Loyola of Los Angeles Law Review

Volume 55 | Number 4 Article 6

Fall 10-19-2022

The Data Privacy Compromise: Reconciling State and Federal Regulatory Regimes on the Path to Preemption

Mi T. Tran

THE DATA PRIVACY COMPROMISE: RECONCILING STATE AND FEDERAL REGULATORY REGIMES ON THE PATH TO PREEMPTION

Mi T. Tran[*]

Today, it is easier than ever before for business entities to collect and sell our data, and most consumers lack comprehensive knowledge of how they can protect their data or recognize the true extent of potential exposure. Although data privacy regulation is gearing up among U.S. states, federal legislators have been stagnant in regard to passing a federal data privacy law. Without clearer, broader protections for consumers, many will be left to deal with overlapping laws and confusing procedures for pursuing legal remedies.

The relationship between federal and state regulation is best maintained when Congress carefully balances the different roles of each. In the context of data privacy, some legislators believe that the states should enact their own laws without federal interference, as some already have, while others believe that federal preemption is imperative to achieving the most efficient protection for consumer data. As the pressure piles on for Congress to pass a federal privacy law, a balanced approach is key to moving forward. This Note proposes a happy medium and explores a multilayered approach to preemption to achieve a uniform baseline for protection without displacing the states' valuable regulatory role in the data privacy sphere.

[*] J.D. Candidate, LMU Loyola Law School, May 2022. Thank you to Professor Lauren Willis, for your invaluable guidance and support, and to the folks at the *Loyola of Los Angeles Law Review* for all of your dedication and hard work—I couldn't have done it without you. Special thanks to my family, friends, and classmates, who have graciously supported me throughout the writing process and beyond.

TABLE OF CONTENTS

I. INTRODUCTION

Samuel Warren and Louis Brandeis' groundbreaking law review article famously introduced the concept of privacy rights in the late 1800s.[1] Back then, the implications of privacy were exclusively maintained in the physical sphere and predated the innovative technologies of the modern world.[2] Today, daily life has become integrated with advanced technologies, with all of the conveniences and inconveniences that come from living in a digital age. Online communities and platforms are pervasive and continue to expand, and nowadays, technology permeates virtually every industry, including communication, education, business and commerce, and even healthcare.[3] As a result, the aforementioned privacy challenges moved beyond the physical realm into the digital domain, and the concept of "information privacy" was born.[4] With social media platforms, advertising companies, online businesses, and even government entities collecting personal data, the risk of privacy violations has increased. Alan Westin, a privacy scholar and advocate, argued that individuals should have control over their personal data, including the amount of information disclosed, maintained, disseminated, and to whom.[5] Recently, the digital industry has been garnering negative attention over the increase in data breaches and invasions of privacy relating to the collection, processing, and selling of individuals' personal information.[6] Federal

1. Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

2. *See generally id.* (discussing individuals' rights to protect the privacy of their lives from physical and mental invasions of others).

3. Jack Turner, *The 7 Main Ways Technology Impacts Your Daily Life*, TECH.CO (May 5, 2021, 12:01 AM), https://tech.co/vpn/main-ways-technology-impacts-daily-life [https://perma.cc/9E5F-4XFT].

4. Alan Westin expanded the concept of privacy beyond bodily autonomy, defining the right to privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).

5. Luisa Rollenhagen, *Alan Westin Is the Father of Modern Data Privacy Law*, OSANO (Sept. 8, 2020), https://www.osano.com/articles/alan-westin [https://perma.cc/K73M-2AAR].

6. Michael Hill & Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO (July 16, 2021, 2:00 AM), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html [https://perma.cc/VZX8-SG6D]. *See generally* Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, WIRECUTTER (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/ [https://perma.cc/S8EN-YXY9] (discussing recent data leaks and breaches).

governments around the world are responding to public outcry by enacting data privacy regulations,[7] but the United States has fallen behind, taking a limited sectoral approach to regulation. Although federal legislators introduced bills early on, the conversation has stalled due to polarizing views on whether data privacy should be regulated by state or federal government entities.[8] In response to the lack of federal action, state governments have begun to address the widespread threats to data privacy, leading with the California Consumer Privacy Act of 2018 (CCPA).[9] The CCPA pioneered state regulatory efforts to curb abuses of personal data collection and use, and its stringent protections for consumers inspired many other states to introduce similar bills.[10] Since the CCPA has taken effect, industry advocates have begun to lobby for a federal baseline privacy law, and there has been a recent influx of federal bills proposed in both the House and Senate.[11]

7. The European Union enacted the General Data Protection Regulation (GDPR), a regulation that applies to all EU members states and is currently the strongest privacy law in the world. Regulation (EU) 2016/679 of Apr. 27, 2016, on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) [hereinafter GDPR]; *General Data Protection Regulation (GDPR)*, INTERSOFT CONSULTING, https://gdpr-info.eu/ [https://perma.cc/XXB9-RHRZ].

8. One roadblock to negotiation over new legislation is whether a federal law should preempt existing state laws. Lauren Feiner, *Lawmakers Kick the Can Down the Road on Discussing the Most Contentious Issues of Privacy Legislation*, CNBC (Feb. 9, 2020, 4:34 PM), https://www.cnbc.com/2020/02/08/lawmakers-postpone-discussing-contentious-privacy-legislation-issues.html [https://perma.cc/SH4L-ELZR]. Last year, draft legislation and indications of privacy hearings in Congress failed to materialize. Cameron F. Kerry, *One Year After Schrems II, the World Is Still Waiting for U.S. Privacy Legislation*, BROOKINGS (Aug. 16, 2021), https://www.brookings.edu/techtank/2021/08/16/one-year-after-schrems-ii-the-world-is-still-waiting-for-u-s-privacy-legislation/ [https://perma.cc/XJP4-UMP5].

9. "The California Consumer Privacy Act (CCPA), enacted in 2018, created new consumer rights relating to the access to, deletion of, and sharing of personal information that is collected by businesses." Golden Data Law, *A Guide to the California Consumer Privacy Act (CCPA)*, MEDIUM (Oct. 14, 2019), https://medium.com/golden-data/a-guide-to-the-california-consumer-privacy-act-ccpa-3a916756ed36 [https://perma.cc/MS5X-9XKT]; Ben Adler, *California Passes Strict Internet Privacy Law with Implications for the Country*, NPR (June 29, 2018, 5:05 AM), https://www.npr.org/2018/06/29/624336039/california-passes-strict-internet-privacy-law-with-implications-for-the-country [https://perma.cc/8NYC-FFYH].

10. Taylor Kay Lively, *US State Privacy Legislation Tracker*, IAPP, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ [https://perma.cc/U2JH-NVZ6] (last updated Feb. 24, 2022).

11. Müge Fazlioglu, *US Federal Privacy Legislation Tracker*, IAPP, https://iapp.org/resources/article/us-federal-privacy-legislation-tracker/ [https://perma.cc/FM33-GJ3H] (last updated Aug. 2, 2021).

The pressure for congressional action is increasing, but legislators must carefully balance state and federal interests and consider the consequences of preemption for consumers and businesses before setting a national standard that will reshape the future of U.S. data privacy. The CCPA has been in effect for more than a year, and as various state laws continue to appear, the need for uniformity will increase. The time for a federal privacy law is now, but to what extent can the new law preempt existing state regulation without watering down protections or displacing important remedial measures?[12] This Note will explore possible answers to this question and propose that, while some form of federal preemption is inevitable, taking a layered approach to federal preemption will set a uniform, national baseline for enforcement while preserving the states' valuable role in the data privacy sphere.

Part II gives an overview of modern data privacy implications for consumers and businesses.[13] Part III will discuss the relationship between federal and state governments in response to data privacy issues and the increasing friction between federal and state interests.[14] Part IV examines different approaches to preemption and how Congress has balanced federal and state interests in other areas of privacy.[15] Finally, Part V will discuss a recently proposed Senate bill and recommend that taking a layered approach to preemption is the most effective method to reconcile federal and state privacy interests.[16] As illustrated by a report from the Brookings Institution,[17] legislators should revise the existing bill, based on preemption concepts from other federal statutes in the privacy arena, and add a sunset clause to reassess the new law's impact in the near future.[18]

12. Stacey Gray, *Navigating Preemption Through the Lens of Existing State Privacy Laws*, FUTURE OF PRIV. F. (July 2, 2021), https://fpf.org/blog/navigating-preemption-through-the-lens-of-existing-state-privacy-laws/ [https://perma.cc/D3KD-RS8N].

13. *See infra* Part II.

14. *See infra* Part III.

15. *See infra* Part IV.

16. *See infra* Part V.

17. The Brookings Institution, also known as "Brookings," is an American nonprofit public policy organization, where experts conduct independent government research to analyze and solve problems in many areas, including national privacy affairs, and publish policy recommendations. *Brookings Institution*, BALLOTPEDIA, https://ballotpedia.org/Brookings_Institution [https://perma.cc/QR45-D2GC].

18. Brookings researchers published a report detailing their policy recommendations regarding federal privacy legislation and offering a baseline framework to address the consequences of

II. THE COSTS AND BENEFITS OF INFORMATION PRIVACY FOR CONSUMERS AND BUSINESSES

"Cyberspace is our new arena for public and private activities."[19] Due to evolving technology advancements and the growth of the digital industry, the physical world has become enmeshed with the virtual world in an information era where it is becoming increasingly difficult to keep anything offline. Nowadays, the convenience, and even necessity, of doing everything online—shopping, socializing, banking, and utilizing healthcare services—has contributed to the exponential growth of data generated on the internet, mostly consisting of individuals' personal information.[20] As technology has continued to evolve, personal data can be collected from any device that is tied to the digital sphere, such as cell phones, "smart" home appliances, and mobile applications.[21] Companies, organizations, and even government entities are collecting personal data from every corner of the digital landscape.[22] Individuals' personal information that was once considered private and easily controlled by users is now commodified in the marketplace, fueling the internet economy and holding high profit value to organizations like online retailers and big technology companies who stand to benefit from collecting and selling such information.[23]

---

preemption for both state and federal interests. This Note explores two key components of Brookings' "tiered approach" to federal preemption of state privacy laws—revising an existing bill and adding a sunset clause—because they offer the most balanced consideration of state and federal regulatory systems. CAMERON F. KERRY ET AL., BRIDGING THE GAPS: A PATH FORWARD TO FEDERAL PRIVACY LEGISLATION 16–19 (2020), https://www.brookings.edu/wp-content/uploads/2020/06/Bridging-the-gaps_a-path-forward-to-federal-privacy-legislation.pdf [https://perma.cc/X9AU-AT6Q].

19. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1610 (1999).

20. *See* Robert Muggah, *Digital Privacy Comes at a Price. Here's How to Protect It*, WORLD ECON. F. (Sept. 8, 2021), https://www.weforum.org/agenda/2021/09/how-to-protect-digital-privacy [https://perma.cc/G3ZK-X86E]. *See generally* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814 (2011) (discussing when information should be considered "personally identifiable information").

21. *See* Rani Molla, *People Say They Care About Privacy but They Continue to Buy Devices That Can Spy on Them*, VOX (May 13, 2019, 5:40 PM), https://www.vox.com/recode/2019/5/13/18547235/trust-smart-devices-privacy-security [https://perma.cc/9EDF-NJ7W].

22. *See* Aliza Vigderman & Gabe Turner, *The Data Big Tech Companies Have on You*, SECURITY.ORG (Aug. 23, 2021), https://www.security.org/resources/data-tech-companies-have/ [https://perma.cc/MZS4-DKP4].

23. Kendra Clark, *Will Tech Companies or Regulators Have the Final Say in Our Privacy Debate?*, THE DRUM (Nov. 16, 2021), https://www.thedrum.com/news/2021/11/16/will-tech-companies-or-regulators-have-the-final-say-our-privacy-debate [https://perma.cc/DJG6-4L38].

As a result, information privacy has emerged as a hot-button issue surrounding the consequences of a data-driven society.

The collection of personal data can greatly benefit individuals, businesses, and society at large,[24] but there is also a potential risk of privacy harms.[25] After the recent uptick in record-breaking data breaches,[26] the general response to the commodification of individuals' personal data has been bleak. A 2017 study of the digital privacy environment found that "many Americans fear they have lost control of their personal information and many worry whether government agencies and major corporations can protect the customer data they collect."[27] Despite citizens' mounting distrust in the United States' data protection practices, the legislative response has been underwhelming and insufficient. At the federal level, regulators continue to rely on sector-specific laws and regulations—some of which fail to adequately protect data—to address privacy harms.[28] In addition, many state laws addressing one privacy issue can lead to varying degrees of compliance and incompatible provisions, as demonstrated by

24. Jules Polonetsky & Omer Tene, *Privacy and Big Data: Making Ends Meet*, 66 STAN. L. REV. 25, 25 (2013) ("Big data creates tremendous opportunity for the world economy not only in the field of national security, but also in areas ranging from marketing and credit risk analysis to medical research and urban planning.").

25. "The risks [of personal data collection] include possibilities for surveillance, loss of privacy, discrimination and loss of reputation and autonomy." Jack Teng et al., *Data Collected by Governments Can Be Useful to Researchers, but Only When Accessed Carefully*, THE CONVERSATION (July 31, 2019, 6:57 PM), https://theconversation.com/data-collected-by-governments-can-be-useful-to-researchers-but-only-when-accessed-carefully-116579 [https://perma.cc/HV3U-QUHF].

26. In the last few years, there were massive breaches of sensitive personal data that affected a vast number of individuals. *See, e.g.*, Nicole Perlroth, *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*, N.Y. TIMES (Oct. 3, 2017), https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html [https://perma.cc/H2MW-3ULE] (billions of email accounts were compromised); Seena Gressin, *The Equifax Data Breach: What to Do*, FED. TRADE COMM'N (Sept. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do [https://perma.cc/JW6V-TGXH] (hackers accessed names, Social Security numbers, birth dates, addresses, driver's license numbers, and credit card numbers belonging to users of a major credit reporting agency); Eric Newcomer, *Uber Paid Hackers to Delete Stolen Data on 57 Million People*, BLOOMBERG (Nov. 21, 2017, 8:21 PM), https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data [https://perma.cc/5TXR-NSMR] (compromised data included names, addresses, and phone numbers of Uber riders and drivers around the world).

27. Kenneth Olmstead & Aaron Smith, *Americans and Cybersecurity*, PEW RSCH. CTR. (Jan. 26, 2017), https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/ [https://perma.cc/X5P8-F334].

28. Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELS. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/GR26-AJXP].

the forty-eight state data breach laws.[29] "U.S. citizens and companies suffer from this uneven approach—citizens because their data is not adequately protected, and companies because they are saddled with contradictory and sometimes competing requirements."[30] While the legal rights provided by different state privacy laws only apply to residents of each respective state, the nature of conducting business online makes it highly likely that a company will be a covered entity in multiple states and thus subjected to competing or incompatible state law provisions.[31] Despite these concerns, any attempts to pass federal privacy laws in the last decade "failed to get off the ground."[32]

The regulation of data privacy has far-reaching implications that affect the interests of commercial industries, governmental and non-governmental organizations, and consumers.[33] Congressional action will undoubtedly shape the future of data privacy, so it is vital that legislators consider different perspectives and regulatory approaches as they move forward with structuring a federal privacy law.

III. THE PATCHWORK OF FEDERAL AND STATE REGULATION OF CONSUMER PRIVACY

A. The Limited Federal Sectoral Approach to Regulating Privacy

The United States, despite being home to some of the most advanced technology data companies in the world, lacks a comprehensive federal privacy law that regulates the use and collection of personal information.[34] Instead, the United States has taken a narrowly

29. Depending on the state, one will find different and sometimes conflicting definitions of "breach," the types of personal information protected, the entities that are covered, and enforcement procedures. *Id.*

30. *Id.*

31. For example, the CCPA covers entities that "do[] business in California" and buy, receive, or sell the personal information of "50,000 or more [California] consumers, households, or devices" and does not require a business to be physically located in California. California Consumer Privacy Act, CAL. CIV. CODE § 1798.140(c) (West 2018).

32. Dan Clark, *A Plea for Protection: Will a Federal Data Privacy Law Save the Day?*, YAHOO!: LAW.COM (Feb. 4, 2019, 2:33 PM), https://www.yahoo.com/now/plea-protection-federal-data-privacy-023303428.html [https://perma.cc/SG3F-L4CA].

33. The potential national effects have been illustrated by the GDPR, the toughest privacy and security law in the world, that protects all consumers in the EU and requires virtually all businesses to comply. Rob Sobers, *A Year in the Life of the GDPR: Must-Know Stats and Takeaways*, VARONIS, https://www.varonis.com/blog/gdpr-effect-review/ [https://perma.cc/SXR5-75US] (last updated June 17, 2020).

34. O'Connor, *supra* note 28; Melody McAnally & Jennifer Svilar, *U.S. Privacy Law: Past, Present and Future*, JD SUPRA (Sept. 20, 2021), https://www.jdsupra.com/legalnews/u-s-privacy-law-past-present-and-future-4213418/ [https://perma.cc/Z3PA-6YHA].

tailored sectoral approach to personal data protection by regulating specific types of data and populations.[35] More than a decade ago, many industries preferred the sectoral model because there was more leeway to self-regulate, and some organizations avoided regulation altogether by falling into one of the gaps left by the patchwork of laws.[36] However, in the context of modern digital privacy, the sectoral model has become outdated when compared to other jurisdictions, like the European Union, which regulates privacy using an omnibus model.[37] The gaps narrowed as more laws were passed, and organizations today are often regulated by overlapping laws, leading to inconsistency and uncertainty—especially as technology continues to expand.[38] For example, the Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Rule (COPPA) both address children's personal information,[39] but they intersect and sometimes conflict with each other, leading to a lack of clarity on protections.[40] Another prominent example illustrating uncertainty is the Health Insurance Portability and Accountability Act (HIPAA), the primary

35. Klosowski, *supra* note 6 (describing a mixture of federal laws that regulate limited areas such as health information, credit reports, student education records, and data collection of children under the age of 13).

36. Daniel Solove, *The Growing Problems with the Sectoral Approach to Privacy Law*, TEACH PRIV. (Nov. 13, 2015), https://teachprivacy.com/problems-sectoral-approach-privacy-law/ [https://perma.cc/SYK8-MDPT].

37. *See, e.g.*, GDPR, *supra* note 7.

38. Solove, *supra* note 36.

39. 20 U.S.C. § 1232g (2018); 15 U.S.C. §§ 6501–6506 (2018). FERPA withholds funds from state schools and districts that deny parents access to the records maintained about their children and that disclose their children's personally identifiable information without parental consent. 20 U.S.C. § 1232g (2018). COPPA allows parents to decide when and how personal information about their children is collected, used, and disclosed online by commercial operators. 15 U.S.C. §§ 6501–6506 (2018).

40. *See* Dian Schaffhauser, *The Problems with FERPA and COPPA in 21st Century Learning*, THE JOURNAL (Dec. 5, 2017), https://thejournal.com/Articles/2017/12/05/The-Problems-with-FERPA-and-COPPA-in-21st-Century-Learning.aspx [https://perma.cc/L7ZQ-79GM]. "[Educational technology] 'vendors and educators still have difficulty understanding how best to comply with COPPA in the educational context and FERPA in the digital context' . . . . For example, 'directory information is opt-out under FERPA, but much of that information is protected as opt-in under COPPA.'" *Id.* By way of example, a user "opts in" by taking an affirmative action, such as marking a checkbox on a website, to offer their consent, where the checkboxes are unmarked by default. "Opt-out" is the opposite, where the checkboxes are already marked by default, but the user may withdraw consent by actively unchecking the box. KJ Dearie, *Opt In vs Opt Out*, TERMLY (Sept. 28, 2021), https://termly.io/resources/articles/opt-in-vs-opt-out/#opt-in-opt-out-whats-the-difference [https://perma.cc/QY2W-GPG4].

health privacy law in the United States, which regulates "covered entities" that hold "individually identifiable health information."[41] As health information is increasingly collected, shared, or used by new types of organizations beyond the traditional health care organizations covered by HIPAA, consumers "may incorrectly think HIPAA provides standards for privacy and security in all contexts where their health information is collected, shared, or used."[42]

The primary enforcer of federal privacy and data security issues is the Federal Trade Commission (FTC), an agency with the broadest federal jurisdiction to protect consumer privacy.[43] The FTC is tasked with protecting consumers and competition from "deceptive and unfair business practices," reaching diverse sectors such as retail, advertising, credit reporting, health, and more.[44] The FTC exercises its authority in one of two ways. First, it can act on privacy-specific statutory authority from Congress. Under these statutes, the FTC has the power to bring civil cases against entities that violate specific statutory provisions.[45] For example, COPPA,[46] the Fair Credit Reporting Act (FCRA),[47] and the Gramm-Leach-Bliley Act[48] are federal statutes that explicitly give the FTC regulatory authority to protect consumer privacy—either with rulemaking, enforcement, or both.

Second, outside of the sector-specific framework, section 5 of the Federal Trade Commission Act (FTCA) is the sole alternative to a general privacy law, and authorizes the FTC to take civil action against

41. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

42. U.S. DEP'T OF HEALTH & HUM. SERVS., EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT REGULATED BY HIPAA 4 (2016), https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf [https://perma.cc/E7VV-NK9L].

43. *About the FTC*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc [https://perma.cc/LJ3D-MVD6].

44. *Id*.

45. Thomas Pahl, *Your Cop on the Privacy Beat*, FED. TRADE COMM'N (Apr. 20, 2017, 11:12 AM), https://www.ftc.gov/news-events/blogs/business-blog/2017/04/your-cop-privacy-beat [https://perma.cc/D5AW-JMUL].

46. COPPA exclusively empowers the FTC with the authority to make and enforce rules protecting the personal information of children under the age of thirteen. 15 U.S.C. §§ 6501, 6506 (2018).

47. The FCRA exclusively empowers the FTC to enforce, but not make, rules protecting information collected by consumer reporting agencies such as credit bureaus, medical information companies, and tenant screening services. Fair Credit Reporting Act, 15 U.S.C. § 1681 (2018).

48. The Gramm-Leach-Bliley Act empowers the FTC to enforce, but not make, rules ensuring that financial institutions protect the privacy of consumers' personal financial information. Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq. (2018).

any private entities that use "unfair or deceptive acts or practices in or affecting commerce."[49] Under section 5, the FTC has pursued privacy and data security cases against "social media companies, mobile app developers, data brokers, ad tech industry participants, retailers, and companies in the Internet of Things space."[50] In general, industry entities are permitted to self-regulate consumer data privacy practices, with minimal federal intervention, which is mainly derived from the FTC's section 5 authorization to sue entities that violate the FTCA.[51] The FTC has been exercising its enforcement authority over data privacy violations since the 1990s, starting with its lawsuit in 1998 against the web platform called "GeoCities."[52] This was a seminal case that laid the groundwork for the FTC's continued expansion over the next two decades and the presently ongoing discussions about data privacy regulation.[53] Since 1998, the FTC has brought hundreds of cases against private entities, large and small, to protect the privacy of consumer data.[54] Although many cases resulted in settlement agreements and never reach a judicial decision, industry entities used these agreements as guidelines for their privacy practices.[55] As such, the

49. Federal Trade Commission Act, 15 U.S.C. § 45(a)(1) (2018).

50. FED. TRADE COMM'N, FTC REPORT TO CONGRESS ON PRIVACY AND SECURITY 1 (2021), https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf [https://perma.cc/L5A8-VH26].

51. "Self-regulation is a broad concept that includes any attempt by an industry to moderate its conduct with the intent of improving marketplace behavior for the ultimate benefit of consumers. Self-regulatory organizations typically include private groups . . . ." Deborah Platt Majoras, Chairman, Fed. Trade Comm'n, Self Regulatory Organizations and the FTC 2 (Apr. 11, 2005), https://www.ftc.gov/sites/default/files/documents/public_statements/self-regulatory-organizations-and-ftc/050411selfregorgs.pdf [https://perma.cc/TG6F-8C5X].

52. Rachel Withers, *Before Facebook, There Was GeoCities*, SLATE (Apr. 16, 2018, 8:07 AM), https://slate.com/technology/2018/04/the-ftcs-1998-case-against-geocities-laid-the-ground work-for-facebook-debates-today.html [https://perma.cc/A2JP-9KQF]. "[J]ust as GeoCities was preparing to go public, the FTC launched a complaint against the site, as part of its crackdown on online privacy practices. The FTC alleged that GeoCities was lying to its customers by misrepresenting how it was using their personal information and was therefore in violation of the Federal Trade Commission Act." *Id.*

53. *See id.*

54. "In a wide range of cases, the FTC has alleged that companies made deceptive claims about how they collect, use, and share consumer data [and] failed to provide reasonable security for consumer data . . . spammed and defrauded consumers . . . shared highly sensitive, private consumer data with unauthorized third parties . . ." and more. Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission Comment, WC Docket No. 16-106, at 4–5 (May 27, 2016), https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf [https://perma.cc/MV2Q-TDDG].

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

spread of the FTC's privacy jurisprudence functionally operates as a "body of common law," where the FTC has codified certain norms and standards, developing baseline privacy protections for consumers.[56] These standards have become specific enough to resemble rules that self-regulating entities find useful.[57] Aside from exercising its enforcement and regulatory powers, the FTC regularly publishes reports and makes recommendations to federal legislators.[58] The culmination of the these efforts in the data privacy landscape has bolstered the FTC's experience and flexibility over decades of regulatory work, even with limited resources and minimal congressional support.[59] Nevertheless, the self-regulatory approach is limited, largely due to the lack of explicit statutory direction. Self-regulation is voluntary by definition, so these entities are not necessarily confined to industry standards.[60] Furthermore, the FTC's approach is mostly reactive and relies on conducting market studies, writing reports, and initiating incremental change through civil enforcement.[61] Importantly, the reach of section 5's protections against "deceptive and unfair acts" is limited, particularly in pursuing "unfairness" violations.[62] The FTC has opined that consumers need additional protections beyond the scope of what section 5 can offer, especially as consumer technologies and complex privacy issues continue to evolve.[63]

---

56. *Id.* at 586.

57. *Id.*

58. *See, e.g.*, FED. TRADE COMM'N, *supra* note 50 (discussing areas for improvement, the need for additional resources, and requesting Congressional action on the FTC's authority).

59. Solove & Hartzog, *supra* note 55, at 676.

60. Jedidiah Bracy, *Will Industry Self-Regulation Be Privacy's Way Forward?*, IAPP (June 24, 2014), https://iapp.org/news/a/will-industry-self-regulation-be-privacys-way-forward/ [https://perma.cc/8E5H-UBNG].

61. FED. TRADE COMM'N, PRIVACY & DATA SECURITY—UPDATE: 2018 2–3 (2019), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf [https://perma.cc/SST8-DRT3].

62. "An act or practice is unfair if (1) it causes or is likely to cause substantial injury, (2) the injury is not reasonably avoidable by consumers, and (3) the injury is not outweighed by benefits to consumers or competition." FED. TRADE COMM'N, FTC REPORT TO CONGRESS ON PRIVACY AND SECURITY, *supra* note 50, at 1. The requirements for proving unfairness are more substantial than deceptiveness, and if all three prongs are not satisfied, the FTC cannot bring a case under section 5. *Id.*

63. "While FTC enforcement can help police the most pernicious and deceptive practices in the marketplace, the agency must develop a clear theory of substantial likelihood of harm to consumers . . . . The harm requirement imposes some limitations around how far the FTC can pursue aggressive uses of sensitive data." Terrell McSweeny, *Psychographics, Predictive Analytics, Artificial Intelligence, & Bots: Is the FTC Keeping Pace?*, 2 GEO. L. TECH. REV. 514, 522 (2018).

While the FTC has played an important gap-filling role in the federal regulatory scheme, commentators have questioned whether the agency—with limited capabilities and lacking resources—has the ability to handle future privacy harms.[64] In a recent settlement with Facebook, the FTC fined the social media giant $5 billion and required Facebook to "implement changes to its privacy practices" for allegedly making "deceptive claims about consumers' ability to control the privacy of their personal data."[65] Critics felt that the settlement was too limited to provide sufficient redress, contending that the $5 billion fine was merely a "drop in the bucket compared to Facebook's profits . . . . [T]he FTC did not change Facebook's fundamental business model nor hold Mark Zuckerberg, the CEO, personally liable" for the privacy harms.[66]

Regardless of the FTC's drawbacks, it is likely still the best agency to help regulate and enforce a federal data privacy law—it has decades of experience in the data privacy realm, it has proven itself to be adaptable to new technologies, and it would be easier to provide the FTC with new tools and resources than build a new regulatory agency from the ground up.[67] With the right resources and better support from Congress, the FTC will be able to "rise to the [privacy] challenge."[68] However, these developments will take a few years before the FTC can be effective, so the pressure to enact a federal baseline privacy law still remains.[69] In the absence of adequate federal regulation, states have become the frontrunners of data privacy regulation.

64. *See id.* at 525, 530.

65. Lesley Fair, *FTC's $5 Billion Facebook Settlement: Record-breaking and History-making*, FED. TRADE COMM'N (July 24, 2019, 8:52 AM), https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history [https://perma.cc/6353-47SA].

66. Chris J. Hoofnagle et al., *The FTC Can Rise to the Privacy Challenge, but Not Without Help from Congress*, BROOKINGS (Aug. 8, 2019), https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/ [https://perma.cc/LJ9N-689M].

67. "The prevailing thought among . . . companies and . . . legislators is that the Federal Trade Commission would be the body that governs whatever kind of comprehensive law is passed." Clark, *supra* note 32.

68. Hoofnagle et al., *supra* note 66.

69. *Id.*

B. The Significance of Emerging State Privacy Laws

The relationship between federal and state governments creates opportunities for policy experimentation in regulation,[70] and states have played a vital role, particularly in complex areas such as privacy. The Supreme Court and federal legislators have long acknowledged that state governments function as "laboratories of democracy,"[71] which are "places where governmental innovations can begin and spread" and "flow[] naturally from a federalist system."[72] A key feature of these laboratories is that state legislators have the flexibility to quickly identify unique privacy issues and have often pioneered regulatory approaches before the federal government took action.[73] Speed and flexibility is important in the context of digital privacy, where technology advances more rapidly than the law can keep up with.[74] While the Supreme Court has declined to parse the nuances of state laboratories or discuss definite conditions for their success, most commentators have agreed that state laboratories are valuable to furthering national interests.[75]

A prime example of state laboratories at work in regulating digital privacy occurred in the early 2000s, when the public became increasingly concerned about the harms of unauthorized data access.[76] California initiated policy experimentation by enacting the first data

70. Hannah J. Wiseman & Dave Owen, *Federal Laboratories of Democracy*, 52 U.C. DAVIS L. REV. 1119, 1121 (2018).

71. *Id.* at 1125; *see also* Ariz. State Legislature v. Ariz. Indep. Redistricting Comm'n, 135 S. Ct. 2652, 2673 (2015) ("[T]he States may perform their role as laboratories for experimentation to devise various solutions where the best solution is far from clear." (quoting *U.S. v. Lopez*, 514 U.S. 549, 581 (1995) (Kennedy, J., concurring))).

72. Wiseman & Owen, *supra* note 70, at 1125.

73. Joanne McNabb, *Can Laboratories of Democracy Innovate the Way to Privacy Protection?*, CENTURY FOUND. (Apr. 5, 2018), https://tcf.org/content/report/can-laboratories-democracy-innovate-way-privacy-protection/ [https://perma.cc/5YLF-G2H8]. ("States have been the source of numerous privacy innovations in past years, including laws on identity theft victim rights, data breach notification, limitations on the use of Social Security numbers, cell phone data privacy, cybersecurity, and cyber-exploitation.").

74. Daniel Malan, *The Law Can't Keep Up with New Tech. Here's How to Close the Gap*, WORLD ECON. F. (June 21, 2018), https://www.weforum.org/agenda/2018/06/law-too-slow-for-new-tech-how-keep-up/ [https://perma.cc/5VSY-YEX5] ("Given the . . . extraordinarily fast technological and social change . . . government legislation . . . [is] likely to be out-of-date or redundant by the time [it is] implemented.").

75. Wiseman & Owen, *supra* note 70, at 1129–30 ("The implicit assumptions . . . appear to be that experimentalism will automatically emerge from federalist governance and that the locus of experimentation will be the states.").

76. Juliana De Groot, *The History of Data Breaches*, DIGIT. GUARDIAN (Dec. 1, 2020), https://digitalguardian.com/blog/history-data-breaches [https://perma.cc/PS9W-6S5E].

breach notification statute in 2003, which requires individuals to be notified if their personal information is compromised.[77] Forty-eight states followed suit by enacting their own data breach notification laws.[78] During that same period, several federal bills were proposed, but none came to fruition.[79] As of today, every U.S. state has its own data breach notification law, providing a useful outline for federal legislators to finally pass a federal data breach notification statute in 2019.[80] Even after a federal law was passed, states have continued their policy experimentation by regulating more nuanced issues caused by data breaches. For example, some states have amended their notification timelines,[81] while others have focused on expanding notification requirements to cover insurance companies.[82]

While these state laboratory experiments have proved useful, waiting for state-by-state legislation, which can take years, results in less comprehensive privacy protections. Indeed, it took more than fifteen years for all fifty states to enact data breach notification laws, and federal legislation addressing data breach notifications did not materialize until 2019.[83] The cumbersome issue with enacting piecemeal privacy protections over a long period of time is the resulting patchwork of laws that can cause difficulties with compliance, mainly because

77. CAL. CIV. CODE §§ 1798.29, 1798.82 (West 2009 & Supp. 2021); O'Connor, *supra* note 28.

78. O'Connor, *supra* note 28.

79. *See, e.g.*, S. 1350, 108th Cong. (2003); S. 1326, 109th Cong. (2005); H.R. 1069, 109th Cong. (2005); H.R. 5582, 109th Cong. (2006); S. 239, 110th Cong. (2007); S. 495, 110th Cong. (2007); S. 1178, 110th Cong. (2007); H.R. 2221, 111th Cong. (2009); S. 139, 111th Cong. (2009).

80. *Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGISLATURES (Jan. 17, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/8FTF-A7UA]; 45 C.F.R. § 164.404 (2019) (it should be noted that this law did not preempt state laws, but rather filled in remaining gaps).

81. Connecticut expanded its existing data breach law in several ways, which includes shortening the time businesses have to notify affected Connecticut residents and the Office of the Attorney General of a data breach from ninety days to sixty. Ryan DiSantis et al., *Connecticut Expands Data Breach Notification Requirements and Establishes a Cybersecurity "Safe Harbor,"* JD SUPRA (July 12, 2021), https://www.jdsupra.com/legalnews/connecticut-expands-data-breach-1319049/ [https://perma.cc/JU6J-DYYU].

82. In 2014, California's Department of Insurance posted a notice "request[ing] that all insurers, insurance producers, and insurance support organizations provide the Insurance Commissioner with any notices or information submitted to the Attorney General's Office in accordance with Civil Code § 1798.82(f)." Cal. Dep't of Ins., Notification of Improper Personal Information Disclosures and Security Breaches (Mar. 17, 2021), https://www.insurance.ca.gov/0250-insurers/0300-insurers/0200-bulletins/bulletin-notices-commiss-opinion/upload/NoticeToInsurersDataBreachReq.pdf [https://perma.cc/N269-TRJ9].

83. *See supra* text accompanying notes 76–80.

the online nature of data privacy issues extends to individuals and consumers regardless of state lines. Because every state's data breach notification statute varies significantly in scope and application, "the variations between each state's laws create a complex and burdensome system for companies operating across many jurisdictions."[84] Companies across the country are burdened with reconciling the differences between requirements, usually with timing of notifications and determining the types of "personally identifiable information" covered under applicable state laws.[85] Even where state laws overlap, there may be "nuanced distinctions that make a significant impact on an entity's notification obligations."[86] Accordingly, the data breach notification laws illustrate the great benefits of state laboratories, but also highlight some of the difficulties that come with relying solely on state regulation.

Policy experimentation has reemerged in the burgeoning data privacy crisis, with California kickstarting the trend of state regulatory responses. In 2018, the CCPA was enacted in an effort to give consumers more control over how and when others may collect, process, and sell their personal data.[87] The CCPA currently boasts the strongest privacy protection regime, bestowing wide-ranging rights on California residents regarding their personal data, including: (1) the right to know what personal information a business collects about them and how it is used and shared; (2) the right to delete personal information collected by an entity; (3) the right to opt-out of the sale of their personal information; and (4) the right to non-discrimination for exercising their CCPA rights.[88] In addition to these enumerated rights, the CCPA broadly covers any for-profit business entities "that do business

84. Mark L. Krotoski et al., *The Need to Repair the Complex, Cumbersome, Costly Data Breach Notification Maze*, BLOOMBERG BNA (Feb. 8, 2016), https://www.morganlewis.com/~/media/files/publication/outside%20publication/article/bna-need-to-repair-data-breach-notification-maze-08feb16.ashx [https://perma.cc/9A3K-P7X4]. For instance, a customer's username and security question qualify as "protected information" in California and Florida, but not in other states like Wisconsin and Connecticut. *Id.*

85. *Id*. "While most states' definitions of [personally identifiable information] cover similar ground—social security number, driver's license number, state ID card number and account or credit/debit card number along with an access code—some states have expanded definitions of protected [personally identifiable information] subject to the data breach notification laws, such as a user name/e-mail address and password, and an individual's DNA profile or unique biometric data." *Id.*

86. *Id*.

87. CAL. CIV. CODE § 1798.100 (West 2018).

88. *Id*.

in California" and meet one of three threshold requirements.[89] Due to the interconnectivity and proliferation of entities conducting business online, and the fact that California has the largest economy whose commerce touches nearly every other state,[90] the CCPA covers a vast amount of businesses operating in the U.S.[91]

The CCPA was jumpstarted by Alastair Mactaggart, who pushed for a ballot measure[92] and strongly advocated for privacy protections against "giant corporations [that] know absolutely everything about [consumers], [who] have no rights."[93] Mactaggart's advocacy was a match that struck the tinderbox of public awareness regarding the complexities of personal data collection; the support for strong privacy regulations began to echo through the entire state of California as concerns increased. While consumer advocates strongly supported the most stringent protections available to consumers as provided by the CCPA, industry stakeholders voiced concerns over workability and compliance issues, and some stakeholders urged legislators to carve out exemptions for certain business practices.[94] Several bills were introduced to "make the law easier for businesses to comply with and less disruptive to their operations—even if that means giving them more control over people's data than privacy advocates would like."[95]

89. *California Consumer Privacy Act (CCPA)*, CAL. OFF. OF ATT'Y GEN., https://oag.ca.gov/privacy/ccpa [https://perma.cc/87NW-AT3Q] ("The CCPA applies to for-profit businesses that do business in California and meet any of the following: have a gross annual revenue of over $25 million; buy, receive, or sell the personal information of 50,000 or more California residents, households, or devices; or derive fifty percent or more of their annual revenue from selling California residents' personal information.").

90. Mark J. Perry, *Putting America's Enormous $21.5T Economy into Perspective by Comparing US State GDPs to Entire Countries*, AM. ENTER. INST. (Feb. 5, 2020), https://www.aei.org/carpe-diem/putting-americas-huge-21-5t-economy-into-perspective-by-comparing-us-state-gdps-to-entire-countries/.

91. Sarah Edri, *Does the CCPA Apply to Businesses Outside of California?*, TRUEVAULT (Oct. 21, 2020), https://www.truevault.com/blog/does-the-ccpa-apply-to-businesses-outside-of-california [https://perma.cc/U5MD-WK2J].

92. Mark Sullivan, *How the Tech Industry is Sowing Confusion About Privacy Laws*, FAST COMPANY (Apr. 9, 2021), https://www.fastcompany.com/90622991/alastair-mactaggart-california-privacy-law-interview. "Alastair Mactaggart founded and bankrolled the privacy activism organization that pushed California's landmark privacy law—the California Consumer Privacy Act (CCPA)—into the books in 2018." *Id.*

93. Adler, *supra* note 9.

94. Lobbyists for large technology companies "have quietly backed legislation that privacy experts say would severely weaken [the CCPA]." Issie Lapowsky, *Tech Lobbyists Push to Defang California's Landmark Privacy Law*, WIRED (Apr. 29, 2019, 3:09 PM), https://www.wired.com/story/california-privacy-law-tech-lobby-bills-weaken/ [https://perma.cc/KME2-KLFN].

95. *Id.*

Industry opposition was generally met with doubt from privacy advocates, who worried that industry stakeholders sought to erode consumer rights provided by the CCPA.[96] Not long after the CCPA was enacted, the costliness of state regulation of data collection became apparent: in the continued absence of federal legislative action, a patchwork of state data privacy laws was quickly developing.[97]

In the last couple of years, an increasing number of states followed in California's footsteps and attempted to enact their own similar laws, but with varying provisions.[98] Much like the phenomenon that occurred with the patchwork of data breach notification laws, the rise of other state privacy laws sparked concerns of compliance with conflicting state laws, especially since the CCPA is so pervasive—although the CCPA "does not regulate commercial conduct occurring wholly outside of California . . . it is rare today for every part of commercial activity to occur entirely outside of the most populous state in the country."[99] As such, any "for-profit business that operates an online website [and] collects any information about California residents" is likely a covered entity as long as it meets one of the CCPA's thresholds, regardless of its home state.[100] While the CCPA's benefits of data protection are felt across the country and praised by privacy advocates, industry advocates are lobbying for a federal law that provides uniform rules and compliance requirements to address widening gaps in the patchwork of privacy legislation.[101]

C. The Build-Up to Preemption: The Divide Between State and Federal Interests

"More companies appear to be growing concerned with the idea of having a jumble of and federal and state data privacy laws, especially with the passage of the [CCPA]."[102] Since 2018, the CCPA has

96. *Id.*

97. Clark, *supra* note 32.

98. At the time of writing, over twenty states have introduced privacy bills, but only Colorado and Virginia have successfully passed their respective bills. Lively, *supra* note 10.

99. Edri, *supra* note 91.

100. *Id.*

101. Joseph Duball, *Stakeholders: Despite Setbacks, Federal Privacy Legislation Still Essential*, IAPP (June 3, 2020), https://iapp.org/news/a/luminaries-say-no-time-like-the-present-for-federal-privacy-legislation/ [https://perma.cc/VY9Q-EM7E].

102. Clark, *supra* note 32.

already been expanded.[103] In addition, Virginia and Colorado have successfully enacted their own laws that will take effect in 2023.[104] These state laws came largely in response to the budding data privacy crisis and the public outcry for data protections, which the federal sector has only regulated in small pieces.[105] In the time that has elapsed since the CCPA became operative, proposals for federal legislation have increased from legislators and industry stakeholders, who fear that the CCPA is too strong and makes compliance unreasonably difficult for businesses. The implications of a federal privacy law require discussions about whether the law should preempt existing state laws such as those in California, Virginia, and Colorado, but advocates on all sides have recommended different approaches: some business advocates suggest express preemption that overpowers any state laws on data privacy, while others simply call for a less restrictive federal law.[106] On the other side of the coin, privacy advocates are concerned with the history of failure in federal regulation of privacy issues and worry that advocates on both sides will be unable to agree on the extent of preemption.[107]

The preemption conflict between federal and state interests in the U.S. is hardly new. From a general standpoint, state legislation prioritizes the interests of the state's constituents, which results in regulatory variations across state lines.[108] Conversely, federal legislators are more likely to prioritize national economic policies and preventing inconsistencies among state laws.[109] Too much of a shift from state to federal regulation—or vice versa—may disproportionately favor the

103. The California Privacy Rights Act (CPRA) will expand consumer rights in the CCPA and was approved by California voters via a ballot initiative in 2020. Matthew A. Diaz & Kurt R. Hunt, *California Approves the CPRA, a Major Shift in U.S. Privacy Regulation*, NAT. L. REV. (Nov. 17, 2020), https://www.natlawreview.com/article/california-approves-cpra-major-shift-us-privacy-regulation [https://perma.cc/B8KD-FAAU].

104. S.B. 1392, 2021 Gen. Assemb., Reg. Sess. (Va. 2021); S.B. 21-190, 70th Gen. Assemb., Reg. Sess. (Colo. 2021).

105. *See infra* Section III.A.

106. *See* Clark, *supra* note 32.

107. *Id.*

108. *See* RICHARD A. EPSTEIN & MICHAEL S. GREVE, FEDERAL PREEMPTION: PRINCIPLES AND POLITICS 1 (June 2007), https://www.aei.org/wp-content/uploads/2011/10/20070604_Federalistg.pdf.

109. *Id.* ("Consumer advocates . . . and state officials argue that broad federal preemption claims . . . interfere with the states' historic police power to protect their citizens against corporate misconduct. In response, corporations and federal agencies insist that preemption offers a vital safeguard against unwarranted and inconsistent state interferences with the national economy . . . .").

interests of one group over the other. At this stage, sweeping federal preemption could easily water down privacy protections and unreasonably restrict state power, which is often a valuable tool to address consumer-related harms.[110] However, excessive deference to state regulation would lead to a patchwork of privacy laws with conflicting rules that may perpetuate unpredictability and make it difficult for entities to assess the costs and benefits of compliance.[111] While industry advocates and federal legislators have voiced the most concern over the patchwork issue, the risks can also negatively impact consumers, who might have a difficult time predicting which laws govern a particular situation and determine what their remedial rights are, if any.[112] Consumer advocates seek to prioritize stronger privacy protections, showing more support for the state regulatory approach because of the robust protection it offers for consumers,[113] arguing that preemption is not necessary in the wake of the CCPA and maintaining the belief that preemption would effectively reduce the privacy protections that states have created.[114] The dynamic between state and federal regulatory interests inevitably involves some push-and-pull from advocates on either side of the privacy spectrum. Regardless of the criticisms surrounding the state law patchwork issues and the effectiveness of the CCPA, California's massive undertaking of data privacy protection has confirmed that state action is a significant factor in data privacy regulation, because it stimulated difficult and important dialogue among advocates of state and federal interests and ultimately com-

110. *See infra* Section III.B.

111. *See* Susan J. Stabile, *Preemption of State Law by Federal Law: A Task For Congress or the Courts?*, 40 VILL. L. REV. 1, 11–12 (1995) ("Those subject to a law [should] have the ability to know not only what the law means but whether or when that law is applicable to them . . . [they] should be able to order their primary behavior with knowledge of whether they will be subject to federal law, state law, or both.").

112. *Id.*; O'Connor, *supra* note 28.

113. India McKinney & Gennie Gebhart, *Consumer Data Privacy Advocates to Senate Committee: Here's How to Protect Consumers*, ELEC. FRONTIER FOUND. (May 8, 2019), https://www.eff.org/deeplinks/2019/05/consumer-data-privacy-advocates-senate-committee-heres-how-protect-consumers [https://perma.cc/G7T9-CUDG].

114. *Id.*; Cristiano Lima & John Hendel, *California Democrats to Congress: Don't Bulldoze Our Privacy Law*, POLITICO (Feb. 21, 2019, 5:07 AM), https://www.politico.com/story/2019/02/21/congress-data-privacy-california-1185943 [https://perma.cc/5JPR-GG9T].

pelled legislators to pay closer attention to the need for privacy legislation on a national level.[115] It seems that the establishment of a baseline federal privacy law is on the horizon, but the question that remains is: To what extent should federal legislation preempt state regulatory power?

IV. CONTEXTUALIZING THE SPECTRUM OF PREEMPTION

In response to the CCPA, federal legislators have submitted federal bill proposals with varying levels of preemption, a cornerstone of disagreement among advocacy groups.[116] "As federal lawmakers consider proposals for a federal baseline privacy law in the United States, one of the most complex challenges is federal preemption."[117] "Without federal preemption, state and local governments may create additional privacy laws that make compliance more complex for organizations and create contradictory requirements. . . . Competing laws makes it more difficult to educate consumers about their privacy rights and makes compliance more complicated for organizations," as demonstrated by the data breach notification laws and the emerging patchwork of data privacy laws following the CCPA.[118]

"[P]reemption is a technically complex subject, as well as being politically controversial."[119] Federal preemption is a "ubiquitous feature" of contemporary regulation in the United States, and "shapes the regulatory environment for most major industries."[120] Its pervasiveness gave rise to debate between "proponents of broad federal preemption [who] often cite the benefits of uniform national regulations . . .

115. Among the recent federal bills introduced, the Consumer Online Privacy Rights Act was regarded as one of the most "comprehensive privacy bills" yet, representing a promising step towards reconciling state and federal interests in the wake of preemption. Khouryanna DiPrima & Alysa Hutnik, *A National Federal Privacy Law? Check Out COPRA, the Most Comprehensive Privacy Bill Introduced Yet*, JD SUPRA (Dec. 2, 2019), https://www.jdsupra.com/legalnews/a-national-federal-privacy-law-check-64429/ [https://perma.cc/Y4GW-UXQA].

116. See Fazlioglu, *supra* note 11, for a detailed look at federal bill proposals.

117. Stacey Gray, *Preemption in US Federal Privacy Laws*, FUTURE OF PRIV. F. (June 14, 2021), https://fpf.org/blog/preemption-in-us-federal-privacy-laws [https://perma.cc/C76D-A28M].

118. ALAN MCQUINN & DANIEL CASTRO, INFO. TECH. & INNOVATION FOUND., A GRAND BARGAIN ON DATA PRIVACY LEGISLATION FOR AMERICA 13 (Jan 14, 2019), https://www2.itif.org/2019-grand-bargain-privacy.pdf [https://perma.cc/6HRH-YB6D].

119. Peter Swire & Pollyanna Sanderson, *A Proposal to Help Resolve Federal Privacy Preemption*, IAPP (Jan. 13, 2020), https://iapp.org/news/a/a-proposal-to-help-resolve-federal-privacy-preemption/ [https://perma.cc/59KE-7CCY].

120. JAY B. SYKES & NICOLE VANATKO, CONG. RSCH. SRVC., R45825, FEDERAL PREEMPTION: A LEGAL PRIMER 1 (2019), https://sgp.fas.org/crs/misc/R45825.pdf [https://perma.cc/ZB4R-5XQZ].

[and] opponents of broad preemption [who] often appeal to the importance of policy experimentation . . . and the 'gap-filling' role of state common law in deterring harmful conduct and compensating injured plaintiffs."[121]

The historical controversy surrounding preemption is replicated in the emerging data privacy crisis: major technology and user-based commercial industries want a uniform national law, so they naturally seek support from federal legislators who want the same. By contrast, consumer privacy advocates continue to emphasize the important roles that states play in providing new protections for consumers. Federal privacy legislation should set a national standard and preempt state governments from passing their own laws to the extent that they would conflict with those provisions, but legislators should tread carefully to preserve state laws that have already had such a large impact on data privacy.[122] Further, allowing states to continue playing a role in privacy enforcement will allow efforts of gap-filling where federal legislation may fall short.[123] "The most important goal of preemption analysis is to strike a proper balance between federal and state interests. . . . By definition, preemption disputes involve lawmaking in an area in which both the federal government and the states have the power to legislate."[124]

Federal preemption operates on a spectrum rather than being all-or-nothing. Under the U.S. Constitution's Supremacy Clause,[125] Congress has the power to displace state law in two main ways: (1) express preemption of state law by explicitly stating which state laws are preempted; or (2) implied preemption.[126] If a federal law does not expressly preempt state law, it may do so impliedly. The Supreme Court has recognized in its jurisprudence that, even in the absence of explicit preemption language, a federal statute can implicitly preempt state law

121. *Id.* at 1–2. Proponents of broad federal preemption argue that "businesses with national operations that serve national markets will be subject to complicated, overlapping, and sometimes even conflicting legal regimes." *Id.* (quoting Alan Untereiner, *The Defense of Preemption: A View from the Trenches*, 84 TUL. L. REV. 1257, 1262 (2010)).

122. *See* Swire & Sanderson, *supra* note 119.

123. *Id*.

124. Stabile, *supra* note 111, at 8–9.

125. U.S. CONST. art. VI, § 2.

126. SYKES & VANATKO, *supra* note 120, at 1–2.

if Congress's intent to do so imbues the statute's "structure and purpose" or if nonspecific statutory language makes it clear.[127] The Supreme Court has recognized two general forms of implied preemption: field preemption[128] and conflict preemption.[129]

Beyond preempting conflicting state laws, Congress must decide the extent to which state regulation is permitted in order to complement the varying aspects of the federal framework.[130] The following subsections will examine federal sectoral laws and the extent to which they preempt state laws. Analyzing the ways in which Congress has addressed the complexities of federal preemption in the privacy sphere can provide some insight for legislators to determine the scope of a new federal privacy law that would, at least to some extent, preempt existing state laws like the CCPA.[131]

A. Express Preemption of State Law

The CAN-SPAM Act of 2003,[132] enforced by the FTC, regulates the sending of commercial e-mails, establishing requirements of transparency and control, while also requiring businesses to respect any consumer requests to opt-out or unsubscribe.[133] In stark contrast to the Telephone Consumer Protection Act's deference to stronger state regulations,[134] the CAN-SPAM Act "supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages."[135] When the law came into effect in 2004, it automatically preempted many existing state laws that explicitly overlapped with CAN-SPAM,

127. Wyeth v. Levine, 555 U.S. 555, 565 (2009).

128. SYKES & VANATKO, *supra* note 120, at 17–18. Field preemption of state law occurs where "[c]ongress has manifested an intention that the federal government occupy an entire field of regulation." *Id.* at 17. Where federal regulation becomes "so pervasive" that there is "no room for states to supplement it," federal enforcement is "assumed to preclude enforcement of state laws on the same subject." *Id.* at 17–18.

129. Preemption of conflicting state laws typically occurs when compliance with both federal and state regulations is a physical impossibility, or the challenged state law contradicts with the full purposes and objectives of Congress. *Id.* at 23–25.

130. Stacey Gray, *supra* note 12.

131. *Id.*

132. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 U.S.C. §§ 7701–7713 (2018) [hereinafter ("CAN-SPAM")].

133. *Id.* § 7701.

134. *See infra* Section IV.B.

135. *Id.* § 7707(b)(1).

even those that created stronger restrictions on spam commercial e-mails.[136]

The purpose of express preemption was to reconcile variations in existing laws, but federal law also excluded any provisions that were uniform across state lines, effectively watering down regulation.[137] For example, most of the state laws that were preempted by CAN-SPAM provided individuals with private causes of action and statutory damages, which could have effectively deterred against spammers.[138] Instead, CAN-SPAM shifted all enforcement authority to the FTC without giving the state laws an opportunity to demonstrate whether they could successfully deter violators with other remedies.[139] From the perspective of state constituents, federal preemption unjustifiably prevented injured individuals from seeking financially-attainable remedies.[140] CAN-SPAM's preemption of state laws was evidently too soon, and its foundation was too weak in comparison to the existing state laws. CAN-SPAM represents a situation where the preemption balance was struck incorrectly, in that the federal regime improperly interfered with state authority and resulted in negative consequences that "watered down" privacy protections.[141] Fortunately, legislators can learn from this mistake when crafting a federal privacy law in the future by avoiding express preemption of state privacy laws if the proposed federal law is clearly less protective. In the context of preempting stringent state laws like the CCPA, legislators should consider incorporating provisions that are at least similar in strength.

B. Preemption of Conflicting Laws

The Telephone Consumer Protection Act of 1991 (TCPA) is one example of a federal law that preempts existing state laws to the extent that there is an impossibility of compliance with multiple laws. The

136. Roger Allan Ford, *Preemption of State Spam Laws by the Federal CAN-SPAM Act*, 72 U. CHI. L. REV. 355, 358 (2005).

137. *See generally* Rita Marie Cain, *When Does Preemption Not Really Preempt? The Role of State Law after CAN-SPAM*, 3 I/S J.L. & POL'Y FOR INFO. SOC'Y 751 (2008) (discussing the consequences of express preemption in the CAN-SPAM Act).

138. *Id*. at 760.

139. State law statutory damages ranged from $25 to $1 million per email, while individuals under CAN-SPAM had no recourse other than to wait for spammers to "reach a critical mass and trigger the FTC to take action." *Id*.

140. Stabile, *supra* 111, at 10.

141. *Id*.

TCPA regulates the use of automatic telephone dialing systems, placing restrictions on telemarketing calls and artificial or prerecorded voice messages.[142] Covered entities, such as telemarketers, must obtain express written consent from consumers before calling and provide opt-out mechanisms.[143] The TCPA gives broad authority of enforcement and rulemaking to the Federal Communications Commission (FCC), a federal agency similar to the FTC that is tasked with regulating interstate and international communications.[144]

The TCPA's preemption power is limited to state laws that conflict with certain interstate technical and procedural standards promulgated by the FCC.[145] Private entities may petition the FCC to preempt state telemarketing laws they believe to be in conflict with the TCPA.[146] Notably, the TCPA does not preempt state laws that provide stronger protections against telemarketers, because stronger restrictions would not create a "physical impossibility" of compliance with both laws; telemarketers would be required to follow whichever law is stricter. The TCPA states: "Except for the [technical and procedural standards] prescribed, nothing in this section or in the regulations prescribed under this section shall preempt any State law that imposes more restrictive interstate requirements . . . ."[147]

Following the express limitations set forth in the statute, courts have upheld state marketing laws despite an entity's preemption claims if the state law creates more restrictive requirements or prohibits certain activities.[148] As a result, many states today have their own laws governing telemarketers with stricter provisions, including state registration requirements to engage in telemarketing; prohibiting all

142. 47 U.S.C. § 227(b)(2) (2018).

143. *Id*.

144. *FCC Actions on Robocalls, Telemarketing*, FED. COMMCN'S COMM'N, https://www.fcc.gov/general/telemarketing-and-robocalls [https://perma.cc/ZEK6-69CC] (last updated July 23, 2018); *About the FCC*, FED. COMMC'NS COMM'N, https://www.fcc.gov/about/overview [https://perma.cc/WPJ9-7YC2].

145. 47 U.S.C. § 227 (2018).

146. *See, e.g.*, Consumer & Governmental Affairs Bureau Seeks Comment on CCAdvertising Petition for Declaratory Ruling on Preemption of North Dakota Telemarketing Rules, 69 Fed. Reg. 61380, 61380 (Oct. 18, 2004) (a Virginia-based company that uses prerecorded messages to conduct political polling asked the FCC to preempt certain provisions of North Dakota state law, claiming that the law is inconsistent with the TCPA and the FCC's telemarketing rules, which permit prerecorded political polling messages).

147. 47 U.S.C. § 227(f)(1) (2018).

148. *See, e.g.*, State *ex rel.* Stenehjem v. FreeEats.com, Inc., 712 N.W.2d 828, 831, 834–35 (N.D. 2006) (declining to allow preemption of a North Dakota law prohibiting interstate political calls to state residents, even though it would otherwise be permitted under TCPA regulations).

prerecorded messages; and requiring telemarketers to provide their real names within the first thirty seconds of a call.[149]

It is true that multiple state telemarketing laws with varying levels of restriction on telemarketers can present compliance costs for marketing companies that do business across state lines and make interstate telephone calls. However, the minimal preemption approach has worked well in this arena, given that the compliance barriers associated with these laws are not impractical or complex like in other areas of the digital privacy sphere—the TCPA regulates commercial *telephone* calls, which means that personal data under the TCPA is easily located, through the means of tracking an individual's geographic location using residential landlines.[150] As such, marketing companies are able to readily distinguish between differing states' laws and ensure compliance before making calls to a particular state.[151] Finally, there are regional variations and a lack of national agreement that make federal preemption difficult to achieve; some states ban the types of calls made (e.g., political calls), while others ban calls depending on the time of day.[152] By contrast, a highly preemptive law like the Fair Credit Reporting Act (FCRA)[153] had a strong national consensus on business practices that made preemption more achievable.[154]

Other federal laws that have succeeded with this preemption approach include the Driver's Privacy Protection Act of 1994 (DPPA), the Video Privacy Protection Act of 1988 (VPPA), and the Employee Polygraph Protection Act of 1988 (EPPA).[155] These statutes follow a similar structure to the TCPA, providing a "floor" for preemption by

149. N.D. CENT. CODE § 51-28-02 (2021); ALA. CODE § 8-19A-12 (2021).

150. It is important to note, however, that the TCPA was enacted in 1991, when residential landlines were still common and easy to relate to one particular state.

151. *See generally* Electronic Privacy Information Center Comments, Docket Nos. CG 02-278, DA 05-2975, at 18 (Jan. 13, 2006), https://epic.org/wp-content/uploads/privacy/telemarketing/tcpacom11306.pdf [https://perma.cc/5Z8Z-EU8D] [hereinafter EPIC Comments] (arguing that the "harms" caused by a "patchwork of state laws" is negligible for the telemarketing industry, which has thrived under such a regime for over a decade).

152. *See, e.g.*, *Supreme Court Upholds N.D. Telemarketing Law*, BISMARCK TRIB. (Oct. 10, 2006), https://bismarcktribune.com/news/state-and-regional/supreme-court-upholds-n-d-telemarketing-law/article_19f5595e-92e3-5839-9aa6-c14cf01fb477.html [https://perma.cc/X8ZF-3GQ4]; CONN. GEN. STAT. § 42–288(c) (2021).

153. Fair Credit Reporting Act, 15 U.S.C. § 1681 (2018).

154. Gray, *supra* note 117.

155. 18 U.S.C. § 2721 (2018), *amended by* Pub. L. No. 106–346, § 101(a), 114 Stat. 1356, 1356A–24; 18 U.S.C. § 2710 (2018); 29 U.S.C. § 2009 (2018).

establishing minimum requirements while permitting state governments to create more restrictive rules. They are also similar to the TCPA in that they were older statutes that regulated localized personal data, which does not present complicated compliance costs.

C. Field Preemption

The Cable Act was an amendment to the Communications Act of 1934,[156] which was Congress's attempt to deregulate the cable industry and promote competition in cable communications.[157] The Cable Act's dual approach to federal preemption in the technological communications arena involves giving expansive regulatory authority to the FCC[158] while carving out specific areas in which state law is preserved. Although the statute's original purpose was to provide a strong federal baseline and preserve certain state laws, the Cable Act's progression—particularly through the FCC—provides an example of when federal law ended up occupying the cable communications field "so comprehensively" that it left little to no room for supplementary state legislation.[159] This transition occurred over time as the FCC successfully used its regulatory authority to establish preemptive national standards in court and through promulgating rules.[160] However, to be clear, field preemption does not involve a total preemption of state laws dictated by Congress—rather, it refers to a "clash between a constitutional exercise of Congress's legislative power and conflicting state law."[161]

As a general rule, the Cable Act gives the FCC "express and expansive" jurisdictional authority over certain technologies.[162] The FCC's primary jurisdictional authority dictates the nature and scope

156. The Communications Act of 1934 created and empowered the Federal Communications Commission to oversee and regulate telephone, telegraph, and radio communications. 47 U.S.C. § 151 (2018).

157. Mark R. Herring, *The FCC and Five Years of the Cable Communications Policy Act of 1984: Tuning Out the Consumer?*, 24 U. RICH. L. REV. 151, 151 n.9 (1989).

158. The FCC is an independent U.S. government agency empowered by Congress to regulate interstate and international communications. It has primary federal authority to implement and enforce communications law and regulations. *About the FCC*, *supra* note 144.

159. Murphy v. Nat'l Collegiate Athletic Ass'n, 138 S. Ct. 1461, 1480 (2018) (quoting R.J. Reynolds Tobacco Co. v. Durham County, 479 U.S. 130, 140 (1986)).

160. *See, e.g.*, Capital Cities Cable, Inc. v. Crisp, 467 U.S. 691, 700 (1984) (affirming the FCC's power to preempt state cable laws).

161. *Murphy*, 138 S. Ct. at 1480.

162. Mozilla Corp. v. Fed. Commc'ns Comm'n, 940 F.3d 1, 75 (D.C. Cir. 2019) (quoting Comcast Corp. v. Fed. Commc'ns Comm'n, 600 F.3d 642, 659 (D.C. Cir. 2010)).

of the areas of law it may regulate under different titles of the Cable Act, which include telecommunications services, radio transmissions, and cable services.[163] The FCC also has limited ancillary jurisdiction over certain related subjects if they do not exceed the FCC's general grant of jurisdiction, are reasonably related to its primary jurisdictional obligations, and do not interfere with solely intrastate matters. Jurisdictional authority is a threshold issue of the FCC's preemption authority, but there are additional limitations even if jurisdictional authority is satisfied.

In addition to the jurisdictional requirement, the FCC's preemption must be "consistent with any express preemption provisions in the Cable Act."[164] These provisions preserve state regulatory authority over a particular technology or service and define both the extent of state authority and the limits of federal authority. For instance, section 253 preserves state regulatory authority in a number of areas including: the ability to protect public safety and welfare, ensure the quality of telecommunications services, and safeguard the rights of consumers; however, subsection (d) explicitly leaves room for preemption "to the extent necessary to correct [any] violation or inconsistency" of subsections (a) and (b).[165] Importantly, provisions like section 253(d) leave room for dispute over whether a state law is "inconsistent" with the FCC's actions.

In situations where the federal and state regimes collide, the FCC holds an advantage over state authority due to the Supremacy Clause and the broad authority conferred upon the FTC by the Cable Act. As a result, courts have been hesitant to disturb the FCC's preemption decisions unless the FCC clearly violates its statutory bounds or diverges from congressional intent. In rare cases where preemption would impact the "usual constitutional balance" between states and the federal government, courts have required a "clear statement" from Congress giving the FCC the authority to preempt.[166]

163. Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 98 Stat. 2779, 2785, 2801.

164. CHRIS D. LINEBAUGH & ERIC N. HOLMES, CONG. RSCH. SERV., R46736, STEPPING IN: THE FCC'S AUTHORITY TO PREEMPT STATE LAWS UNDER THE COMMUNICATIONS ACT 8 (2021), https://crsreports.congress.gov/product/pdf/R/R46736 [https://perma.cc/2K9E-7X4D].

165. Cable Communications Policy Act of 1984, 47 U.S.C. §§ 253(a)–(d) (2018); *see also* 47 U.S.C. § 152(b) (2018) (expressly prohibiting the FCC from regulating exclusively intrastate services under its ancillary jurisdiction); 47 U.S.C. § 332(c)(7)(A) (2018) (preserving state regulatory authority over personal wireless service facilities).

166. *See, e.g.*, Nixon v. Mo. Mun. League, 541 U.S. 125, 127 (2004) (holding that the FCC could not preempt a state statute that prevented municipalities and public utilities from providing

The scope of the FCC's preemption authority has been regularly challenged in litigation, especially in complex situations where specific statutory provisions of the Cable Act are at issue. The FCC's power under Congress has frequently prevailed, although its preemption authority is still evaluated on a case-by-case basis, and recent case law demonstrates the difficulty in achieving field preemption power over complex interstate commerce such as communication services. For example, in 2018, the FCC used its preemption authority to reverse a rule imposing net-neutrality requirements on broadband internet access service providers and preempted *any* state laws that would continue to enforce the net neutrality requirements.[167] In turn, the U.S. Court of Appeals for the Sixth Circuit rejected the FCC's "sweeping preemption" of "any" state net-neutrality laws, but left room for the FCC to preempt laws on a case-by-case basis under principles of conflict preemption.[168] Even more recently, the Ninth Circuit Court of Appeals issued a decision to uphold California's net neutrality law, rejecting arguments that the law was barred by field preemption of the Act.[169]

V. A LAYERED APPROACH TO PRIVACY PREEMPTION

In the data privacy arena, it is clear that preemption is necessary, and a federal privacy law is inevitably on the horizon. But preserving the states' robust roles in furthering the national objective is also important. Finding a middle ground for a preemptive federal law involves a careful balancing of interests and regulatory authorities to build a strong national baseline without encroaching on the important

telecommunications services or facilities because the Cable Act lacks a clear statutory statement supporting preemption); Gregory v. Ashcroft, 501 U.S. 452, 460 (1991) (explaining that, because States should have exclusive power to choose their own constitutional officers, federal courts must be certain of Congress's intent before allowing interference and overriding this balance).

167. *See Restoring Internet Freedom*, WC Docket No. 17-108, Declaratory Ruling, Report and Order, and Order, 33 FCC Rcd. 311, 427 (2018).

168. Conflict preemption requires a fact-intensive analysis and applies to "state law that, under the circumstances of the particular case, stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress—whether that 'obstacle' goes by the name of conflicting; contrary to; repugnance; difference; irreconcilability; inconsistency; violation; curtailment; interference, or the like." Mozilla Corp. v. Fed. Commc'ns Comm'n, 940 F.3d 1, 74, 85 (D.C. Cir. 2019).

169. ACA Connects–Am.'s Commc'ns Ass'n v. Bonta, 24 F.4th 1233, 1247–48 (9th Cir. 2022) (citing La. Pub. Serv. Comm'n v. Fed. Commc'ns Comm'n, 476 U.S. 355, 375 (1986)) ("The Communications Act itself reflects a federal scheme that leaves room for state regulation that may touch on interstate services.").

role that states play. Many have proposed a variety of ways to deal with this situation, but this Note argues that the best solution is proposed by the Brookings Institution, which published a report recommending a "tiered approach" to preemption to balance federal and state interests.[170] Specifically, federal legislators could use the general structure of the Consumer Online Privacy Rights Act (COPRA) bill,[171] which provides a comprehensive model of state and federal duality, and revise some of its provisions based on certain aspects of the three models of preemption and related statutes, outlined in Part IV. In addition, adding a sunset clause would require legislators to reassess the impact of the law on state and federal interests and make necessary adjustments to stay on track with technological advancements and any privacy issues that may arise.[172]

A. Revising the General Structure of the Consumer Online Privacy Rights Act

Senator Maria Cantwell of Washington introduced the COPRA bill in late 2019 that would establish privacy rights, outlaw harmful and deceptive practices, and improve data security safeguards on a national scale.[173] This bill, like several others, was introduced with the purpose of preempting state privacy laws such as the CCPA. Although it is not the first federal privacy bill to explicitly address state law preemption, COPRA provides the most comprehensive baseline model that, with some revisions, would align with both federal and state interests.[174]

Much like other privacy bills that have been proposed, COPRA seeks to "give Americans control over their personal data . . . [and establish] strict standards for the collection, use, sharing, and protection of consumer data."[175] Notably, although consumer advocates have generally lobbied against preemption, COPRA has been endorsed by

170. KERRY ET AL., *supra* note 18, at 16–19.

171. Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019).

172. KERRY ET AL., *supra* note 18, at 18–19.

173. *See generally* Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019).

174. Adam Schwartz, *Sen. Cantwell Leads with New Consumer Data Privacy Bill*, ELEC. FRONTIER FOUND. (Dec. 3, 2019), https://www.eff.org/deeplinks/2019/12/sen-cantwell-leads-new-consumer-data-privacy-bill [https://perma.cc/6P3G-2KVN].

175. Press Release, Maria Cantwell, U.S. Sen., Senate Democrats Unveil Strong Online Privacy Rights (Nov. 26, 2019), https://www.cantwell.senate.gov/news/press-releases/cantwell-senate-democrats-unveil-strong-online-privacy-rights [https://perma.cc/M6CJ-JRY7].

several consumer and civil rights advocates—probably because it focuses on preserving consumer control over personal information and leaves room for state policy experimentation outside of preemption.[176]

COPRA expressly limits its preemption provisions by carving out exceptions that preserve state laws and regulatory power. In addition to section 302(b),[177] which lists several types of state laws that COPRA will not preempt, COPRA will not preempt any state law that provides stronger protection for consumer privacy rights. Section 302(c) states, in pertinent part: "[T]his Act shall supersede any State law to the extent such law *directly conflicts* with the provisions of this Act . . . and then only to the extent of such direct conflict. . . . Any State law, rule, or regulation shall not be considered in direct conflict if it *affords a greater level of* protection to individuals protected under this Act."[178]

The language of section 302(c) creates two issues that would undermine the goal of preemption, which is to set a strong national standard for privacy practices, compliance systems, and consumer expectations.

First, the phrase "directly conflicts" is too narrow, inevitably fueling debate over whether a state law "conflicts" with COPRA in a "direct" manner. Instead, COPRA should borrow broader language from statutes like the Cable Act that preempts "inconsistent" laws.[179] It is important to note that interpretation issues with preemption cannot be totally avoided when it comes to splitting regulatory authority between state and federal entities, as demonstrated by some notable cases challenging preemption under the Cable Act, but the FCC's definitions of what is or is not "consistent" has repeatedly prevailed in court.[180] It is also helpful to clarify that COPRA only preempts state laws regulating the collection, processing, sharing, and selling of data covered under

176. *Id.*

177. The types of state laws that will not be preempted include: general consumer protection laws regulating deceptive, unfair, or unconscionable practices; civil rights laws; student and employee privacy rights laws; etc. Consumer Online Privacy Rights Act, S. 2968, 116th Cong. § 302(b) (2019).

178. *Id.* § 302(c) (emphasis added).

179. "Except as provided in section 557 of this title, any provision of law of any State, political subdivision, or agency thereof, or franchising authority, or any provision of any franchise granted by such authority, which is inconsistent with this chapter shall be deemed to be preempted and superseded." 47 U.S.C. § 556(c) (2018).

180. *See, e.g.*, Capital Cities Cable, Inc. v. Crisp, 467 U.S. 691, 704 (1984); Mozilla Corp. v. Fed. Commc'ns Comm'n, 940 F.3d 1, 80 (D.C. Cir. 2019).

the law. As such, the language of section 302(c) should be revised to avoid confusion. The Brookings Institution "recommend[s] the preemption of state laws 'regulating the *collection, processing, sharing, and security* of covered data to the extend such law is inconsistent' with the federal law or regulation."[181]

Second, the phrase "afford a greater level of protection" would permit states to override preemption, simply by enacting privacy laws that place greater restrictions on entities than would the federal law. This provision should be removed, per the Brookings Institution's recommendation, to avoid undermining the strength of federal preemption.[182] Taking this approach would place COPRA in the weakest preemption bucket along with the TCPA, and a patchwork of state laws that conflict with each other—even if they do not conflict with the federal law—would eventually emerge.[183] Because COPRA would regulate a majority of entities doing business across state lines and internet-related data collection practices, personal data is far less localized due to the nature of modern information sharing. As a result, the law would not find as much success with limited preemption over state laws like the TCPA did. Furthermore, although a patchwork of state privacy laws may provoke congressional action, a lack of consensus stemming from the political divide over privacy protections could stall the legislation process.[184]

The layered approach to preemption draws specific features from "preemption of conflicting laws" and "express preemption."[185] The Cable Act also offers important insights into how giving federal agencies strong enforcement and rulemaking authority can create "field preemption" down the line, but giving the FTC express rulemaking authority in an effective manner will require years of congressional support and experimentation,[186] the nuances of which are outside the scope of this discussion. In the meantime, Congress may choose to work towards bolstering the FTC's capabilities and, in the future, reassess integrating stronger FTC rulemaking authority into COPRA's statutory framework.

181. KERRY ET AL., *supra* note 18, at 17 (emphasis added).
182. *Id.* at 15.
183. *Id.* at 16.
184. *Id.* at 4.
185. *See infra* Sections IV.A–B.
186. *See infra* Section III.A.

B. Adding a Sunset Clause

As the final layer to preemption, the Brookings Institution recommends adding a sunset clause to expire certain provisions in the new law.[187] This Note supports this recommendation for two main reasons. First, expiring a provision within the law, on a certain date can reduce the risk of legislative complacency. The looming "sunset" date will leave room for the effects of legislation to unfold naturally, and any provisions that might prove ineffective or require updating are more likely to be addressed upon expiration, when Congress is forced to reassess the law and resolve issues that may have arisen. Of course, it is likely that this scenario will revive the conflict between state and federal interests, where industry advocates might lobby for the sunset clause's removal, while consumer privacy advocates would seek to improve the law and keep the clause in place. An illustrative example of this type of conflict occurred with the FCRA's sunset clause.[188] A sunset clause would assist lawmakers in making difficult decisions relating to the complexities and "experimental nature" of data privacy.[189]

Second, instead of sunsetting the entire law and forcing Congress to address every provision, the sunset clause should focus on provisions that implicate the balance between state and federal interests, much like the FCRA's clause. Balancing state and federal interests requires revisiting and modifying the amounts of regulatory power afforded to each regime. Furthermore, stimulating the privacy dialogue between the two regimes will ensure that concerns from both ends are heard. As a preliminary suggestion, applying a partial sunset clause to the recommended structure of COPRA discussed in this paper would be a good start. Specifically, Congress should implement a sunset

187. KERRY ET AL., *supra* note 18, at 7, 18. A sunset clause is a legal provision that provides for the automatic termination of a government program, agency, or law on a certain date unless the legislature affirmatively acts to renew it. Stephen R. Latham, *Sunset Law*, BRITANNICA (Apr. 8, 2020), https://www.britannica.com/topic/sunset-law [https://perma.cc/9SBV-PY42].

188. "The financial services industry wants Congress to reauthorize national standards, [while] consumer advocates . . . are urging Congress to give the states a role in creating credit policies in the . . . areas they're currently barred . . . ." Eileen Alt Powell, *'Sunset' Provisions in Fair Credit Reporting Act Spark Debate*, ARIZ. DAILY SUN (May 17, 2003), https://azdailysun.com/sunset-provisions-in-fair-credit-reporting-act-spark-debate/article_c9b46271-0580-5a02-b90e-6bfc4c951b59.html [https://perma.cc/K43B-7SGP].

189. *See* RICHARD C. SHELBY, AMENDING FAIR CREDIT REPORTING ACT, S. REP. NO. 108-166, at 6 (2003) (Congress chose to add a sunset clause because the "experimental nature of [the FCRA] provisions" would necessitate future review of the effects).

clause, taking effect between five and eight years[190] from enactment, to reinstate the original language that allows states to enact laws that "afford a greater level of protection" without being preempted.[191] In the meantime, the federal law can offer overdue satisfactory protections that will temporarily reconcile polarizing interests. The sunset clause would give state and federal regulators adequate time to assess the effectiveness of the new federal law and identify the areas in which states can contribute with policy experimentation once the provision expires. Discussions between advocacy groups are certain to emerge, especially since provisions affecting state and federal interests would face risk of termination, and Congress can take these into consideration along with the effectiveness of the current preemption structure when determining whether modifications should be made.

VI. CONCLUSION

The emerging state privacy laws have revived important conversations about the costs and benefits of data privacy to consumers and businesses in the context of the digital era. Likewise, they have revived conversations about the benefits and limitations of federal and state regulatory regimes, and how privacy protections can become too weak or too strong if the correct balance is not struck. In addition, the pace at which data privacy and technology evolves will continue to present challenges for legislation, and lawmakers should be as adaptive as possible, even though it might be impossible for the legal landscape to fully catch up to developments in the digital domain. While the solution presented here does not completely reconcile the polarized views on federal privacy preemption, it will at least provide some compromise and reprieve as lawmakers continue to navigate options to ensure strong privacy protections and uniformity.

190. The inspiration for this time range is drawn from the FCRA's statutory language, which contained a sunset clause of eight years after enactment. Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 (2018).

191. Consumer Online Privacy Rights Act, S. 2968, 116th Cong. § 302(c) (2019).