modernized their privacy laws"). Although the United States is often looked upon as a global leader, the European Union is "leading the charge as to data privacy laws," and it would benefit the United States to enact a comprehensive standard that "could steer the international laws in a direction more desirable to [its] interests." *Id.* at 23.

64. *See, e.g.*, Souboti, *supra* note 14, at 550–51 (arguing a federal law similar to the GDPR would ease the compliance burden on American businesses that already must comply with the GDPR's more stringent requirements); Light, *supra* note 25, at 892 ("The United States needs nothing short of a federal equivalent of the GDPR."). For the direct text of Europe's General Data Protection Regulation, see Council Directive 2016/679, 2016 O.J. (L 119) (EU). *See also* Jan Philipp Albrecht, *How the GDPR Will Change the World*, 2 EUR. DATA PROT. L. REV. 287, 288 (2016) (identifying the GDPR's key provisions and predicting the impact they will have on an international scale). Key provisions include meaningful consumer consent, the right to data portability, standardized privacy icons, data protection impact assessments, and the appointment of data protection officers. *Id.*

65. *See* Light, *supra* note 25, at 895–96 (expressing concern that other countries are adopting privacy regimes like the GDPR while the United States is falling behind). Until the United States implements a federal regulation on par with the GDPR, its businesses will likely struggle to use data in accordance with international legal standards. *Id.* at 896. For a discussion of why the GDPR may not be

B. *An Unsecure Connection: Legislative Deficiencies Within the Current Regime*

In addition to the policy concerns prompting the introduction of the ADPPA, Congress sought federal data privacy legislation to address legislative deficiencies in the United States' current statutory framework.[66] Section II.B.1 below analyzes the United States as home to a mix of federal sectoral privacy laws that only protect certain types of data in limited circumstances. Section II.B.2 then examines the different state data privacy laws and their implications for consumers and businesses.

1. *The United States' Privacy Framework is Insufficient*

Unlike other countries' governing documents, the United States Constitution does not expressly recognize a right to privacy.[67] Instead, the right has been enumerated through U.S. Supreme Court decisions.[68] Within the context of data privacy specifically, Congress has generated a mix of federal laws designed to target certain types of data across different industries in special circumstances.[69]

---

the best model for the United States to follow, see *infra* Section V.A (discussing the GDPR's disadvantages).

66. *See* Gold, *supra* note 16 (explaining "the United States might be better served" by a single comprehensive law that regulates across all industries instead of generating a mix of state data privacy laws and federal privacy laws that are designed to protect certain types of data in limited instances).

67. *Compare EU Charter of Fundamental Rights*, Art. 7 & 8, EUR. UNION AGENCY FUNDAMENTAL RIGHTS, https://fra.europa.eu/en/eu-charter/article/7-respect-private-and-family-life [https://perma.cc/6EJD-JNEM] (last visited June 25, 2023) (expressly recognizing a right to privacy for all citizens of the European Union), *with* Griswold v. Connecticut, 381 U.S. 479, 482–85 (1965) (recognizing an implied right to privacy enshrined within the First, Third, Fourth, Fifth, and Ninth Amendments to the United States Constitution even though the Constitution itself does not mention the word "privacy").

68. *See, e.g.*, *Griswold*, 381 U.S. at 484 (holding that the different personal protections provided by the First, Third, Fourth, Fifth, and Ninth Amendments to the United States Constitution come together to create an implied right to privacy). "[S]pecific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance." *Id.* (citing Poe v. Ullman, 367 U.S. 497, 516–22 (Douglas, J., dissenting)). Through this analysis, the Court maintains that there is a "zone of privacy created by several fundamental constitutional guarantees." *Id.* at 485.

69. *See* Tyler J. Smith, *Haystack in a Hurricane: Mandated Disclosure and the Sectoral Approach to the Right to Privacy*, 37 Y. J. REG. BULLETIN 25, 30–31 (2019) (noting the insufficiencies within the federal sectoral nature of the United States' current data privacy regime, which includes laws targeting only specific industries or limited types of personal information). The author points to HIPAA and FERPA as two examples of laws generating confusion among consumers due to their significant overlap in the school setting. *Id.* at 31. *See also Energy & Com. Memorandum*, *supra* note 63 ("The United States . . . relies on sector-specific privacy-related federal statutes that establish varying degrees of protection, impose different collection and use limitations on various entities, and provide consumers with varying degrees of individual rights.").

The Gramm-Leach-Bliley Act (GLBA), for example, requires consumer financial services to divulge how they share and disclose data.[70] The Children's Online Privacy Protection Act (COPPA) imposes requirements on operators of websites or online services directed to children under the age of thirteen who know they are collecting personal information from children.[71] Moreover, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) created national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.[72]

Some commentators criticize these federal laws because they limit the FTC's ability to broadly protect data privacy due to their limited applicability and narrow scope.[73] The U.S. Supreme Court's 2016 decision in

70. *See generally* Gramm-Leach-Bliley Act, 16 C.F.R. pt. 314 (2023) (protecting consumer financial data). The GLBA limits when financial institutions can disclose a consumer's nonpublic personal information to nonaffiliated third parties. *See How to Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act*, FED. TRADE COMM'N (July 2002), https://www.ftc.gov [https://perma.cc/4R7C-UR89] (discussing GLBA compliance). The FTC requires financial institutions to notify customers about their information-sharing practices and inform them of their right to "opt-out" if they do not want their information to be shared with certain nonaffiliated third parties. *Id.*

71. *See generally* Children's Online Privacy Protection Act, 16 C.F.R. pt. 312 (2023) (imposing rules on businesses that collect, use, and store the personal data of children under the age of thirteen). COPPA requires operators of websites and online services to disclose exactly how data from children is collected and what it is used for, and to obtain parental consent prior to collecting personal information such as name, address, social security number, age, etc. from child users. *See Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, FED. TRADE COMM'N (June 2017), https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business [https://perma.cc/3BP9-5P92] (discussing COPPA compliance).

72. *See generally* Health Insurance Portability and Accountability Act of 1996, 45 C.F.R. pt. 160 (2023) (establishing standards for the protection of an individual's medical records or other personally identifiable health information). HIPAA's Privacy Rule applies to health plans and healthcare providers that conduct healthcare transactions electronically. *See The HIPAA Privacy Rule*, U.S. DEPT. HEALTH & HUM. SERVS. (Mar. 31, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/index.html [https://perma.cc/M9FL-5X2H] (discussing the national standards established by the HIPAA Privacy Rule). The Rule sets limits on how healthcare providers can use and disclose sensitive patient health information without an individual's authorization and provides individuals with certain rights over their information, such as examining copies of health records and requesting corrections. *Id.*

73. *See, e.g.*, Smith, *supra* note 69, at 30–31 (arguing the absence of national oversight and the isolated, sectoral approach to data privacy provides only "piecemeal" protection and leaves consumers "at the mercy of corporations who are constantly seeking new ways to profit"); Jason Heitz, Comment, *Federal Legislation Does Not Sufficiently Protect American Data Privacy*, 49 N. KY. L. REV. 287, 292–94 (2022) (criticizing the GLBA and COPPA as two examples of federal privacy statutes that target only certain types of data in limited circumstances, and thus fail to provide robust protections to consumers). *But see* Gold, *supra* note 16 ("[T]here might be instances where it does make sense to have enforcement ability vested in certain agencies for specific industries."). For example, Ms. Gold explained that the Food

Spokeo, Inc. v. Robins[74] complicates matters as well, making it more challenging for consumers to privately vindicate their data privacy rights.[75] There, the Court held that a "bare procedural violation" of the Fair Credit Reporting Act (FCRA) was insufficient to establish Article III standing, which requires a showing of a "concrete and particularized" and "actual or imminent" injury-in-fact.[76] In effect, *Spokeo* limits cybersecurity plaintiffs' chances of recovery because they often allege statutory violations of federal privacy law that are difficult to prove or quantify, and cite to the risk of real harm rather than to any tangible injury.[77]

The shortcomings of the current framework are further underscored by examining lower court decisions.[78] In *In re Google Inc. Cookie Placement Consumer Privacy Litigation* (*In re Google*),[79] Google allegedly deceived plaintiffs by placing cookies on their devices—text files containing small pieces of data that allow companies to monitor a user's web activity.[80] Because

---

and Drug Administration (FDA) or the U.S. Department of Health and Human Services (HHS) might continue to be in a good position to oversee certain privacy requirements pertaining to clinical trials or the use of health data. *Id.*

74. 136 S. Ct. 1540 (2016).

75. For further discussion of *Spokeo* and its impact on private rights of action in federal privacy statutes, see *infra* Section V.B.

76. *Spokeo*, 136 S. Ct. at 1548–49 (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)) (explaining why a statutory violation of the FCRA was insufficient to meet the demands of Article III standing). The Court explained:

> A violation of one of the FCRA's procedural requirements may result in no harm. For example, even if a consumer reporting agency fails to provide the required notice to a user of the agency's consumer information, that information regardless may be entirely accurate. In addition, not all inaccuracies cause harm or present any material risk of harm. An example that comes readily to mind is an incorrect zip code. It is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm.

Id. at 1550.

77. *See* Matthew S. DeLuca, Note, *The Hunt for Privacy Harms After Spokeo*, 86 FORDHAM L. REV. 2439, 2456–60 (2018) (analyzing the impact of the Supreme Court's concrete injury standard on plaintiffs bringing privacy and cyber claims by looking to several lower court decisions interpreting *Spokeo*); *see also* Jennifer V. Nguyen, Comment, *Standing as the Gatekeeper to Privacy Claims: Spokeo's Effect*, 22 INTELL. PROP. & TECH. L.J. 59, 64 (2018) (explaining how *Spokeo* is "particularly significant in privacy cases because injuries are difficult to prove and quantify, which is why Congress created statutory rights"). For further development of this argument, see *infra* Section V.B (discussing potential issues with the ADPPA's private right of action in light of the Supreme Court's *Spokeo* decision).

78. For further development of this argument, see *infra* notes 83–84, 87–88 and accompanying text.

79. 806 F.3d 125 (3d Cir. 2015).

80. *Id.* at 131 (explaining how cookies are used). The court stated:

> These third-party cookies are used by advertising companies to help create detailed profiles on individuals . . . by recording every communication request by that browser to sites that are participating in the ad network, including all search terms the user has entered. The information is sent to the companies and associated with unique cookies—that is how the tracking takes place. The cookie lets the tracker associate the web activity

the United States lacks a comprehensive data privacy law, plaintiffs were forced to sue under laws such as the Wiretap Act, the Stored Communications Act (SCA), and the Computer Fraud and Abuse Act (CAFAA)—none of which Congress intended to be internet data privacy statutes.[81] The United States Court of Appeals for the Third Circuit dismissed each of plaintiffs' federal claims, explaining first that Google did not violate the Wiretap Act because it was a "part[y] to any communications that [it] acquired," thus satisfying the statutory exception.[82] Similarly, Google did

> with a unique person using a unique browser on a device. Once the third-party cookie is placed in the browser, the next time the user goes to a website with the same [d]efendant's advertisements, a copy of that request can be associated with the unique third-party cookie previously placed. Thus the tracker can track the behavior of the user . . . .

Id. (alterations in original). According to plaintiffs, their web browsers included built-in features that prevented the installation of cookies by third-party servers, known as cookie blockers. *Id.* at 132. Some browsers featured an "opt-in" cookie blocker that the user could activate themselves, as plaintiffs did in this case, whereas others featured an "opt-out" cookie blocker that is activated by default. *Id.* Google's privacy policy acknowledged these cookie blockers, stating that "most browsers are initially set up to accept cookies, but you can reset your browser to refuse all cookies or to indicate when a cookie is being sent," which led plaintiffs to believe that Google was not tracking their activity after they opted to block the installation of cookies. *Id.*

81. *See id.* at 135–45, 145–49 (addressing each of plaintiffs' federal claims). For a discussion of congressional intent behind the Wiretap Act, see *Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act)*, U.S. DEPT. JUST., https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1284#vf4tzl [https://perma.cc/SPJ2-KTPW] (last visited June 25, 2023) (stating Congress passed the Wiretap Act due to extensive wiretapping by government agencies and private individuals without the consent of involved parties). For a discussion of congressional intent behind the SCA, see *Overview of Governmental Action Under the Stored Communications Act (SCA)*, CONG. RSCH. SERV. (Aug. 3, 2022), https://crsreports.congress.gov/product/pdf/LSB/LSB10801[perma link unavailable] (claiming Congress enacted the SCA to address government wiretaps and other communication tracing issues). For a discussion of congressional intent behind CAFAA, see *Cybercrime and the Law: Computer Fraud and Abuse Act (CAFAA) and the 116th Congress*, CONG. RSCH. SERV. (Sept. 21, 2020), https://crsreports.congress.gov/product/pdf/R/R46536 [perma link unavailable] (describing CAFAA as a broad statute intended to prohibit several categories of computer-related fraud, including unauthorized access to government computers).

82. *In re Google*, 806 F.3d at 135, 145 (explaining how to plead a prima facie case under the Wiretap Act). A plaintiff must show the defendant "(1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication, (5) using a device." *Id.* at 135 (quoting *In re* Pharmatrak, Inc. Priv. Litig., 329 F.3d 9, 18 (1st Cir. 2003)). The court noted one of several statutory exceptions to the Wiretap Act being 18 U.S.C. § 2511(2)(d), which "provides that, ordinarily, no cause of action will lie against a private person 'where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception.'" *Id.* (quoting 18 U.S.C. § 2511(2)(d) (2018)). The court agreed with defendants' contention that "they were the intended recipients of—and thus 'parties' to—any electronic transmissions that they acquired and tracked, and that . . . their conduct cannot have been unlawful under the statute." *Id.* at 140.

not violate the SCA because plaintiffs' personal computers are not "facilit[ies] through which . . . electronic communication[ ] service[s] [are] provided" as required by the statute.[83] Finally, the court determined that Google did not violate CAFAA because plaintiffs failed to plead sufficient facts demonstrating they suffered "damage or loss" within the meaning of the Act.[84]

One year later in *In re Nickelodeon Consumer Privacy Litigation* (*In re Nickelodeon*),[85] a case with similar facts, the Third Circuit again dismissed each of plaintiffs' federal claims.[86] There, the court concluded that defendant's placing of cookies on plaintiffs' computers did not violate the Wiretap Act and the SCA for the same reasons articulated in *In re Google*.[87] The

83. *Id.* at 145–46 (quoting *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 988 F. Supp. 2d 434, 446 (D. Del. 2013), *aff'd in part, vacated in part, remanded*, 806 F.3d 125 (3d Cir. 2015)) (explaining how to plead a prima facie case under the SCA). A plaintiff must show the defendant "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system." *Id.* (quoting 18 U.S.C. § 2701(a) (2018)). The court explained that "a home computer of an end user is not protected by the [Act]." *Id.* at 146 (alteration in original) (quoting Garcia v. City of Laredo, 702 F.3d 788, 793 (5th Cir. 2012)).

84. *Id.* at 148–49 (analyzing plaintiffs' CAFAA claim). CAFAA "creates a cause of action for persons 'who suffer[ ] damage or loss' because . . . a third party 'intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer.'" *Id.* at 148 (first and third alterations in original) (quoting 18 U.S.C. §§ 1030(a)(2)(C), (g) (2018)). Under the statute, "damage" constitutes "any impairment to the integrity or availability of data, a program, a system, or information." *Id.* (quoting 18 U.S.C. § 1030(e)(8) (2018)). Loss constitutes "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Id.* (quoting 18 U.S.C. § 1030(e)(11) (2018)). The Third Circuit acknowledged that defendants likely seized plaintiffs' internet data to use as a "marketable 'commodity,'" but maintained that there was incomplete evidence to find defendants ever participated in such a market or prevented plaintiffs from "capturing the full value of their internet usage information for themselves." *Id.* at 148–49.

85. 827 F.3d 262 (3d Cir. 2016).

86. *See id.* at 274–78, 295 (dismissing plaintiffs' claims under the Wiretap Act and the SCA). *But see* Heitz, *supra* note 73, at 299–301 (noting one significant difference between *In re Google* and *In re Nickelodeon* is that *In re Nickelodeon* involved tracking cookies placed on children's browsers, whereas *In re Google* did not). Although the children in *In re Nickelodeon* were under the age of thirteen, plaintiffs could not sue under COPPA because that statute does not allow for a private right of action, and the FTC did not bring an enforcement action on plaintiffs' behalf. *Id.* at 300. In *In re Google*, the FTC fined Google but none of the harmed individuals could personally recover under federal law. *Id.* at 299. The author uses both cases to illustrate the lack of protection consumers experience with respect to their data privacy. *Id.* at 299, 301.

87. *See In re Nickelodeon*, 827 F.3d at 274, 276–77. For a discussion of why the Third Circuit dismissed plaintiffs' claims under the Wiretap Act and the SCA in *In re Google*, see *supra* notes 82–83 and accompanying text.

Video Privacy Protection Act (VPPA) also offered plaintiffs no relief, as the personally identifiable information (PII) disclosed by defendants did not coincide with the statute's definition of PII.[88]

The Ninth Circuit took a slightly different approach to the adjudication of data privacy violations in *In re Facebook, Inc. Internet Tracking Litigation* (*In re Facebook*),[89] by adopting a broader reading of the Wiretap Act than the Third Circuit.[90] According to the court, simultaneous, unknown duplication and forwarding of GET requests[91] made to a web page's server

88. *See In re Nickelodeon*, 827 F.3d at 278–90 (discussing the VPPA claim). Defendants disclosed plaintiffs' internet protocol (IP) addresses, browser fingerprints, and unique device identifiers. *Id.* at 282. A browser fingerprint is a composition of a user's browser and operating system settings, and a unique device identifier is "a 64-bit number (hex string) that is randomly generated when a user initially sets up his device and should remain constant for the lifetime of the user's device." *Id.* at 282 n.124 (quoting Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1254 (11th Cir. 2015)). To state a claim under the VPPA, "a plaintiff must allege that '[a] video tape service provider . . . knowingly disclose[d], to any person, personally identifiable information concerning any consumer of such provider.'" *Id.* at 279 (alterations in original) (quoting 18 U.S.C. § 2710(b)(1) (2018)). The Third Circuit determined that Congress did not intend for the statute to be so broad as to cover all aspects of consumer privacy, "even as video-watching technology changed over time" and dismissed plaintiffs' claim on that ground. *Id.* at 285.

89. 956 F.3d 589 (9th Cir. 2020), *cert. denied*, *sub nom.* Facebook, Inc. v. Davis, 141 S. Ct. 1684 (2021).

90. *See id.* at 607–08 (rejecting the Third Circuit's narrow interpretation of the Wiretap Act in *In re Google* and *In re Nickelodeon* and adopting the First and Seventh Circuits' approach that the Act is to be interpreted more broadly). The court explained:

> We adopt the First and Seventh Circuits' understanding that simultaneous, unknown duplication and communication of GET requests do not exempt a defendant from liability under the party exception. As we have previously held, the "paramount objective of the [Electronic Communications Privacy Act, which amended the Wiretap Act] is to protect effectively the privacy of communications." We also recognize that the Wiretap Act's legislative history evidences Congress's intent to prevent the acquisition of the contents of a message by an unauthorized third-party or "an unseen auditor."

Id. at 608 (alterations in original) (first quoting Joffe v. Google, 746 F.3d 920, 931 (9th Cir. 2013); then quoting S. REP. NO. 90-1097, at 2154 (1968)). The court also sustained plaintiffs' claims under the California Invasion of Privacy Act (CIPA) and under state law claims, including invasion of privacy, intrusion upon seclusion, breach of contract, and breach of the implied covenant of good faith and fair dealing. *Id.* at 601, 608.

91. *See id.* at 607 (explaining what GET requests are and how Facebook used them). "The GET request serves two purposes: it first tells the website what information is being requested and then instructs the website to send the information back to the user. The GET request also transmits a referrer header containing the personally-identifiable URL information." *Id.* This communication usually "occurs only between the user's web browser and the third-party website." *Id.* Websites with Facebook plug-ins, however, have a code that "directs the user's browser to copy the referrer header from the GET request and then send a separate but identical GET request and its associated referrer header to Facebook's server." *Id.* Through this duplication and collection of GET requests, Facebook can compile individuals' browsing histories and sell such data to third-party services. *Id.*

did not qualify for the party exception under the Wiretap Act.[92] The court explained that allowing a company to engage in the unauthorized duplication and forwarding of users' information would result in broad intrusion into consumers' personal data and "allow[ ] the exception to swallow the rule."[93] The court also dismissed plaintiffs' SCA claim but for a different reason than the Third Circuit; the GET requests did not fall within the statute's definition of "electronic storage."[94]

Taken together, these federal statutes and cases exemplify how the United States' "piecemeal" approach to regulating data privacy is inadequate and leaves consumers susceptible to exploitation without proper relief.[95] Instead of providing robust privacy protections through one comprehensive law, consumers must either wait for the FTC to act on their behalf or vindicate their rights privately under narrow statutes with limited scopes enacted by a Congress that had other objectives in mind.[96]

2. *The Recent Proliferation of State Laws Has Proven to be Problematic*

Finally, the growing patchwork of state laws is not an efficient long-term solution to this problem.[97] Shortly after Europe implemented the GDPR, California was the first state to enact comprehensive data privacy

92. *See id.* at 607–08. For further discussion of the *In re Facebook* court's rationale under the Wiretap Act, see *supra* note 90 and accompanying text.

93. *In re Facebook*, 956 F.3d at 608 (summarizing the court's reasoning).

94. *Id.* at 608–10 (defining "electronic storage" as "temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" (quoting 18 U.S.C. § 2510(17) (2018))). Plaintiffs argued their browsers stored a copy of the URL requests in the toolbar while they remained present at a particular webpage, making this storage incidental to the electronic communication. *Id.* at 608. Once "the user hits the Enter button or clicks on a link, the communication is in the process of being sent and received between the user and the first-party website." *Id.* The court rejected this argument, explaining that "[t]he communications in question—the GET requests themselves—are not the communications stored in the user's toolbar." *Id.* at 609. Rather, the requests are sent directly between the user and the third-party website, and the "text displayed in the toolbar serves only as a visual indication . . . of the location of their browser." *Id.*

95. *See* Heitz, *supra* note 73, at 299 ("If users cannot prevent advertising companies from installing tracking cookies on their browsers under federal law, federal law and the notice and choice framework do not sufficiently protect Americans' data privacy."). Heitz highlights *In re Nickelodeon* and *In re Google* as two cases that demonstrate the United States' failure to provide a robust data protection regime. *Id.* at 288–301. *See also* Smith, *supra* note 69, at 30–31 (explaining why the federal sectoral approach to data privacy falls short and proves to be confusing for consumers).

96. *See* Smith, *supra* note 69, at 30 (criticizing the United States' piecemeal approach to data privacy and lack of national oversight). For a discussion of Congress's objectives behind the Wiretap Act, the SCA, and CAFAA see *supra* note 81. For a discussion of where the FTC did not intervene on plaintiffs' behalf and plaintiffs had no option to privately vindicate their data privacy rights, see *supra* note 86 (discussing *In re Nickelodeon* and plaintiffs' inability to recover under COPPA).

97. *See* Light, *supra* note 25, at 876 (claiming the United States needs a solution that will have lasting effects, such as a comprehensive federal privacy law to

legislation via the California Consumer Privacy Act of 2018 (CCPA).[98] Shortly thereafter, California amended the CCPA with the California Privacy Rights Act of 2020 (CPRA), which, among other things, extends broad data privacy protections to employees, job applicants, and independent contractors.[99] Notably, the CPRA creates a comprehensive regime similar to that of Europe's GDPR.[100]

In 2021 and 2022, four states followed California's lead in passing data privacy legislation, including Colorado, Virginia, Utah, and Connecticut.[101] Colorado, Virginia, and Connecticut achieved a comprehensive framework similar to that of California's, whereas Utah's law is more cir-

---

protect consumers from data breaches). Although the United States has only just begun to develop "cursory [privacy] regulations at the state level," which share a similar goal of protecting individual privacy, they are not uniform and thus do not offer the extensive protections that other countries are developing around the world. *Id.*

98. *See generally* CAL. CIV. CODE §§ 1798.100–.199.100 (West 2022) (enacting the California Consumer Privacy Act of 2018 and providing consumers with more control over their personal data); *see also* Alexandra Henry, Comment, *The California Consumer Privacy Act's Potential Incompatibility with the United States' Legal and Economic Landscape*, 23 SMU SCI. & TECH. L. REV. 227, 227 (2020) (claiming the CCPA is similar to the GDPR because it offers some of the most stringent data privacy protections for its residents and permits users to request deletion of their data).

99. *See generally* CAL. CIV. CODE § 1798.199.10 (West 2022) (amending the CCPA with the California Privacy Rights Act of 2020). The CPRA is known for establishing the California Privacy Protection Agency, "which is vested with full administrative power, authority, and jurisdiction to implement and enforce the California Consumer Privacy Act of 2018." *Id. See also* Hannah Beppel, *Everything You Need to Know About the California Privacy Rights Act*, ADP, https://www.adp.com/spark/articles/2022/10/everything-you-need-to-know-about-the-california-privacy-rights-act.aspx [https://perma.cc/V9DX-XNYG] (last visited June 25, 2023) (noting the CPRA applies to organizations that have even one employee working in California—either in person or remotely—even if the organization itself is not based in the state). The law, however, does not apply to employees working outside the state of California. *Id.*

100. *See* JEFFERY DENNIS & KYLE JANECEK, NEWMEYER & DILLON LLP, IANA GAYTANDJIEVA, ANGELA POTTER, EDIDIONG UDOH, ALEXANDER FETANI, MARCELLO FERRARESI & VICTORIA PRESCOTT, ONETRUSTDATAGUIDANCE, COMPARING PRIVACY LAWS: GDPR V. CCPA & CPRA, 12–22 (2022), https://www.dataguidance.com/sites/default/files/gdpr_v_ccpa_and_cpra_v6.pdf [https://perma.cc/8H5T-V5U6] (noting that the GDPR and CPRA have similar definitional provisions, in that both inform consumers of their right to opt-in or opt-out of the erasure, collection, sale, or disclosure of their personal data). While the similarities are expansive, the laws diverge over the scope of their application, provisions surrounding limitations on the collection of personal information, and on certain obligations, such as accountability. *Id.* at 7–10. For a discussion of the GDPR's key provisions, see Albrecht, *supra* note 64 and accompanying text.

101. *See generally* Colorado Privacy Act, S.B. 21-190, 74th Gen. Assemb., Reg. Sess. (Colo. 2021) (effective July 1, 2023); Virginia Consumer Data Protection Act, S.B. 1392, 2021 Gen. Assemb., Reg. Sess. (Va. 2021) (effective Jan. 1, 2023); Utah Consumer Privacy Act, S.B. 227, 2022 Gen. Assemb., Reg. Sess. (Utah 2022) (effective Dec. 31, 2023); Connecticut Data Privacy Act, S.B. 6, 2022 Gen. Assemb., Reg. Sess. (Ct. 2022) (effective July 1, 2023); *see also* Anokhy Desai, *US State Privacy Legislation Tracker*, INT'L ASSOC. PRIV. PRO. (June 9, 2023), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ [https://perma.cc/3R5X-RJS8] (high-

cumscribed.[102] Utah opted for a narrower definition of personal information and implemented a higher threshold for determining when businesses are subject to compliance.[103] The CPRA still provides the broadest consumer data protections and continues to pave the way for other states, but it too falls short; the CPRA lacks protections against targeted advertising and profiling, which the other four state laws contain.[104] As commentators note, this disparate state framework will likely lead to a "compliance nightmare," with small businesses suffering the

lighting Iowa, Tennessee, Indiana, and Montana as several states where comprehensive data privacy laws will go into effect between 2024 and 2026).

102. *See Comparing U.S. State Data Privacy Laws vs. the EU's GDPR*, BLOOMBERG L. (May 3, 2023), https://pro.bloomberglaw.com/brief/data-privacy-laws-in-the-us/ [https://perma.cc/J2WB-XXL5] (highlighting the differences between the Colorado Privacy Act, the Virginia Consumer Data Protection Act, the California Consumer Privacy Act of 2018, the California Privacy Rights Act of 2020, and the GDPR); *see also* Alan R. Friedman, Robin Wilcox & Austin Manes, *Comparing the 5 Comprehensive Privacy Laws Passed by US States*, KRAMER LEVIN (June 10, 2022), https://www.kramerlevin.com/en/perspectives-search/comparing-the-5-comprehensive-privacy-laws-passed-by-us-states.html [https://perma.cc/GRC8-3HTD] (stating California has the "broadest consumer rights" but lacks protections the other four states have adopted). Utah's law in particular is more tailored than the laws of the four other states. *Id.* In addition, the Connecticut law almost explicitly adopts large portions of the Colorado and Virginia laws, including "the definition of personal data, how to process sensitive personal data and when to perform data protection impact assessments." *Id.*

103. *See* Friedman, Wilcox & Manes, *supra* note 102 (highlighting the differences between Utah's law and the CPRA with respect to business compliance). The CPRA applies to businesses that have $25 million annual in gross revenue or process the data of at least 100,000 consumers or derive at least fifty percent of revenue from selling or sharing data. *Id.* Utah's law applies to businesses that have $25 million in annual gross revenue and process the data of at least 100,000 consumers or process the data of at least 25,000 consumers and derive at least fifty percent of gross revenues from selling personal data. *Id.* Notice how Utah's law encompasses additional requirements and is structured conjunctively, whereas the CPRA is disjunctive. *Id.* Utah's law also does not offer consumers the right to correct personal data that companies have collected from them, unlike the statutes of the other four states. *Id.*

104. *See id.* (identifying differences between California's law and those of the other four states). According to the authors, notable differences include California's lack of restrictions on profiling and the impact of the law due to its large state population; California's statute applies to 40 million residents, while Utah and Virginia's statutes apply to only 3 million residents. *Id. See also* Myriah V. Jaworski & Paul F. Schmeltzer, *An Enterprise-Wide Data Privacy Solution to the State Privacy Law Problem*, SHRM (Nov. 2, 2022), https://www.shrm.org/resourcesandtools/legal-and-compliance/state-and-local-updates/pages/state-data-privacy-laws.aspx [https://perma.cc/85DB-TNAY] (highlighting additional differences between the five laws). In Colorado and California, for example, businesses must honor consumer cookie preferences set through browser settings as part of an "opt-out" of targeted advertising and the sale of consumer information. *Id.*

most.[105] It also makes it inherently confusing for consumers to understand their data privacy rights—especially those who live and work between states.[106]

III. CRACKING THE CODE: THE AMERICAN DATA PRIVACY AND PROTECTION ACT

In response to consumer needs and business challenges, the House Energy and Commerce Committee introduced the ADPPA in June of 2022.[107] The bill applies to "covered entit[ies]," meaning any entity or person that "collect[s], process[es], or transfer[s] covered data."[108] Congress defines "covered data" as "information that identifies or is linked or reasonably linkable . . . to an individual or a device," such as cookies or IP addresses.[109] Congress even delineated a subsection of "sensitive covered

105. *See* Light, *supra* note 25, at 876 (explaining how it is often not feasible for small businesses with less money and resources to comply with the influx of new state data privacy requirements in comparison to larger businesses, since state-by-state compliance can be extremely costly and complex). Instead, small businesses may attempt to comply by "pick[ing] the most comprehensive [law] and devot[ing] their resources to complying with that one." *Id.* at 888.

106. *See* Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, N.Y. TIMES (Sept. 6, 2021), https://www.nytimes.com [https://perma.cc/LT6L-FU2Q] (noting that the risk of too many state laws with different requirements will generate confusion among consumers). In addition to the federal laws and varying state laws, the author highlights how some state-level laws even "carve out coverage of individual aspects of data privacy," including Illinois' BIPA. *Id.* For further discussion of BIPA and its requirements, see *supra* note 49 and accompanying text.

107. *See generally* American Data Privacy and Protection Act, H.R. 8152, 117th Cong., 2d Sess. (2022) (introducing a new robust data privacy regime for the United States); *see also* House Energy and Commerce Committee Chair Cathy McMorris Rodgers, *supra* note 17 (discussing the novelty of the ADPPA as compared to Congress's past efforts to enact comprehensive federal data privacy legislation).

108. *See* H.R. 8152 § 2(9)(a)(i) (clarifying the meaning of "covered entity"). The term does not include "a governmental entity such as a body, authority, board, bureau, commission, district, agency, or political subdivision of the Federal Government or a State, Tribal, territorial, or local government," nor a "person or an entity that is collecting, processing, or transferring covered data on behalf of a Federal, State, Tribal, territorial, or local government entity." *Id.* §§ 2(9)(B)(i)–(ii). The ADPPA also identifies a subset of "large data holder[s]," which includes:

> [C]overed entit[ies] or service provider[s] that, in the most recent calendar year[,] (i) had annual gross revenues of $250,000,000 or more; (ii) and collected, processed, or transferred—(I) the covered data of more than 5,000,000 individuals or devices that identify or are linked or reasonably linkable to 1 or more individuals . . . and (II) the sensitive covered data of more than 200,000 individuals or devices that identify or are linked or reasonably linkable to 1 or more individuals.

Id. §§ 21(A)(i)–(ii).

109. *Id.* §§ 8(A)–(B) (defining "covered data" and highlighting exclusions). Exclusions include: "(i) de-identified data; (ii) employee data; (iii) publicly available information; or (iv) inferences made exclusively from multiple independent

data" under which specific rules apply for certain types of personal information, including Social Security numbers, credit card numbers, precise geolocation information, etc.[110]

Covered entities may not "collect, process, or transfer covered data" except where necessary to "maintain a specific product or service requested by the individual to whom the data pertains," and may not transfer such data without the individual's affirmative express consent (i.e., opting-in).[111] Covered entities are further prohibited from transferring covered data beyond what is "reasonably necessary," and must disclose what data they collect, what they use it for, and how long they retain it.[112] Finally, covered entities are prohibited from utilizing covered data in a manner that discriminates "on the basis of race, color, religion, national origin, sex, or disability."[113]

---

sources of publicly available information that do not reveal sensitive covered data with respect to an individual." *Id.* §§ (B)(i)–(iv).

110. *Id.* §§ 28(A)(i), (iii), (vi) (outlining provisions applicable to sensitive covered data); *see also* Christian Tamotsu Fjeld & Cynthia Larose, *Understanding the American Data Privacy and Protection Act*, ML STRATEGIES (June 8, 2022), https://www.mlstrategies.com/insights-center/viewpoints/53931/2022-06-08-understanding-american-data-privacy-and-protection-act#scope [https://perma.cc/FF6X-KBQT] (explaining the bill also covers "sensitive covered data"). Sensitive covered data protects digital markets, including drivers' license numbers and categories of health, geolocation, financial, log-in, racial and sexual information, private communications, personal digital media, and web-browsing activity. *Id.* The ADPPA permits the FTC to add additional categories of data to this definition through the rulemaking procedures of the Administrative Procedures Act (APA). *Id.*

111. *See* H.R. 8152 § 101(a)(1) (noting other permissible circumstances where covered entities can transfer data); *see also id.* § 2(1)(A) (defining "affirmative express consent"). "The term 'affirmative express consent' means an affirmative act by an individual that clearly communicates the individual's freely given, specific, and unambiguous authorization for an act or practice after having been informed, in response to a specific request from a covered entity that meets the requirements of subparagraph (B)." *Id.*

112. *Id.* §§ 101(a)–(b), 103(a) (explaining how covered entities can collect data). "A covered entity may not collect, process, or transfer covered data unless the collection, processing, or transfer is limited to what is reasonably necessary and proportionate . . . ." *Id.* § 101(a). This provision is known as "privacy by design" or "data minimization," and is novel to the comprehensive data privacy law debate in the United States. *See* Berzok, *supra* note 61 (discussing the concept of privacy by design). Mr. Berzok stated:

> The whole bill [the ADPPA] is architected on the idea that companies should not gather, store, or really use information about consumers that they do not need. Companies should really only be collecting the information they need to provide their services. This has been part of previous discussions, but has never been a main pillar of the bill like it is with the ADPPA.

Id. Even if the ADPPA is not passed, Mr. Berzok surmises that privacy by design will be a key part of future bills. *Id.*

113. *See* H.R. 8152 § 207(a)(1) (outlining requirements for the protection of civil rights); *see also* Stacey Gray, *The Bipartisan House Privacy Bill Would Surpass State Protections*, LAWFARE (July 21, 2022, 8:54 AM), https://www.lawfareblog.com/bipartisan-house-privacy-bill-would-surpass-state-protections [https://perma.cc/MKQ6-CFKE] (describing the ADPPA's civil rights provision as "groundbreaking"). Un-

The bill also, for the first time, provides consumers with the right to access, correct, and delete their data and object before it is transferred to a third party or subjects them to targeted advertising (i.e., opting-out).[114] Congress tasked the FTC with enforcement and directed the agency to issue regulations elaborating on certain provisions, including that covered entities adopt reasonable security practices depending on their size to avoid future data breaches.[115]

One of the most notable aspects of the ADPPA is its preemption provision.[116] The bill would preempt any law, regulation, rule, standard, or requirement of any state that is covered by a subdivision of the Act, but expressly carves out nineteen exceptions.[117] According to the U.S. Supreme Court, there are generally two ways a preemption provision might be drafted.[118] Federal law can either expressly preempt state law by containing explicit preemptive language, or impliedly preempt state law when

---

like the current framework of state data privacy laws, which do not directly address data-driven discrimination, the ADPPA would expand civil rights protections by "prohibiting direct and indirect algorithmic discrimination affecting housing, employment, financial, and similar opportunities; addressing racial and other discrimination in online spaces, such as price discrimination, that is already illegal in offline spaces." *Id.*

114. *See* H.R. 8152 § 203(b) (including a provision for "Individual Autonomy"). Section 203(a) provides that covered entities, upon receiving a "verified request from the individual," must abide by the individual's decision to access, correct, delete, or export their data to another covered entity. *See id.* §§ 203(a)(1)–(4).

115. *See* Federal Trade Commission Act, 15 U.S.C. § 45(a)(2) (2018) (granting the FTC authority to prevent "unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce"); *see also* H.R. 8152 § 402 (noting state attorney generals and state privacy authorities also enjoy enforcement power). Such authorities may bring actions on behalf of their residents to enjoin the violative practice, enforce compliance with the ADPPA or its implementing regulations, obtain damages, civil penalties, restitution, or other compensation, and recover reasonable attorney's fees and other litigation costs reasonably incurred. *Id.* §§ 402(a)(1)–(4). *See also id.* §§ 208(a)(1)–(2)(A) (specifying minimum requirements for data security practices that covered entities must follow based on their "size and complexity"). These include an assessment of vulnerability, preventive and corrective action, evaluation of preventive and corrective action, information retention and disposal, training, designation, and incident response. *Id.* §§ 208(b)(1)–(7).

116. *See* Kelly, *supra* note 32 and accompanying text (discussing the novelty of the ADPPA because of its preemptive power).

117. For the direct text of the ADPPA's preemption provision, see *supra* note 21 (clarifying that no state shall adopt any law covered by the provisions of the ADPPA and outlining the exceptions).

118. *See* Bryan L. Adkins, Alexander H. Pepper & Jay B. Sykes, *Federal Preemption: A Legal Primer*, CONG. RSCH. SERV. 2 (May 18, 2023) (citing Gade v. Nat'l Solid Wastes Mgmt. Ass'n, 505 U.S. 88, 98 (1992)), https://sgp.fas.org/crs/misc/R45825.pdf [https://perma.cc/G8T7-3RLC] (explaining the two ways that federal law can preempt state law). For further discussion of the Court's preemption jurisprudence, see *infra* notes 119 and 121 and accompanying text.

its structure and purpose implicitly reflect Congress's preemptive intent.[119] Under Section 404, it is clear that Congress drafted the ADPPA to include express preemptive language.[120]

The Court generally recognizes four subcategories of express preemption, but only one is relevant to the ADPPA—"covering" preemption.[121] In *CSX Transportation, Inc. v. Easterwood*,[122] the Court concluded that "covering" preemption is "more restrictive," and preemption "will lie only if the federal regulations substantially subsume the subject matter of the relevant state law."[123] Although the Court applied the "presumption against preemption" in its analysis, its modern jurisprudence seems to do away with that and focuses on congressional intent as the "ultimate touchstone" of every express preemption case, which the Court evaluates by looking to the statute's plain text.[124]

---

119. *See* Adkins, Pepper & Sykes, *supra* note 118, at 2 (differentiating between implied and express preemption). The Court has identified two subcategories of implied preemption; the first is field preemption—where federal law so extensively regulates an activity as to support the inference that Congress intended to leave no room for additional state regulation. *Id.* The second is conflict preemption, which "occurs when compliance with both federal and state regulations is impossible (impossibility preemption) or when state law poses an 'obstacle' to the accomplishment of the 'full purposes and objectives' of Congress (obstacle preemption)." *Id.* (footnote omitted) (first citing Fla. Lime & Avocado Growers, Inc. v. Paul, 373 U.S. 132, 142–43 (1963); then quoting Hines v. Davidowitz, 312 U.S. 52, 67 (1941)).

120. For the direct text of the ADPPA's express "covering" preemption provision, see *supra* note 21. *See also Hearing on ADPPA*, *supra* note 23, at 127 (statement of Rep. Kathy Castor) ("[I]n this bill we use covering preemption, so when state laws aren't substantially subsumed by Federal law they won't be preempted.").

121. *See* Adkins, Pepper & Sykes, *supra* note 118, at 6 (identifying four subsets of explicit preemption).

> The Supreme Court has interpreted federal statutes that expressly preempt (1) state laws "related to" certain subjects, (2) state laws concerning certain subjects "covered" by federal laws and regulations, (3) state requirements that are "in addition to, or different than" federal requirements, and (4) state "requirements," "laws," "regulations," and "standards."

Id.

122. 507 U.S. 658 (1993).

123. *Id.* at 662, 664 (interpreting a preemption clause within the Federal Railroad Safety Act as allowing states to enact laws related to railroad safety until the federal government adopted regulations "covering the subject matter" of such laws). The Court clarified that "[t]o prevail on the claim that the regulations have pre-emptive effect, petitioner must establish more than that they 'touch upon' or 'relate to' that subject matter . . . for 'covering' is a more restrictive term." *Id.* at 664 (citation omitted). *See also* MD Mall Assocs., LLC v. CSX Transp., Inc., 715 F.3d 479, 490–91, 495 (3d Cir. 2013), *as amended* (May 30, 2013) (holding that the Federal Railroad Safety Act's express preemption provision was not "covering" because the fact that a regulation "involves" the same general topic contemplated by state law does not mean it "covers" it). "[A] federal law does not preempt state laws where the activity regulated by the state is merely a peripheral concern of the federal law . . . ." *Id.* at 489 (alterations in original) (quoting N.Y. Susquehanna & W. Ry. Corp. v. Jackson, 500 F.3d 238, 252 (3d Cir. 2007)).

124. *See* Adkins, Pepper & Sykes, *supra* note 118, at 4–5 (analyzing trends within the Court's preemption jurisprudence). *Compare* Wyeth v. Levine, 555 U.S.

Finally, the ADPPA calls for a private right of action.[125] In addition to enforcement by the FTC, state attorney generals, and the California Privacy Protection Agency (CPPA), individuals may file lawsuits in federal court and obtain compensatory damages, injunctive or declaratory relief, and reasonable attorneys' fees and litigations costs.[126] By including a private right of action, the ADPPA joins the current trend of federal data privacy laws providing for individual lawsuits.[127]

555, 565, 575 (2009) (discussing the "two cornerstones" of the Court's preemption jurisprudence as "the purpose of Congress" and the "assumption that the historic police powers of the States were not to be superseded by the Federal Act unless that was the clear and manifest purpose of Congress [i.e., the presumption against pre-emption]" (quoting Medtronic, Inc. v. Lohr, 518 U.S. 470, 485 (1996))), *and* Altria Grp., Inc. v. Good, 555 U.S. 70, 76 (2008) ("If a federal law contains an express pre-emption clause, it does not immediately end the inquiry because the question of the substance and scope of Congress' displacement of state law still remains."), *with* Puerto Rico v. Franklin Cal. Tax-Free Tr., 579 U.S. 115, 125 (2016) (holding that where a "statute 'contains an express pre-emption clause,' we do not invoke any presumption against pre-emption but instead 'focus on the plain wording of the clause, which necessarily contains the best evidence of Congress' pre-emptive intent'" (quoting Chamber of Com. v. Whiting, 563 U.S. 582, 594 (2011))). The Court regularly applied the presumption against preemption in the 1980s–early 2000s, but has not invoked it recently in express preemption cases and instead follows its holding in *Puerto Rico*. *See* Adkins, Pepper & Sykes, *supra* note 118, at 3–4.

125. *See* American Data Privacy and Protection Act, H.R. 8152, 117th Cong., 2d Sess. § 403 (2022) (outlining the ADPPA's private enforcement provision). The provision grants enforcement to "persons" who have experienced violations of the Act by a covered entity or service provider and permits them to bring a civil action against such entity "in any Federal court of competent jurisdiction." *Id.* § 403(a)(1). Enforcement rights are also granted to the Commission (FTC) and state attorney generals. *Id.* § 403(a)(3). Finally, the CPPA is granted enforcement authority "in the same manner, it would otherwise enforce the California Consumer Privacy Act, Section 1798.1050 et. seq." *Id.* § 404(b)(3).

126. *See id.* § 403 (outlining different elements of the private right of action). Prior to bringing suit, for example, individuals must notify the FTC and their state attorney general in writing of their desire to initiate a civil action. *Id.* § 403(a)(3)(A). The FTC and state attorney general then have sixty days to determine whether they will independently intervene and take action. *Id.* Individuals must also provide covered entities with forty-five days to cure the alleged violation. *Id.* § 403(c)(1)(B). If, within forty-five days, the covered entity cures the violation and provides the individual with written notice that the violation has been cured and that no further violations will occur, the action may be dismissed. *Id.* § 403(c)(2).

127. *See* Cameron F. Kerry & John B. Morris, *In Privacy Legislation, A Private Right of Action is Not an All-or-Nothing Proposition*, BROOKINGS INST. (July 7, 2020), https://www.brookings.edu/blog/techtank/2020/07/07/in-privacy-legislation-a-private-right-of-action-is-not-an-all-or-nothing-proposition/ [https://perma.cc/W89Q-X5AX] ("[F]ederal privacy legislation [is] unlikely to pass without a private right of action in some form . . . ."). The authors point out that the "progenitor of federal privacy laws," the Fair Credit Reporting Act (FCRA), included a private right of action for individuals to recover for actual damages, punitive damages in cases of willful or intentional violations, and reasonable attorney's fees. *Id.* The FCRA's progeny—the Privacy Act, the Electronic Communications Privacy Act, the Video Privacy Protection Act, and the Telephone Consumer Protection Act (TCPA)—allow for private lawsuits in various ways. *Id.*

IV. HACKING INTO THE ADPPA'S REGULATORY LANDSCAPE: THE PREEMPTION DEBATE

The ADPPA makes substantial progress towards improving data privacy protections for consumers in the United States and easing the compliance burden on businesses; yet it garners criticism from various stakeholders, namely for its preemption provision.[128] If the ADPPA's preemption power is limited and provides too many carve outs, the law risks being ineffective in practice.[129] On the other hand, if it is too preemptive, it risks stripping states of their lawmaking abilities and facing constitutional scrutiny.[130] Ultimately, the ADPPA strikes the appropriate balance between these two competing interests and will be effective in practice because it sets a clear federal standard, provides strong protections, and preserves existing carve outs for areas traditionally controlled by state au-

128. *See, e.g.*, Tsukayama, *supra* note 28 (opposing the ADPPA because of how it would undercut state data privacy laws). *But see* Bolton, Pugh, Lesmes, Zabierek & Simpson, *supra* note 22 (discussing the importance of having a privacy law that preempts states on substantive provisions covered at the federal level, but also preserves existing privacy-related frameworks and carve outs for areas traditionally controlled by state authority).

129. *See* Gold, *supra* note 16 ("[A] more preemptive statute is going to be better for compliance and for individuals' rights."). For a discussion of the ADPPA's carve outs, see *supra* note 21.

130. *See* Letter from Rob Bonta, California Office Att'y Gen., to Cong. Leaders (July 19, 2022), https://oag.ca.gov/system/files/attachments/press-docs/Letter%20to%20Congress%20re%20Federal%20Privacy.pdf [https://perma.cc/H46D-DZRN] (expressing concerns about the ADPPA). The letter, co-signed by the attorney generals of nine other states, states "[a]ny federal privacy framework must leave room for states to legislate responsively to changes in technology and data collection practices. This is because states are better equipped to quickly adjust to the challenges presented by technological innovation that may elude federal oversight." *Id. See also* Tsukayama, *supra* note 28 (expressing concern that the ADPPA "would roll back rights to data privacy that states have enshrined in their constitutions"). Tsukayama calls for a preemption provision that would "serve as a floor but not a ceiling," allowing states to enact more stringent privacy legislation if they wish. *Id.*

thority.[131] At the same time, lawmakers must recognize where the ADPPA falls short and continue to work together to improve data privacy protections for all stakeholders.[132]

Section A below discusses the scope of the ADPPA's "covering" preemption provision and analyzes the competing views as to what its impact will be, and Section B considers whether the ADPPA will be able to withstand preemption-based constitutional attacks.

A. *A New Network: Preemption Within the ADPPA*

Although the ADPPA adopts a narrow "covering" preemption provision, legislators intentionally carved out certain laws because states are the "laborator[ies] of democracy" and must be able to respond to changes in technology and expand rights for their constituents where necessary.[133] Non-preempted laws include, among others, consumer protection laws,

---

131. *See Hearing on ADPPA*, *supra* note 23, at 172–74 (statement of Rep. Frank Pallone, Chairman, H. Comm. Energy & Com.) (opposing Rep. Eshoo's Amendment to the ADPPA and discussing the ADPPA's strengths). Chairman Pallone states:

> I mean, it is no secret that there is robust protection for, you know, anti-discrimination protection, bans on targeted [ads] for kids, global opt-outs for sensitive data, targeted—data broken—I mean, there is so many things here that are really comprehensive consumer data privacy legislation, and that is a deal that benefits all Americans.

Id. at 174. Moreover, the Chairman claims there is "[n]o state, in my opinion, [that] has a law that is as strong as this Federal bill [the ADPPA], not even California." *Id.* at 173. Nevertheless, the Chairman does recognize that there are a few areas "where the California law is a—is stronger, and we have made an exception [for those areas]." *Id.* at 172.

132. *See id.* at 13 (statement of Rep. Gus Bilirakis, Subcomm. Consumer Prot. & Com.) (recognizing the "bipartisan efforts" representatives have undertaken to get the ADPPA to this point, but acknowledging that "our work is still not done").

133. *See id.* at 172 (statement of Rep. Frank Pallone, Chairman, H. Comm. Energy & Com.) (noting areas where the California law is stronger than the ADPPA and stating legislators have made exceptions for those areas); *see also id.* at 170 (statement of Rep. Anna Eshoo) (advocating for less state preemption through her introduction of the Eshoo Amendment). Rep. Eshoo states:

> I have heard members over the years, over and over and over again, talking about the laboratories of experimentation, the states, the states, the states. This in no way impairs the Federal legislation that is being taken up. What it does recognize is that states are far more limber, and what they have in place—yes, the Federal law, but they should be able to add to that.

Id.; Soubouti, *supra* note 14, at 532–33 (arguing states need to be able to "experiment with innovative approaches to protect [their] citizens" because "each state serves as a 'laboratory' of democracy"). *But see* Cameron F. Kerry, *Will California be the Death of National Privacy Legislation?*, BROOKINGS INST. (Nov. 18, 2022), https://www.brookings.edu/blog/techtank/2022/11/18/will-california-be-the-death-of-national-privacy-legislation/ [https://perma.cc/WH62-C4RN] (claiming lawmakers only agreed to specific state law carve outs to get certain senators on board with the ADPPA). "California officials mounted a full court lobbying press against its [the ADPPA's] preemption of provisions in state laws that are 'covered by' provisions in the federal law." *Id.*

data breach notification laws, health privacy laws, and student privacy laws—areas under which consumers could still vindicate their rights and states could enact regulations even if the ADPPA is enacted.[134]

Notwithstanding the select carve outs, commentators are confident the ADPPA will achieve a robust data protection regime in practice because its provisions are "significantly stronger" than California's CPRA—the United States' most protective data privacy law to date.[135] The ADPPA, for example, incorporates the same substantive consumer rights as the CPRA and goes one step further by requiring the consumer's affirmative consent for the collection and use of "sensitive data."[136] It also regulates a broader scope of entities, including businesses of all sizes and nonprofits, and establishes cutting-edge civil rights protections for marginalized communities impacted by the discriminatory use of data.[137] Further, the ADPPA grants the CPPA enforcement authority so that Californians have a voice in the administration of the law.[138]

Despite these strides, California lawmakers have pushed back, arguing for a "federal floor" that would allow states to provide rights in addition to those established by federal law.[139] Commentators point to the ADPPA's

134. For a discussion of the laws that will not be preempted by the ADPPA, see *supra* note 21 and accompanying text.

135. *See* Gray, *supra* note 113 (recognizing any successful federal privacy law must be at least as protective as California's CPRA for reasons "that are both political and substantive"). "Politically, House Democrats from California represent the largest voting contingency by state and must be satisfied with a bill for it to move forward." *Id.* Substantively, California residents represent the largest U.S. state by population—constituting the "fifth largest global economic power,"—and thus enjoy significant privacy protections already under the CPRA. *Id.* Because the ADPPA would preempt these protections, lawmakers "must ensure that Californians end up equally or better protected under a federal regime." *Id. But see Detailed Analysis Shows CPRA is Significantly Stronger than ADPPA*, CALIFORNIANS FOR CONSUMER PRIV. (Aug. 12, 2022), https://www.caprivacy.org/analysis-shows-cpra-is-significantly-stronger-than-adppa/ [https://perma.cc/4XCA-XKS9] (refuting claims that the ADPPA is a stronger privacy law than the CPRA).

136. *See* Gray, *supra* note 113 (comparing the ADPPA to the CPRA). For a discussion of the ADPPA's provision on sensitive covered data, see *supra* note 110 and accompanying text.

137. *See* Gray, *supra* note 113 (comparing the ADPPA to the CPRA). For a discussion of the ADPPA's definition of "covered entities," see *supra* note 108 and accompanying text. For a discussion of the ADPPA's civil rights provision, see *supra* note 113 and accompanying text.

138. For a discussion of the ADPPA's enforcement provision, see *supra* note 115 and accompanying text.

139. *See* Rep. Anna Eshoo, *supra* note 28 (introducing an amendment to the ADPPA that would protect California's ability to strengthen privacy protections for its residents in the future). *But see Hearing on ADPPA*, *supra* note 23, at 172–74 (statement of Rep. Frank Pallone, Chairman, H. Comm. Energy & Com.) (discussing his opposition to the Eshoo Amendment and advocating for the ADPPA's strong consumer protections in comparison to those provided by California's data privacy law). Chairman Pallone states:

> [A]s much as I appreciate the fact that some states and some attorney generals may feel, oh, you know, we are going to do better, the reality is that is probably not going to happen, because it hasn't happened. It just

express carve out for BIPA to illustrate this point, as BIPA is not preempted under Section 404(b)(2)(M) even though Section 3(A) broadly covers "biometric information."[140] In effect, this allows Illinois to retain its narrowly focused biometric privacy law, but precludes other states from passing a similar or even identical law to protect their constituents.[141] This raises concerns that consumers in other states will be left vulnerable to biometric data violations, especially because the ADPPA is less protective of biometric data than BIPA.[142] The ADPPA, for example, does not always require opt-in consent to collect or transfer biometrics and does not offer as strong of a private right of action.[143]

While the BIPA carve out may represent a gap in the law, it does not undermine the ADPPA's progress and warrant doing away with the bill.[144] Lawmakers recognize the gaps in the bill's preemption provision but

---

> hasn't happened at all, for all practical purposes. And the other problem, too, is that if states decide that they are going to enact stronger laws and somehow get around to it, which I don't think they will, who is going to determine whether it is stronger? Every state is going to say it is stronger, and then we are going to end up in courts and litigation forever.

Id. at 173.

140. *See* American Data Privacy and Protection Act, H.R. 8152, 117th Cong., 2d Sess. §§ 2(3)(A)(i)–(v), 404(b)(2)(M) (2022) (preserving BIPA). For a brief discussion of BIPA, see *supra* note 49 and accompanying text.

141. *See* Tsukayama, *supra* note 28 (explaining how this is a loss to state efforts in Texas, Washington, and New York—all of which have been working to implement their own biometric data privacy laws after Illinois paved the way with BIPA in 2008); *see also* Daniel Solove, *Further Thoughts on ADPPA, The Federal Comprehensive Privacy Bill*, TEACHPRIVACY (July 30, 2022), https://teachprivacy.com/further-thoughts-on-adppa-the-federal-comprehensive-privacy-bill/ [https://perma.cc/35EB-8TKF] (stating "[t]here might be no more BIPAs in the future" due to the ADPPA's broad preemptive power).

142. *See* Tsukayama, *supra* note 28 (discussing why this creates a strong incentive for federal privacy legislation to "serve as a floor but not a ceiling"). For a discussion of why the ADPPA is less protective of biometric data than BIPA, see *infra* note 143 and accompanying text.

143. For the direct text of the ADPPA's provision covering biometric data, see H.R. 8152 §§ 2(3)(A)(i)–(v). For the direct text of BIPA's private right of action, see Illinois Biometric Information Privacy Act of 2008, 740 ILL. COMP. STAT. 14/20 (2022) ("Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in a federal district court against an offending party."). *See also* Tsukayama, *supra* note 28 (claiming the ADPPA's private right of action is not as strong as BIPA's). This is because Illinois state courts do not require plaintiffs to demonstrate harm, unlike federal courts, which require a showing of harm to assert Article III standing under *Spokeo*. *Compare* Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1207 (Ill. 2019) ("[A]n individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act."), *with* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1550 (2016) ("Robins [the plaintiff] cannot satisfy the demands of Article III by alleging a bare procedural violation. A violation of one of the FCRA's procedural requirements may result in no harm.").

144. For a discussion of why the BIPA carve out may be problematic, see *supra* note 143 and accompanying text. For a discussion of the ADPPA's strong protec-

maintain that those gaps have clearly been contemplated by other state and federal laws.[145] Moreover, a federal law with less preemptive power might leave individuals and companies "flipping through pages" trying to figure out what Congress explicitly carved out, and thus, which laws offer the most appropriate means for relief.[146] Any successful federal data privacy law requires some preemptive power, and the ADPPA strikes the appropriate balance.[147] It offers the uniform approach consumers and businesses need given the interstate nature of electronic commerce and associated data breaches, while also allowing states to regulate where necessary.[148]

B. *Potential Breach? Predicting the ADPPA's Constitutional Viability*

The ADPPA or a similar future statute may face preemption-based constitutional attacks due to the current controversy surrounding its scope.[149] Notwithstanding such challenges, the ADPPA likely would survive constitutional scrutiny because Section 404(b)(1) expressly provides for the preemption of all state laws, regulations, rules, standards, and requirements *covered* by the Act, or a rule, regulation, or requirement

---

tions in comparison to other state privacy laws, namely the CPRA—the strongest state privacy law to date—see *supra* notes 135–38 and accompanying text.

145. *See Hearing on ADPPA*, *supra* note 23, at 172 (statement of Rep. Kathy Castor) (recognizing the ADPPA would preempt only some of the provisions of other design code bills). At least with respect to laws concerning the data privacy of children, there are bills "moving through states right now," and "[t]hose preempted provisions would be the ones covered by this bill dealing with advertising and privacy." *Id.* *But see* Gold, *supra* note 16 ("Congress was trying hard not to get in the way of all these existing laws . . . but it [the ADPPA] will not be that useful if the federal government has their hands tied."). When asked about whether the ADPPA would be effective in practice given the holes it leaves open and thus the potential alternative avenues for individuals to vindicate their rights under non-preempted laws, Ms. Gold indicated that perhaps the ADPPA "tried to do too much and became too complex" with all the existing carve outs. *Id.*

146. *See* Gold, *supra* note 16 (explaining how privacy experts would still be "flipping through pages back and forth to figure out what applies where," so a more preemptive statute is going to be "better for compliance and individuals' rights").

147. *See* Soubouti, *supra* note 14, at 532 ("Preemption is crucial to the federal data privacy law debate because one federal law would greatly simplify industry compliance efforts in the long run by establishing uniform national standards."); *see also Hearing on Protecting America's Consumers*, *supra* note 22, at 85 (statement of Rep. Bob Latta) (discussing the importance of a preemptive federal data privacy statute).

148. For a discussion of why a state-led privacy regime causes challenges for various stakeholders, see *supra* Section II.A.1–2. For a discussion of the ADPPA's preemption provision, see *supra* note 21.

149. For a discussion of the controversy surrounding the scope of the ADPPA's preemption provision, see *supra* Section IV.A.

promulgated under it.[150] The text alone suggests that Congress intends for the ADPPA to explicitly preempt states from enacting their own data privacy laws unless provided for otherwise in Section 404(b)(2).[151]

Even in challenging the plain language, however, the ADPPA should pass constitutional muster under the *Easterwood* "covering" preemption analysis.[152] In *Easterwood*, the Court determined that federal railroad maximum-speed regulations preempted state law claims related to railroad safety because they "substantially subsumed" and comprehensively regulated the subject of train speeds—thus reflecting Congress's intent to preclude additional state regulations.[153] Similarly, the ADPPA's preemption provision establishes an intent to "substantially subsume" and comprehensively regulate the subject of data privacy at the state level.[154] It also expressly precludes states from enacting certain legislation in that area.[155] Any constitutional challenge to the ADPPA's "covering" preemption provi-

150. *See* Puerto Rico v. Franklin Cal. Tax-Free Tr., 579 U.S. 115, 125 (2016) (describing how a reviewing court should analyze an express preemption-based challenge). The Court stated: "[B]ecause the statute 'contains an express preemption clause,' we do not invoke any presumption against pre-emption but instead 'focus on the plain wording of the clause, which necessarily contains the best evidence of Congress' pre-emptive intent.'" (quoting Chamber of Com. v. Whiting, 563 U.S. 582, 594 (2011)). For further discussion of the Court's "covering" preemption jurisprudence, see *supra* note 124 and accompanying text. For the direct text of the ADPPA's express "covering" preemption provision, see *supra* note 21.

151. *See Hearing on ADPPA*, *supra* note 23, at 172 (statement of Rep. Kathy Castor) ("[I]n this bill we use covering preemption, so when state laws aren't substantially subsumed by Federal law they won't be preempted."). For the direct text of the ADPPA's express "covering" preemption provision, see *supra* note 21. *See also Puerto Rico*, 579 U.S. at 125 ("[F]or purposes of the pre-emption provision[,] [the analysis] begins 'with the language of the statute itself,' and that 'is also where the inquiry should end,' [if] 'the statute's language is plain.'" (quoting United States v. Ron Pair Enter., Inc., 489 U.S. 235, 241 (1989))).

152. *See* CSX Transp., Inc. v. Easterwood, 507 U.S. 658, 673–76 (1993) (explaining the Court's approach to adjudicating an express preemption challenge). For further discussion of the Court's specific reasoning in *Easterwood*, see *infra* notes 153 & 156 and accompanying text.

153. *See Easterwood*, 507 U.S. at 673–76 (discussing the Court's rationale). Despite federal regulations issued by the Secretary of Transportation under the FRSA, the plaintiff claimed the "petitioner breached its common-law duty to operate its train at a moderate and safe rate of speed." *Id.* at 673. Because, however, the federal regulations determining safe train speeds were adopted in furtherance of the statute's goal to prevent hazards posed by train-track conditions, the Court read the federal speed limits as "not only establishing a ceiling, but also precluding additional state regulation of the sort that respondent seeks to impose on petitioner." *Id.* at 674. It is important to note that this reflects the Court's 1990s preemption jurisprudence, where it applied the "presumption against pre-emption," yet still determined that the federal regulations adopted by the Secretary preempted plaintiff's state law negligence action insofar as it asserted that the train was traveling at an "excessive speed." *Id.* at 668, 675.

154. *See Hearing on ADPPA*, *supra* note 23, at 172 (statement of Rep. Kathy Castor) (claiming the ADPPA uses "covering preemption"). For the direct text of the ADPPA's express "covering" preemption provision, see *supra* note 21.

155. For the text of the ADPPA's express "covering" preemption provision, see *supra* note 21.

sion would have to demonstrate that Congress did not intend to displace supplementary state regulations, which would be difficult given Section 404(b)'s express preemptive language and lawmakers' repeated calls for a "covering" preemption provision at legislative hearings.[156]

V. REPROGRAMMING THE FUTURE OF DATA PRIVACY

Until lawmakers enact the ADPPA, experts can only predict how it will operate in practice.[157] The effects of passing the ADPPA as it currently stands are discussed below.[158] Section A considers how the ADPPA would interact alongside Europe's GDPR, and Section B explores the viability of the ADPPA's private right of action.

A. *More Coding: ADPPA vs. GDPR*

Despite the ADPPA's broad protections, commentators question how it will operate against the GDPR's stringent requirements.[159] The GDPR covers almost all types of personal data, subjects both the government and

156. *See* Adkins, Pepper & Sykes, *supra* note 118, at 11 (analyzing the *Easterwood* Court's two-part holding). Although the Court held that federal law preempted state law claims alleging the train traveled at an unsafe speed despite complying with federal maximum-speed regulations, the Court determined that "federal regulations of grade crossing safety *did not* preempt state law claims alleging that a train operator failed to maintain adequate warning devices at a crossing where a collision had occurred." *Id.* (emphasis added) (citing *Easterwood*, 507 U.S. at 665–73). Where the Court's analysis differed was with respect to the scope of the statutory language; the federal regulations concerning warning devices required states receiving railroad funding to establish a "highway safety improvement program" and merely "consider and rank the dangers posed by grade crossings." *Easterwood*, 507 U.S. at 665–66 (quoting 23 C.F.R. §§ 924, 924.9(a)(4) (2023)). Thus, the regulation did not "substantially subsume" the subject of warning device adequacy because it only established "general terms of the bargain between the Federal and State Governments" and did not reflect an intent to displace supplementary state regulations. *Id.* at 666–67. For the direct text of the ADPPA's express "covering" preemption provision, see *supra* note 21. *See also Hearing on ADPPA*, *supra* note 23, at 172 (statement of Rep. Kathy Castor) (discussing the ADPPA's use of "covering preemption").

157. For diverging opinions over how the ADPPA will operate in practice given the scope of its preemption provision, see *supra* Section IV.A.

158. For further discussion of the ADPPA's potential impact on international data privacy law and private rights of action, see *infra* Section V.A–B.

159. *See, e.g.*, *How Does the Proposed American Data Privacy and Protection Act Compare to the GDPR?*, OSBORNE CLARKE (Aug. 8, 2022), https://www.osborneclarke.com/insights/how-does-proposed-american-data-privacy-and-protection-act-compare-gdpr [https://perma.cc/7G7H-9W4Q] (acknowledging that while the ADPPA would create a data privacy framework in the United States similar to that of Europe's GDPR, the ADPPA "is in many ways different to the GDPR"). If the ADPPA is enacted, international companies must know the details of the new legislation and understand how the requirements can be addressed by "leveraging any compliance documentation and procedures already existing at the company in order to avoid a fragmented and unharmonized privacy compliance program." *Id.* *But see* Souboti, *supra* note 14, at 551 (claiming uniformity of data privacy laws at the national and international level would be ideal considering the "borderless nature of the Internet").

for-profit and nonprofit entities to compliance, and applies protections to all individuals regardless of E.U. citizenship status.[160] The ADPPA, in contrast, specifically excludes certain personal information, does not subject governmental bodies to compliance, and applies protections to United States residents only.[161]

As a result, businesses in compliance with the ADPPA would not necessarily comply with the GDPR, thus perpetuating the same issues American businesses currently face, but on an international scale.[162] At the same time, the United States should be cautious of adopting a regime more similar to the GDPR, despite the potential commercial benefits, because commentators suspect it is responsible for changing market conditions that have hampered the European Union's economy.[163]

---

160. *See* Council Directive 2016/679, 2016 O.J. (L 119) (EU) (clarifying that governmental bodies will be exempt from GDPR compliance when data is gathered and processed for the purpose of prevention, investigation, detection, or the prosecution of criminal offenses). For a summary of the GDPR's key provisions, see Albrecht, *supra* note 64.

161. *See How Does the Proposed American Data Privacy and Protection Act Compare to the GDPR?*, *supra* note 159 (comparing the ADPPA to the GDPR). For a discussion of the ADPPA's definition of "covered entities," see *supra* note 108. For a discussion of the ADPPA's definition of "covered data," see *supra* note 109. For a discussion of whom the ADPPA provides protections to, see Gaffney, Linebaugh & Holmes, *supra* note 32, at 2 (stating the ADPPA "give[s] *consumers* various rights over covered data, including the right to access, correct, and delete their data held by a particular covered entity" (emphasis added)); *see also* David Stauss & Shelby Dolen, *Analyzing the American Data Privacy and Protection Act's Private Right of Action*, HUSCH BLACKWELL (Aug. 1, 2022), https://www.bytebacklaw.com/2022/08/analyzing-the-american-data-privacy-and-protection-acts-private-right-of-action [https://perma.cc/R7CV-ZGWX] (noting that the ADPPA's reference to "consumers" is limited to United States citizens, because only citizens may bring private rights of action under Section 403 of the bill).

162. *See* Soubouti, *supra* note 14, at 551 (discussing the implications of the United States adopting a comprehensive federal data privacy regime like Europe's GDPR). A more stringent standard might ease the compliance burden on businesses that already must comply with the GDPR's requirements. *Id.* Otherwise, the United States will be left with divergent national and international standards that present the same problem businesses currently face—a disparate data privacy framework (i.e., "a new international patchwork of laws"). *Id.* "Ultimately, a comprehensive federal privacy law that establishes strong, uniform protections for data privacy will benefit industries like the financial services sector by providing certainty, maintaining consumer trust, and avoiding stifling industry innovation." *Id.* at 550. *See also* Light, *supra* note 25, at 892 ("The United States needs nothing short of a federal equivalent of the GDPR.").

163. *See, e.g.*, Stephanie Comstock Ondrof, Comment, *"Senator, We Run Ads": Advocating for a US Self-Regulatory Response to the EU General Data Protection Regulation*, 28 GEO. MASON L. REV. 815, 847 (2021) (describing the economic costs associated with the GDPR's stringent compliance requirements). These include increased market consolidation, limited access to news and entertainment sources, confusion among businesses, and barriers to entry for startup corporations. *Id.* Studies estimate the United States would face compliance costs and market ineffectiveness at a rate of nearly $122 billion per year if it were to adopt a comprehensive regime like Europe's GDPR. *Id. See also* Soubouti, *supra* note 14, at 551 (recognizing the GDPR's "rigid fine structure" as a downfall of the law and cautioning United States

B. *Access Granted? Exploring the ADPPA's Private Right of Action*

Some privacy commentators applaud the ADPPA's private right of action because it incorporates two ways to ensure the vindication of one's rights (i.e., "a hybrid enforcement regime").[164] Proponents argue individuals should be permitted to seek compensation for their legally protected privacy interests and maintain that private rights of action would induce compliance by supplementing other modes of enforcement.[165] Indeed, private enforcement deters potential wrongdoers by allowing for a consistent enforcement mechanism even when FTC funding or political will are lacking.[166] In fact, several federal privacy statutes already successfully implemented the hybrid enforcement regime, including the Telephone Consumer Protection Act (TCPA) and the FCRA, which "use[ ] private parties as an adjunct to, or substitute for, public enforcement."[167]

---

lawmakers to "avoid overwhelming U.S. industries with a burdensome data privacy framework as stringent as the GDPR"); Laurent Belsie, *Impacts of the European Union's Data Protection Regulation*, NAT. BUREAU ECON. RSCH. (July 2022), https://www.nber.org/digest/202207/impacts-european-unions-data-protection-regulations [https://perma.cc/V3CK-DBCV] (noting the GDPR has hindered the introduction of new technology into the market and made administrative compliance costly and burdensome for certain companies).

164. *See* Scholz, *supra* note 33, at 1646–47 (identifying a "hybrid enforcement regime" as more effective than a purely public or private enforcement regime). According to Scholz, private enforcement is necessary to support public enforcement because it "broadens and democratizes the public forum for sharing and analyzing disputes in the information economy beyond the limits of administrative agencies." *Id.* at 1647. *See also* Hirsch, *supra* note 16, at *14 (discussing the benefits of incorporating a private right of action into comprehensive federal data privacy legislation).

165. *See, e.g.*, Scholz, *supra* note 33, at 1639 ("Private rights of action are the most direct regulatory access point to the private sphere. They leverage private expertise and knowledge, create accountability through discovery, and have expressive value in creating privacy-protective norms."). Scholz contends that private rights of action are an integral part of a successful federal data privacy regime, in addition to public enforcement via the FTC or state attorney generals. *Id.* at 1644–45.

166. *See id.* at 1647, 1666 (explaining how private enforcement avoids underenforcement by administrative agencies, which could potentially lead to large-scale non-enforcement of the right); *see also supra* note 86 (where Heitz discusses *In re Nickelodeon* as an example of when private enforcement would have helped plaintiffs vindicate their rights in the absence of FTC intervention).

167. *See* Scholz, *supra* note 33, at 1656 (quoting Edward J. Janger, *Privacy Property, Information Costs, and the Anticommons*, 54 HASTINGS L.J. 899, 907 (2003)). Scholz claims these laws have been "largely successful in achieving concrete outcomes." *Id.* The TCPA governs "abusive telemarketing practices," and the FCRA "limit[s] [the] abuse of consumer credit files." *Id.* Public and private enforcement complement each other under these statutes; public actors are well-suited to address collective action problems since class actions with small claims are unlikely to pass judicial muster. *Id.* Public agencies can also provide guidance, administer bright-line rules, and provide ongoing guidance to industries, but they cannot address every instance of wrongful data privacy usage. *Id.* "Private rights of action allow every wrong under a statute to be a potential subject of litigation. Thus, private actors provide the primary incentive for companies to comply and agencies

Opponents of the private right of action generally acknowledge that individuals should have a right to redress but raise concerns about how it would operate in practice.[168] Namely, experts fear it would induce frivolous litigation and increase the potential for class action lawsuits that would expose companies to damages regardless of the claim's merit.[169] United States Supreme Court precedent in *Spokeo* further calls into question the viability of a private right of action because the Court held that a "bare procedural violation" of the FCRA was insufficient to establish Article III standing.[170] Standing requires a showing of a concrete, particularized, and actual or imminent injury-in-fact, and thus was not satisfied by the plaintiff's allegation that defendant illegally stored his personal information in violation of federal law.[171] Because the ADPPA does not require consumers to show "injury-in-fact" before filing a complaint and

---

to continue to enforce these laws in every interaction with every consumer." *Id.* at 1657.

168. *See, e.g.*, Gold, *supra* note 16 (questioning whether there should be a private right of action within the ADPPA); Rebecca Kern, *Bipartisan Draft Bill Breaks Stalemate on Federal Data Privacy Negotiations*, POLITICO (June 3, 2022, 5:46 PM), https://www.politico.com/news/2022/06/03/bipartisan-draft-bill-breaks-stalemate-on-federal-privacy-bill-negotiations-00037092 [https://perma.cc/27FL-3P9G] (discussing the United States Chamber of Commerce's opposition to the ADPPA's private right of action). For further discussion of how the private right of action may create problems in practice, see *infra* note 169 and accompanying text.

169. *See* Gold, *supra* note 16 (stating a private right of action could create a dangerous precedent and increase the presence of frivolous litigation). Rather, it might be more useful to have agencies vested with the authority to enforce the law do so. *Id.* This might be better all-around for businesses from a compliance perspective, and would also yield consistent enforcement mechanisms going forward. *Id.* Ms. Gold raises the point that when different courts are coming to different conclusions about the interpretation of one law, it becomes tricky for organizations operating in multiple jurisdictions to know what is needed to comply. *Id.* At least with enforcement vested in one federal agency, businesses can better understand the compliance obligation. *Id. See also* Kern, *supra* note 168 (noting the United States Chamber of Commerce has strongly opposed any bill including a private right of action due to concerns that it would generate high numbers of class action lawsuits).

170. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1550 (2016) (holding that the plaintiff could not satisfy the injury-in-fact demands of Article III standing by alleging only a procedural violation of the FCRA and thus could not survive defendant's motion to dismiss for lack of standing).

171. *Id.* at 1549–50 (explaining why a procedural violation of the FCRA alone may be insufficient to satisfy the demands of Article III standing). The Court explained:

> Congress' role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right. Article III standing requires a concrete injury even in the context of a statutory violation.

Id. at 1549. For further discussion of the Court's rationale in *Spokeo*, see *supra* note 76 and accompanying text. *See also* Solove, *supra* note 141 (cautioning that every time Americans use the private right of action in federal court, they will be forced to "deal with the dragon of standing" prompted by *Spokeo*). As a result, the U.S. Supreme Court has "shut out many valid cases involving clear violations of federal

limits recovery to federal courts, plaintiffs suing under the law could fail to meet the standing requirement laid out in *Spokeo* and effectively lose the ability to privately vindicate their rights.[172]

C. *Conclusion*

Privacy comes at a cost, and any comprehensive federal legislation will have its tradeoffs.[173] Nevertheless, Congress carefully considered the interests of all stakeholders and crafted a law that achieves its goals and will be effective in practice.[174] The ADPPA provides robust protections to consumers, offers businesses the clarity needed to ease compliance burdens, and leaves states with enough autonomy to enact new legislation where necessary.[175] There is not one solution that will appease all stakeholders, but the ADPPA is the closest bipartisan effort to finding a workable solution, and this reflects hope for the future.[176]

Despite the great strides the ADPPA makes towards its goals, commentators and privacy experts diverge over the breadth of its preemption provision.[177] The effectiveness of the law hinges on this important determination, coupled with its ability to withstand preemption-based constitutional challenges.[178] Ultimately, any comprehensive federal statute will leave some gaps in the law because states have already started to legislate

---

privacy statutes with causes of action" because most federal privacy laws recognize only intangible harms. *Id.*

172. *See* Hirsch, *supra* note 16, at *15 (claiming cases like *Spokeo* impact Congress's ability to incorporate effective statutory language for the private right of action); *see also* Stauss & Dolen, *supra* note 161 (explaining that plaintiffs may be unable to bring their claim in federal court even if a covered entity or service provider violates the provisions of the ADPPA absent a showing of concrete injury given the Supreme Court's holding in *Spokeo*). Showing "injury" for privacy violations has proven difficult in the past, and because the ADPPA limits plaintiffs' access to federal (and not state) courts, "this limitation could be determinative in many [future] lawsuits." *Id.*

173. For a discussion of which laws under the ADPPA would receive carve outs and which laws would not, see *supra* Section IV.A. For the direct text of the ADPPA's preemption provision, see *supra* note 21.

174. For a discussion of stakeholders' competing views over the scope of the ADPPA's preemption provision, see *supra* Section IV.A. For a discussion about why the ADPPA will likely be successful in practice and will withstand preemption-based constitutional challenges, see *supra* Section IV.B.

175. For a discussion about why consumers and businesses desire a comprehensive federal data privacy statute, see *supra* Section II.A.1–2. For a discussion about the balance lawmakers tried to achieve when crafting the ADPPA's preemption provision, see *supra* Section IV.A.

176. For a discussion of the different stakeholder interests—namely, those of consumers and businesses—see *supra* Section II.A.1–2. For a discussion about why lawmakers have struggled to find a bipartisan solution to this complex issue in the past, see *supra* notes 25–31.

177. For a discussion of the diverging opinions over the scope of the ADPPA's preemption provision, see *supra* Section IV.A.

178. *See id.* For a more detailed discussion of whether the ADPPA will be able to withstand preemption-based constitutional challenges, see *supra* Section IV.B.

in this area, but this does not warrant doing away with the ADPPA.[179] Its advantages outweigh its disadvantages, and lawmakers have strategically contemplated the gaps it leaves open.[180]

Creating comprehensive federal data privacy legislation is certainly no easy task, and the ADPPA is likely only the beginning of the federal data privacy regime that is to come for the United States.[181] A new era of increased consumer protections awaits, and the ADPPA serves as an integral steppingstone to get there.[182]

---

179. For further discussion of the potential gaps in the law, see *supra* Section IV.A (discussing BIPA and noting how it will be difficult for other states to enact biometric data privacy laws if the ADPPA is ultimately enacted). For a discussion of the non-preempted laws carved-out from the ADPPA's preemption provision, see *supra* note 21.

180. For further discussion of lawmakers' thoughts about the bill, see *Hearing on ADPPA*, *supra* notes 23 & 132 (statement of Rep. Gus Bilirakis, Subcomm. Consumer Prot. & Com.) (demonstrating an understanding that there is still work to be done in terms of achieving a comprehensive federal data privacy standard in the United States despite the ADPPA's achievements). For a discussion of what "gaps" could be left in the ADPPA, see *supra* note 21 for a list of non-preempted laws. For a discussion of which states have already enacted data privacy laws, see *supra* Section II.B.2.

181. *See Hearing on Protecting America's Consumers*, *supra* note 22, at 4–5 (statement of Rep. Jan Schakowsky) ("This [the ADPPA] is a . . . pivotal, an important, moment in our journey to ensure that online privacy rights are there for all Americans, and we are definitely on our way. . . . The road has been long and sometimes quite bumpy . . . but here we are today, and we had a wonderful process.").

182. *See id.* at 156 (statement of Rep. Jan Schakowsky) (claiming there are aspects of the ADPPA that can still be improved going forward but applauding the House Energy & Commerce Committee for introducing "bipartisan, bicameral legislation" that consumers, businesses, and Americans care deeply about).