Missouri Law Review

Volume 84 | Issue 4 Article 8

Fall 2019

The Federalist Regulation of Privacy: The Happy Incidents of State Regulatory Activity and Costs of Preemptive Federal Action

Henry Adams

NOTE

The Federalist Regulation of Privacy: The Happy Incidents of State Regulatory Activity and Costs of Preemptive Federal Action

Henry Adams[*]

I. INTRODUCTION

The impact of society's digital integration is difficult to articulate. It suffices to say much of our lives are now digitized, and digital technologies have yielded immeasurable benefits to the individual and society at large. Change heralds challenge, and the digital paradigm-shift has brought challenges of comparable numerosity and magnitude. Privacy is at the forefront of those challenges. In recent years, the digital industry has been subject to increased scrutiny over the rising number of privacy scandals and perceived market failures related to the collection and use of individuals' personal information.[1] New technologies, market developments, and increases in public attention have culminated in widespread perceptions of privacy threats and abuses.[2] Governments around the globe are responding by revamping their regulation of privacy and the digital industry.[3] In stark contrast, the United States federal government has maintained its rudimental self-regulatory approach.[4] A handful of

* B.S. Ecology and Evolutionary Biology, Tulane University, 2017; J.D. Candidate, University of Missouri School of Law, 2020. I would like to thank Professors R. Lawrence Dessem and Dennis Crouch for their guidance during the writing of this Comment, as well as the Missouri Law Review for its help in the editing process.

1. *See, e.g.*, Rosie Perper, *New Zealand's Privacy Commissioner Lashes Out at Facebook, Calling Those Behind the Company 'Morally Bankrupt Pathological Liars'*, BUSINESS INSIDER (Apr. 8, 2019), https://www.businessinsider.com/new-zealand-privacy-commissioner-calls-facebook-morally-bankrupt-pathological-liars-2019-4 [perma.cc/HVC4-G8CQ]; *see also* Inge Graef, et al., *Fairness and Enforcement: Bridging Competition, Data Protection and Consumer* Law, 8 INT'L DATA AND PRIVACY L. 3, 200 (Nov. 18, 2018), https://doi.org/10.1093/idpl/ipy013 [perma.cc/4Z9V-ARG8] ("Recent years have shown a surge of interest from various enforcement agencies to remedy commercial behaviour exploiting the increasing information and power asymmetries between consumers and firms.").

2. Graef, *supra* note 1, at 202.

3. Bennett Cyphers, et al., *Data Privacy Scandals and Public Policy Picking Up Speed: 2018 in Review*, ELECTRONIC FRONTIER FOUND. (Dec. 31, 2018), https://www.eff.org/deeplinks/2018/12/data-privacy-scandals-and-public-policy-picking-speed-2018-year-review [perma.cc/EY6E-KKXS].

4. ALAN MCQUINN & DANIEL CASTRO, A GRAND BARGAIN ON DATA PRIVACY LEGISLATION FOR AMERICA 2 (Jan. 2019), http://www2.itif.org/2019-grand-bargain-

states, spearheaded by California's enaction of the California Consumer Privacy Act of 2018 ("CCPA"), have moved to fill the gap left by federal inaction.[5] The scope of the CCPA is unrivalled by any previous United States privacy regulation, and with its activation date quickly approaching, industry actors have focused their lobbying efforts in Washington D.C. to the increasing reception of federal legislators.[6] Any congressional action could have major repercussions for state and federal regulators' ability to police the collection and use of citizens' personal information, and accordingly, such action may redefine privacy in the United States. The present scenario raises important questions about federalism and novel informational privacy regulations. Few commentators have addressed the issue directly,[7] and no one has done so recently. What role should the federal government and states play in addressing the privacy concerns of Americans? Should the federal government preempt the CCPA and its progeny in favor of active federal regulation of the digital industry's collection and use of personal information? What are the consequences of allowing the CCPA and similar state laws to regulate the control of their citizens' personal information? This Comment will explore such questions.

Section II briefly introduces contemporary understandings of privacy to contextualize the privacy challenges United States regulators currently face. Section III focuses on the federal government's approach to regulating privacy

---

privacy.pdf?_ga=2.231229721.704269606.1568736616-415320514.1568736616 [perma.cc/P5E2-988Y].

5. Mitchell Noordyke, *US State Privacy Comprehensive Law Comparison*, INT'L ASSOC. OF PRIVACY PROF'LS, INC. (Apr. 18, 2019), https://iapp.org/news/a/us-state-comprehensive-privacy-law-comparison/ [perma.cc/LH63-CBCE].

6. *See, e.g.*, Press Release, U.S. Senate Comm. on Commerce, Science & Transportation, Wicker to Hold Hearing Examining Consumer Data Privacy Issues, (Feb. 8, 2019), https://www.commerce.senate.gov/public/index.cfm/2019/2/wicker-to-hold-hearing-examining-consumer-data-privacy-issues [perma.cc/JQ37-F7KA] ("It is this committee's responsibility and obligation to develop a federal privacy standard to protect consumers without stifling innovation, investment, or competition . . . I hope this first hearing will offer valuable insights that will help set the stage for meaningful bipartisan legislation."). However, the recent stir in Congress may simply fall through, as have numerous previous attempts of federal level privacy legislation. *See* Richard M. Marsh, Jr., *Legislation for Effective Self-Regulation: A New Approach to Protecting Personal Privacy on the Internet*, 15 MICH. TELECOMM. & TECH. L. REV. 543, 556–59 (2009) (discussing previous, and fruitless, federal consideration of enacting privacy legislation).

7. Concerning the regulation of private actors, others have addressed federalism in both the data security and cybersecurity contexts, but the author is only aware of the following inquiries into data privacy regulations: Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 904 (2009); Patricia L. Bellia, *Federalization in Information Privacy Law*, 118 YALE L.J. 868, 870 (2009); Tony Glosson, *Data Privacy in Our Federalist System: Toward an Evaluative Framework for State Privacy Laws*, 67 FED. COMM. L.J. 409, 411 (2015) (approaching the issue with constitutional analysis under the Dormant Commerce Clause).

issues. Section IV focuses on privacy regulation at the state-level, emphasizing the complex relationship between federal and state regulators in national responses to emerging privacy issues. Section V then explains the history and structure of the CCPA before Section VI assesses the implications of the CCPA's enaction and the likely response of federal regulators, concluding with the assertion that strict preemptive action could result in less effective national regulation and prohibit state government attempts to address harm to their constituents. If Congress genuinely wishes to address widespread privacy concerns, it should do so carefully in a way that preserves the ability of states to regulate freely in the area.

II. PRIVACY: BACKGROUND AND LEGAL PERSPECTIVES

The interesting thing about privacy is "nobody seems to have any very clear idea what it is."[8] Labeling privacy as a coherent and consistent right, rather than an evolving conception of social necessity subject to change, simplifies the reality of this "messy and complex subject."[9] Concise, holistic definitions of privacy have evaded scholars since Justice Louis Brandeis and Samuel Warren proffered "The Right of Privacy" to American law.[10] Brandeis and Warren were concerned that new technologies, specifically cameras, would enable private actors to intrude on the privacy of other individuals.[11] As "perhaps the most famous and certainly the most influential law review article ever written,"[12] their work went on to inspire a century of scholarship which has culminated in the irreconcilable "divergent strands" of theory that comprise modern

8. Judith Jarvis Thomson, *The Right to Privacy*, 4 PHIL. PUB. AFF. 295, 295 (1975); Ignacio N. Cofone & Adriana Z. Robertson, *Privacy Harms*, 69 HASTINGS L.J. 1039, 1044 (2018) ("In the forty years since she made this observation, the literature has made little progress on this front.").

9. HELLEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 67 (2010); Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1093 (2002) ("Privacy does not have a universal value that is the same across all contexts. The value of privacy in a particular context depends upon the social importance of the practice of which it is a part.").

10. The two characterized individual privacy as the "right to be let alone." Samuel D. Warren & Louis D. Brandeis, *The Right of Privacy*, 4 HARV. L. REV. 193, 195 (1890); Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2087 (2001) ("Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all.").

11. Warren & Brandeis, *supra* note 10, at 195; Cofone & Robertson, *supra* note 8, at 1045.

12. Melvin Nimmer, *The Right of Publicity*, 19 L. AND CONTEMPORARY PROBS. 203, 203 https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2595&context=lcp [perma.cc/Y8AY-P533].

privacy law.[13] The strand of "informational privacy" provides a foundation for understanding privacy in our digital era.

A. INTRODUCTION TO INFORMATIONAL PRIVACY IN THE DIGITAL AGE

At the emergence of computer technologies in the 1960s, Alan Westin described "informational privacy" as the power of "individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[14] Westin's concept of informational privacy began the "privacy-control" paradigm that forms the basis of modern informational privacy law.[15] Privacy-control emphasizes individuals' ability to control and limit access to information about themselves.[16] In the modern digital era, privacy scholars and legislative frameworks have "gravitated towards the idea of privacy as a personal right to control the use of one's data."[17]

The era of "big data" has revived the subject of informational privacy.[18] Emerging technologies have created "novel forms of data flow,"[19] much of

13. *See, e.g.*, Post, *supra* note 10, at 2087; Solove, *supra* note 9, at 1092 (contenting all previous "attempts to conceptualize privacy by locating the common denominator to identify all instances of privacy have thus far been unsatisfying."); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 422 (1980) (attempting to define privacy as a "distinct and coherent" concept); Edward Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 963 (1964) ("My purpose . . . is to propose a general theory of individual privacy [to] reconcile the divergent strands of legal development-which will put the straws back into the haystack. The need for such a theory is pressing."); KENT GREENAWALT, LEGAL PROTECTIONS OF PRIVACY: FINAL REPORT TO THE OFFICE OF TELECOMMUNICATIONS POLICY 3 (1976) ("Few concepts are more elusive than privacy and attempts at definition have inevitably either been too vague to be of much help or too narrow to catch all aspects of the concept.").

14. ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1660 (1999) ("The conventional wisdom seeks to place the individual at the center of decisionmaking about personal information use by conceiving of privacy as a right of control over data use.").

15. Schwartz, *supra* note 14, at 1659.

16. Cofone & Robertson, *supra* note 8, at 1045; Solove, *supra* note 9, at 1105–06.

17. Schwartz, *supra* note 14, at 1659.

18. Big Data "has commonly come to represent the drastic increase in the volume, variety, and velocity of data that can be analyzed." Joseph Jerome, *Big Data: Catalyst for a Privacy Conversation*, 48 IND. L. REV. 213, 214 (2014); BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? UNDERSTANDING THE ISSUES, FED. TRADE COMM'N (Jan. 2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf [perma.cc/25HK-J26N].

19. Tal Z. Zarsky, *Privacy and Manipulation in the Digital Age*, 20 THEORETICAL INQUIRIES L. 157, 158 (2019).

which consists of "personal information" relating to individuals.[20] The digital industry recognized the profit-potential of collecting, processing, and selling personal information decades ago.[21] As the market has developed, that value has incentivized the proliferation of practices and technologies that "preserve the current status quo of maximum information disclosure."[22] That trend has only intensified as new technologies and the "Internet of Things"[23] integrate consumer products into the digital ecosystem, exacerbating privacy concerns by exponentially increasing the volume, quality, and value of personal information collected from individuals.[24] The result is "some of our most sensitive information ends up amassed in giant, unstructured pools of information kept by tech industry giants."[25] The United States' current informational privacy

20. *See* 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, 1850 (2011); Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1134 (2015).

21. Schwartz, *supra* note 14, at 1689–90 ("For the current online industry, moreover, personal information largely has the quality of nonrivalrous consumption, which means that one firm's utilization of it does not leave less for any other company. As a result, almost all major Internet enterprises and computer companies benefit from developing standards, including new technology, that preserve the current status quo of maximum information disclosure.").

22. *Id*.

23. The "internet of things" is the synthesis of everyday, and often household, items with internet and wireless technologies. It "is the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other). This includes everything from cellphones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of." Jacob Morgan, *A Simple Explanation Of 'The Internet Of Things'*, FORBES (May 13, 2014), https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#19fe9d191d09 [perma.cc/754T-QJSR]; Ejaz Ahmed, et al., *The Role of Big Data Analytics in the Internet of Things*, 129 COMPUTER NETWORKS 2, 459 (2017), https://www.researchgate.net/publication/317617290_The_role_of_big_data_analytics_in_Internet_of_Things ("The explosive growth in the number of devices connected to the Internet of Things (IoT) and the exponential increase in data consumption only reflect how the growth of big data perfectly overlaps with that of IoT."); Jane E. Kirly & Scott Memmel, *Rewriting the "Book of the Machine": Regulatory and Liability Issues for the Internet of Things*, 19 MINN. J.L. SCI. & TECH. 455, 458 (citing industry estimates of internet of things growth).

24. *See* Kirly & Memmel, *supra* note 23, at 458; Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 437–38 (2018) (citing Dimiter v. Dimitrov, *Medical Internet of Things and Big Data in Healthcare*, 22 HEALTHCARE INFORMATICS RES. 156, 156 (2016)).

25. Ohm, *supra* note 20, at 1193 ("Google holds every search query each of us has ever entered, and many have documented how this represents our 'database of intentions,' perhaps the largest database of sensitive information on earth. Facebook maintains a similarly sensitive database of past photos, videos, and status updates. And email providers store massive repositories of sensitive messages. But every one of these providers differs from Health Vault and Mint by collecting sensitive information inci-

predicament was anticipated and reported to federal lawmakers nearly four decades ago:

> [N]ongovernmental invasions of privacy are not limited to individual efforts. Corporations, financial institutions, and other large organizations all seek to compile information on individuals and employ that information to their own benefit. Often the information is obtained, directly or indirectly, from an individual who agreed to permit collection of the data for a particular reason; but the data is frequently centrally compiled and used for other purposes, ultimately giving the entity holding the information tremendous economic, social and even political leverage over the individual. In effect, private institutions have acquired some of the coercive capability which hitherto had been an exclusive power of government. We face a future where information will play a central role, where control of information about a person could be tantamount to controlling that person.[26]

While there are benefits to the digital industry's expansion,[27] there are also great harms.[28] Privacy harms, like the definition of privacy itself, are subject to continuous discussion.[29] Whether you characterize privacy harms as

---

dentally, not in a targeted matter. And these providers also store this sensitive information commingled with less sensitive and nonsensitive information.") (footnotes omitted).

26. Greenawalt, *supra* note 13, at ix–x.

27. *See* WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 382–83 (2016) ("[I]ncreased processing and use of personal data is inevitable and offers enormous value to society.").

28. *See* Ohm, *supra* note 20, at 1190.

29. *See, e.g.*, M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1132 (2011) (reviewing privacy harms and delineating them as subjective and objective); *see also* Ohm, *supra* note 20, at 1125 (reviewing privacy harms); Schwartz, *supra* note 14, at 1656 (personal autonomy); Jerome, *supra* note 18, at 241 (societal trust); Patrick F. Gallagher, *The Internet Website Privacy Policy: A Complete Misnomer?*, 35 SUFFOLK U. L. REV. 373, 380 (2001) (reputational harm); Nathan Newman, *The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google*, 40 WM. MITCHELL L. REV. 849, 852 (2014) (discussing cumulative harms from data mining and behavior advertising); Scott J. Shackelford, *When Toasters Attack: A Polycentric Approach to Enhancing the "Security of Things,"* 2017 U. ILL. L. REV. 415, 440–41 (2017) (discussing the "myriad of ways" consumers can be harmed, including bad credit ratings); *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, FED. TRADE COMM'N (2012) https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [perma.cc/KWY7-WLZF]; *Big Data: Seizing Opportunities, Preserving Values*, EXEC. OFF. OF THE PRESIDENT 51–53 (2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

objective or subjective,[30] the increased concerns of individuals are evidence of some harm occurring.[31] Advancements in consumer technologies exacerbate privacy concerns and increase the already widespread calls for protective legislation.[32] However, United States regulators, particularly at the federal level, "have lagged in grappling with the new problems raised by the digital revolution."[33]

III. OVERVIEW OF THE FEDERAL GOVERNMENT'S REGULATION OF PRIVACY IN THE DIGITAL ERA

The United States "famously does not have omnibus federal data privacy law."[34] Rather than regulate the digital industry's collection and use of personal information in a cohesive framework, Congress has selected certain industries and "sensitive" information types to receive heightened regulation, resulting in a legislative patchwork of sectorial federal regulations. Within those expressly regulated areas, federal agencies actively promulgate rules and police the collection of digital information with civil actions. Outside of that patchwork, the collection and use of personal information is not regulated through codified rules, and industry entities can self-regulate their data practices with minimal policing from federal regulators. The Federal Trade Commission ("FTC") is the primary regulator of the federal scheme, and as the *de facto* digital specialist for the past two decades, the agency has garnished the informal title of the "Federal Technology Commission."[35]

[perma.cc/LW68-7A79] (acknowledging tangible to intangible harms to individuals and groups).

30. *See* Calo, *supra* note 29, at 1131.

31. Defining privacy harms is outside the scope of this discussion of increased U.S. informational privacy regulations. We continue by assuming privacy harms are both tangible and intangible, and that such intangible privacy harms are largely a result of contextual societal and perceptions of digital industry abuse. *See* Solove, *supra* note 9, at 1093 ("The value of privacy in a particular context depends upon the social importance of the practice of which it is a part.").

32. Terrell McSweeny, *Psychographics, Predictive Analytics, Artificial Intelligence, & Bots: Is the FTC Keeping Pace?*, 2 GEO. L. TECH. REV. 514, 518–19 (2018) (citing WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 5 (2018)).

33. Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review Obfuscation: A User's Guide for Privacy and Protest by Finn Brunton and Helen Nissenbaum Cambridge and London: The MIT Press 2015*, 126 YALE L.J. 1180, 1182 (2017).

34. Margot E. Kaminski, *When the Default Is No Penalty: Negotiating Privacy at the NTIA.*, 93 DENV. L. REV. 925, 926 (2016) (citing Paul M. Schwartz, *The Value of Privacy Federalism*, SOCIAL DIMENSIONS OF PRIVACY 324, 324–27 (2015)).

35. Omar Tene, *With Ramirez, the FTC Became the Federal Technology Commission*, IAPP (Jan. 18, 2017), https://iapp.org/news/a/with-ramirez-ftc-became-the-federal-technology-commission/ [perma.cc/N5HH-5ZZJ].

A. The Sectorial Patchwork of Federal Privacy Regulations: The FTC's Active Regulation by Rulemaking and Enforcement in Limited Areas

In the words of the current FTC commissioner Noah Phillips, it "is not an accident of history" that federal regulation "focuses privacy and security rules on the sectors of the economy where Congress has determined such rules are most needed."[36] As noted by Phillips, federal lawmakers have deemed certain types of information "sensitive" enough to warrant formal federal regulation,[37] and the result is the handful of narrow privacy laws tailored to specific sectors of the economy.[38] The sectorial framework regulates "limited types of information, in limited situations,"[39] and each statute empowers a federal agency, commonly the FTC, to promulgate rules and police entity compliance.[40]

The Children's Online Privacy Protection Act of 1998 ("COPPA") is one law in the patchwork that empowers the FTC to protect children's personal information.[41] COPPA requires the FTC to promulgate and enforce rules to give the parents of children "under the age of 13"[42] the ability to control private entities' collection and use of their children's data.[43] COPPA's privacy provisions prohibit the collection and use of child information without first obtaining

---

36. Noah Joshua Phillips, *"Keep It: Maintaining Competition in the Privacy Debate"*, FED. TRADE COMM'N, https://www.ftc.gov/system/files/documents/public_statements/1395934/phillips_-_internet_governance_forum_7-27-18.pdf [perma.cc/83PB-N85P].

37. *Id.*

38. The nature of the sectorial approach has been criticized as inflexible. For example, there is much uncertainty surrounding the application of HIPAA, the federal statute regulating medical records discussed in note 24, to the emerging wearable technology and mobile health industry. *See* Elvy, *supra* note 24, at 498 (internal citation omitted); J. Frazee, et al., *mHealth and Unregulated Data: Is this Farewell to Patient Privacy?*, 13 IND. HEALTH L. REV. 385, 392 (2016).

39. Rebecca Lipman, *Online Privacy and the Invisible Market for Our Data*, 120 PENN. ST. L. REV. 777, 787–88 (2016).

40. *See* Bruce P. Smith, *Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-Help*, 1 J.L. ECON. & POL'Y 171, 173 (2005).

41. 15 U.S.C. §§ 6501–06 (2018); 16 C.F.R. §§ 312 et seq. (2018) (accompanying regulations).

42. 15 U.S.C § 6501(1) (2018).

43. § 6502(b) (listing the specific requirements under the act); *FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information by Amending Children's Online Privacy Protection Rule*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over [perma.cc/LDR6-LURU] ("The Federal Trade Commission adopted final amendments to the Children's Online Privacy Protection Rule that strengthen kids' privacy protections and give parents greater control over the personal information that websites and online services may collect from children under 13."); *Statutes Enforced or Administered by the Commission*, FED. TRADE COMM'N,

meaningful consent from parents.[44] Covered entities must provide parents clear access to a document detailing their COPPA rights and the specific entity's privacy policy.[45] COPPA's privacy provisions empower parents with rights: to know what information is collected from their children;[46] to know how the entity uses that information;[47] to know if and how the entity discloses that information to third-parties;[48] to review any information the entity has already collected;[49] to delete any collected information;[50] and to revoke their prior consent to the entity's practices.[51] COPPA's data security provisions ensure the continued integrity of children's data collected and maintained by the entity.[52]

Other areas in the federal privacy-regulation patchwork that empower the FTC include the regulation of consumer credit information under the Fair Credit Reporting Act ("FCRA"),[53] financial information under the Gramm-Leach-Bliley Act,[54] commercial emailing practices under the CAN-SPAM Act,[55] and consumer health data, which is not subject to Department of Health and Human Services' jurisdiction under the Health Portability and Accountability Act ("HIPAA"),[56] under the Health Information Technology Provisions of American Recovery and Reinvestment Act of 2009.[57]

---

https://www.ftc.gov/enforcement/statutes [perma.cc/DP4J-65Q2] ("This Act [COPPA] protects children's privacy by giving parents tools to control what information is collected from their children online.").

44. 16 C.F.R. § 312.3 (2018) (listing privacy rights under the act).

45. § 312.4(d).

46. § 312.4(b).

47. *Id*.

48. *Id*.

49. § 312.6 ("Right of parent to review personal information provided by a child.")

50. *Id*.

51. § 312.4(d)(2)–(3).

52. § 312.8.

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

54. Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–09 (2018); 16 C.F.R. § 314 (2018) (accompanying regulations).

55. Controlling the Assault of Non-Solicited Pornography and Marketing Act, 15 U.S.C. §§ 7701–7713 (2018).

56. Health Insurance Portability and Accountability Act, Pub. L. No. 104–191, 110 Stat. 1936 (1996) (codified as amended in scattered U.S.C. §§ 26, 29 & 42 (2018)); *see* 45 C.F.R. §§ 160–164 (2018).

57. 42 U.S.C. §§ 17937(a),17937(g) (2018); *see, e.g*., Health Breach Notification Rule, 16 C.F.R. § 318 (2009) (empowering the FTC to promulgate regulatory requirements for entities that breach health information).

B. Federal Regulation Outside of the Privacy Patchwork: The FTC's Passive Approach to Policing Industry Collection and Use of Personal Information

Digital industry entities are generally allowed to self-regulate their collection and use of individuals' personal information with minimal federal oversight, the bulk of which is comprised of the FTC's retroactive enforcement actions against deceptive or unfair practices. Section 5 of the Federal Trade Commission Act ("FTCA") authorizes the FTC to bring civil enforcement actions against private entities using "unfair or deceptive acts or practices in or affecting commerce."[58] While the FTC's Section 5 authority predates modern digital technologies,[59] the agency first applied the enforcement powers to the digital sphere in the late 1990s after the need for internet privacy protections became evident.[60] The FTC's regulation has greatly expanded since 1998.

The FTC's Section 5 enforcement is the only source of federal privacy protections outside of the sectorial legislative patchwork.[61] As of early 2016, the agency had brought "over 500 cases" to uphold the "privacy and security of consumer information."[62] The approach has resulted in the "FTC Common Law,"[63] which is essentially a growing list of information privacy and security no-no's.[64] The FTC's enforcement-based regulation under Section 5 acts as a

58. Federal Trade Commission Act, 15 U.S.C. § 45(a)(1) (2018); Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2246 (2015) (stating "the concepts of deceptiveness and unfairness in the FTC Act are intentionally defined at an extremely broad level."); 15 U.S.C. §6502(b) (2018) (listing the specific requirements under the act).

59. *See* Wheeler-Lea Act of 1938, Pub. L. No. 75-447, 52 Stat. 111 (1938).

60. The humble origins of the FTC's transformation into the "Federal Technology Commission" followed from its first online privacy action against the private entity GeoCities in 1998. For perspective, only 2% of internet sites provided user privacy policies at that time. Phillips, *supra* note 36; *Privacy Online: A Report to Congress*, FED. TRADE COMM'N (1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf [perma.cc/F92G-2R6Y].

61. See *infra* Section III(A).

62. Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, WC Docket No. 16–106 (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 [perma.cc/94EF-L87V].

63. Justin (Gus) Hurwitz, *Data Security and the FTC's Uncommon Law*, 101 IOWA L. REV. 955, 966 (2016) ("In recent years, the Commission has begun referring to its consumer protection efforts – especially those based in its unfairness authority and those relating to privacy and data security – as developing a 'common law' body of rules.").

64. LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1232 (11th Cir. 2018) (explaining the generation of FTC common law through case-by-case litigation).

flexible substitute for static federal statutes. Despite its flexibility, the self-regulatory approach has its limitations.[65]

Section 5 prohibits two distinct forms of conduct: "deceptive" practices and "unfair" practices.[66] The FTC most commonly enforces Section 5's prohibition of "deceptive practices."[67] Entities are liable under Section 5's prohibition of "deceptive practice" for any "representation, omission, or practice" that is "material and likely to mislead consumers acting reasonably under the circumstances."[68] FTC enforcement actions against deceptive practices allow the agency to presume consumer harm while reserving discretion to bring enforcement actions.[69] The retroactive enforcement approach allows private entities to "self-regulate" by publishing their own promises and implementing practices sufficient to maintain those promises.[70] In contrast to the FTC's regulation of "deceptive" practices, Section 5's vague prohibition of "unfair" practices prohibits practices that cause or are likely to cause "substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[71] Despite the theoretical flexibility Section 5's unfairness prohibition provides the FTC with its proactive prohibition and vague definition, the agency's enforcement jurisprudence against unfair practices remains largely undeveloped[72] and

65. Despite the smart-TV industry failing to ensure "private consumer data is adequately encrypted, and that consumers understand that their viewing habits and even some in-room conversations are being hoovered up and monetized," their practices are not prohibited under the FTC's current framework. *See* Jane Kirtley & Scott Memmel, *Too Smart for Its Own Good: Addressing the Privacy and Security Challenges of the Internet of Things*, 22 J. INTERNET L. 1, 20 (2018).

66. 15 U.S.C. § 45(a)(1) (2018).

67. *Id.*

68. Letter from Edith Ramirez, Chairwoman, Fed Trade Comm'n, to Věra Jourová, Commissioner for Justice, Consumers, and Gender Equality, European Commission, *Describing Federal Trade Commission Enforcement of the New EU-U.S. Privacy Shield Framework*, FED. TRADE COMM'N (Feb. 23, 2016), https://www.ftc.gov/public-statements/2016/02/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice [perma.cc/5Y8G-VC53].

69. Philip J. Weiser, *Entrepreneurial Administration*, 97 B.U. L. REV. 2011, 2061 (2017) (internal citations omitted).

70. *Id.* at 2062.

71. 14 U.S.C. § 45(n) (2018).

72. Terrell McSweeny, *Psychographics, Predictive Analytics, Artificial Intelligence, & Bots: Is the FTC Keeping Pace?*, 2 GEO. L. TECH. REV. 514, 520 (2018) (stating the FTC has used its "unfair practices in the privacy and security context . . . more sparingly.").

is "more controversial and susceptible to legal challenges."[73] While rare,[74] private entities have challenged FTC enforcement actions judicially, but those challenges were largely unsuccessful prior to 2018.[75] Recently, the U.S. Court of Appeals for the Eleventh Circuit rebuked the FTC's exercise of its unfairness jurisprudence, concluding the FTC's attempted prohibition applied "a scheme Congress could not have envisioned."[76]

The FTC's impromptu regulation of digital industry privacy abuses has been controversial. Its ability to address national privacy concerns with Section 5 is severely lacking due to the agency's limited capacity, expanding regulatory responsibilities, and fundamental approach to policing privacy abuses.[77] Current[78] and former FTC officials have openly voiced concerns about the agency's regulatory capabilities.[79] The fifty-two employees[80] in the FTC's Division of Privacy and Identity Protection are tasked with regulating the entire United States' economy for not only for privacy abuses but abuses related to identity theft and data security as well.[81] The amount of emerging platforms, technologies, and practices subject to FTC regulation is increasing at a tremendous pace, yet novel threats to consumer privacy remain unaddressed[82] until sufficient public outcry catalyzes the FTC to act.[83] Even

---

73. Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 1012 (2018).

74. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 610–11 (2014) (noting the lack of judicial challenges in FTC enforcement actions against unfair data practices).

75. *See, e.g.*, Fed. Trade Com'n v. Accusearch Inc., 570 F.3d 1187, 1193 (10th Cir. 2009) (stating that Section 5(a) of "the FTCA enables the FTC to take action against unfair practices that have not yet been contemplated by more specific laws."); *see also* Fed. Trade Comm'n v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 617 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015) (rejecting the argument that the FTC failed to provide notice of what constitutes an unfair practice and that an FTC action alleging "unfair" data security practices requires the violation a specifically promulgated rule).

76. LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1237 (11th Cir. 2018).

77. *See, e.g.*, McSweeny, *supra* note 72, at 520.

78. Oversight of the Federal Trade Commission: Hearing Before the Subcomm. On Dig. Commerce and Consumer Prot. of the H. Comm. on Energy and Commerce, 115th Cong. (2018) (statement of FTC Commissioner Rebecca Kelly Slaughter).

79. McSweeny, *supra* note 72, at 520.

80. FISCAL YEAR 2019 CONGRESSIONAL BUDGET, FED. TRADE COMM'N. 41 (2018), https://www.ftc.gov/system/files/documents/reports/fy-2019-congressional-budget-justification/ftc_congressional_budget_justification_fy_2019.pdf [perma.cc/BM7Z-FHUK].

81. *See* Division of Privacy and Identity Protection, FED. TRADE COMM'N., https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/ourdivisions/division-privacy-and-identity [perma.cc/ (last visited Nov. 11, 2019).

82. *See generally* McSweeny, *supra* note 72, at 514.

83. A recent example is the FTC's enforcement against "robo-calls" under the agency's Telemarketing Sales Rule authority. *See* Rosario Méndez, *Robocallers*,

when the FTC chooses to exercise its limited capacity, its ability to prevent foreseeable harms through enforcement of consent decrees has been criticized as ineffective and insufficient,[84] for good reason.[85] Missouri Senator Josh Hawley has repeatedly expressed concerns over the lack of federal regulation under the FTC.[86] More recently, Senator Hawley and Connecticut Senator Richard Blumenthal rebuked the FTC, stating it was time for the agency to "learn from a history of broken and under-enforced consent orders."[87] The agency itself has repeatedly called for Congress to empower it with the authority to levy civil penalties against private entities.[88] Just two months after his 2018 confirmation, FTC chairman Joseph Simons expressed "serious concern" for the agency's "authority with respect to data security and also privacy," stating: "I'm very nervous that we really do not have the remedial authority that we need in order to create a sufficient deterrent to deter the kind of conduct that we want to deter."[89] Simons cited the agency's lack of authority to impose

---

You're Out, FED. TRADE COMM'N, https://www.consumer.ftc.gov/blog/2019/03/robocallers-youre-out [perma.cc/GK3F-ZQ5W].

84. *See* Solove & Hartzog, *supra* note 84, at 605 (2014) ("Indeed, the FTC lacks the general authority to issue civil penalties and rarely fines companies for privacy-related violations under privacy-related statutes or rules that provide for civil penalties.").

85. For example, at the time of the Cambridge Analytica scandal in 2018, Facebook had been under a previous FTC consent decree in 2011 concerning privacy violations. Marc Rotenberg, *How the FTC Could Have Prevented the Facebook Mess*, TECHONOMY (Mar. 22, 2018), https://techonomy.com/2018/03/how-the-ftc-could-have-avoided-the-facebook-mess/ [perma.cc/3ZHT-BNBS].

86. *See e.g.*, Letter from Josh Hawley, Sen., State of Mo., to Joseph J. Simon, Chairman, Fed. Trade Comm'n, WASH. POST (Mar. 11, 2019) https://www.washingtonpost.com/context/letter-to-the-federal-trade-commission-from-sen-josh-hawley/d10e8794-be00-4f4b-878b-5538779adfbd/ [perma.cc/EKQ6-UJVH].

87. Emily Stewart, *Senators on Facebook's Potential $5 Billion Fine: Not Good Enough*, VOX (May 7, 2019), https://www.vox.com/recode/2019/5/7/18535631/facebook-ftc-fine-richard-blumenthal-josh-hawley [perma.cc/H53P-U7TA].

88. For a list of FTC Agency Officials' calls for increased regulatory power, *see Consumer Data Privacy: Examining the European Union's General Data Protection Regulation and the California Consumer Privacy Act, Hearing Before the S. Comm. On Commerce, Science, and Transportation*, GEO. L. CTR. ON PRIVACY & TECH., (Oct. 10, 2018) https://www.commerce.senate.gov/public/_cache/files/baf68751-c9bc-4b15-ab0f-d4a5f719027c/613A226358E5D68237ADC96F3A505F55.moy-2018-10-10-senate-commerce-written-statement-final.pdf [perma.cc/3UT3-WNM7] (Statement of Laura Moy, Executive Director of the Center on Privacy & Technology at Georgetown Law).

89. C. Ryan Barber, *FTC's Limited Data-Privacy Power Makes Chair Joe Simons Nervous*, NAT'L L.J., (June 20, 2018), https://www.law.com/nationallawjournal/2018/06/20/ftcs-limited-data-privacy-power-makes-chair-joe-simons-nervous/?slreturn=20180817094305 [perma.cc/9KK7-LQPS].

civil penalties and the lack of efficient rulemaking authority when stating "Section 5 . . . cannot address all privacy and data security concerns in the marketplace[.]"[90]

In response to the FTC's limited regulatory capability, state governments have increasingly enacted regulations to address the novel issues emerging from the digital industry's collection and use of personal information. Many of these state responses have contributed to the United States' legal privacy landscape by innovating new regulatory approaches and pioneering new areas to regulate, supporting the assertion that state-level regulation is vital for effective national regulation in the digital sphere.

IV. STATE GOVERNMENTS' ROLE IN REGULATING DIGITAL INDUSTRY PRIVACY CONCERNS

The importance of state-level regulation of privacy was acknowledged as far back as 1977 when federal regulators first commended states for creating "innovative [privacy] protections . . . in their regulation of private-sector organizations."[91] Despite the increase in federal privacy regulation since then,[92] that aged sentiment holds true today and the "role of State governments in protecting personal privacy is . . . still enormously important."[93]

The United States regulation of privacy and the digital industry involves a dynamic interplay between state and federal regulators.[94] The circumstances of these interactions vary, but throughout observed examples, state-level activity is beneficial for regulation at the national level. Two general patterns of

90. Richard E. Gottlieb, *FTC Seeks Greater Data Security, Privacy Authority*, MANATT, PHELPS & PHILLIPS, LLP. (Aug. 2, 2018), https://www.manatt.com/Insights/Newsletters/Financial-Services-Law/FTC-Seeks-Greater-Data-Security-Privacy-Authority [perma.cc/D74D-ELT8].

91. *Personal Privacy in an Information Society*, PRIVACY PROTECTION STUDY COMM'N (1977) ("[T]he significant increase in State regulatory efforts to protect the interests of the individual in records kept about him, noted above, has already led a number of States to tryout innovative protections, particularly in their regulation of private-sector organizations.").

92. *See, e.g.*, the Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2018); 16 C.F.R. § 412 (2018) (accompanying regulations); Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–09 (2018); 16 C.F.R. §§ 314.1–314.5 (2018) (accompanying regulations); Family Educational Rights and Privacy Act, 20 U.S.C. § 1232(g) (2018); 34 C.F.R. §§ 99.1–99.8 (2018) (accompanying regulations); Health Information Portability and Accountability Act, Pub. L. No. 104–191, 110 Stat. 1936 (1996) (codified as amended in scattered U.S.C. §§ 26, 29 & 42 (2018)); 45 C.F.R. §§ 160–164 (2018) (accompanying regulations); Fair Credit Reporting Act, 15 U.S.C. §1681 (2018).

93. *Personal Privacy in an Information Society*, *supra* note 91, at 487.

94. *See generally* Bellia, *supra* note 7, at 868 (concluding federal preemption of certain state privacy regulations is necessary); *see also* Schwartz, *supra* note 7, at 902 (arguing against an omnibus federal privacy law that preempts state regulatory efforts).

state involvement are apparent: (1) pioneering state efforts, where states precede federal regulators either by identifying areas lacking necessary regulation or by innovating novel regulatory methods, and (2) gap-filling state efforts, where states enforce existing federal laws to maintain effective national regulation and compensate for the limitations of federal regulators. Any future congressional action must carefully weigh the costs and benefits of limiting states' capacity to regulate within the area.

A. Pioneering Federalism: States Contribute to Effective National Regulation by Preceding Federal Action and Experimenting with Innovative Regulatory Methods

States continue to play a central role in the United States' regulation of privacy in the evolving digital industry.[95] Justice Brandeis rationalized the benefits of state regulation in our federalist system nearly a century ago,[96] and his perspectives remain relevant in the modern digital sphere.[97] Brandeis opined that "state laboratories" confer national benefits by experimenting with novel regulatory methods and identifying new regulatory areas.[98] There are great advantages to states' ability to rapidly respond to issues emerging from the digital industry. States are adept at "identify[ing] areas of regulatory significance" and taking action,[99] which is especially important in the digital sphere where "fast-changing new technologies" can give rise to unforeseen threats to privacy.[100] The relative speed of state legislatures has enabled them

95. Schwartz, *supra* note 7, at 917 ("State privacy law has started the twenty-first century with renewed activity.").

96. New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) ("It is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, [1] serve as a laboratory; and [2] try novel social and economic experiments without risk to the rest of the country."); James A. Gardner, *The New Judicial Federalism: A New Generation Symposium Issue: The "States-as-Laboratories" Metaphor in State Constitutional Law*, 30 VAL. U. L. REV. 475, 478 (1996) (interpreting Brandeis as "saying that state experimentation produces beneficial knowledge, and that states should therefore be permitted and encouraged to experiment to the greatest possible extent.").

97. *See* Schwartz, *supra* note 7, at 917–18.

98. *New State Ice Co.*, 285 U.S. at 311 (Brandeis, J., dissenting); *see* Schwartz, *supra* note 7, at 917–18.

99. Schwartz, *supra* note 7, at 917; Michael S. Greve, *Laboratories of Democracy*, AM. ENTERPRISE INST., at 1 (2001) ("Successful state and local experiments with airline deregulation, welfare reform, and school choice taught valuable lessons, built public confidence in innovative policies, and provided a testing ground for social scientists' models and policy recommendations that might well have gone unheeded in a centralized political environment.").

100. Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 YALE L.J. 785, 821 (2001).

to precede federal action in many digital industry related areas.[101] State regulators confer national benefits by identifying novel targets for regulations and crafting experimental regulatory approaches, which provide useful comparisons for existing state and federal regulators to modify their approaches accordingly.[102]

A notable example of states responding to emerging digital threats involves data breach notification statutes.[103] In an effort to address the increasingly common and harmful practice of unauthorized data access, California pioneered the first data breach notification regulation in 2002 by requiring that breached entities notify consumers in the event their personal information was compromised.[104] By 2007, thirty-three states had enacted similar laws.[105] California's regulatory experiment quickly led to numerous federal proposals, none of which materialized.[106] States compensated for the federal inaction, and by 2009, forty-five states had enacted data breach notification laws.[107] The state-level data breach notification statutes provided federal lawmakers useful templates and industry feedback when it finally moved to fill shortcomings the state laws highlighted.[108] Now, every state and United States territory has enacted data breach statutes,[109] with which states continue to experiment.[110] For

101. *See* Schwartz, *supra* note 7, at 917 (discussing state data breach notification laws).

102. *See id.* at 918; MALCOLM M. FEELEY & EDWARD RUBIN, FEDERALISM: POLITICAL IDENTITY AND TRAGIC COMPROMISE 26 (2008) ("[State] variations may ultimately provide information about a range of alternative government policies and enable the nation to choose the most desirable one.").

103. *See* Schwartz, *supra* note 7, at 917.

104. CAL. CIV. CODE §§ 1798.29, 1798.82 (2017); *see* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 915 (2007).

105. Schwartz & Janger, *supra* note 104, at 915.

106. *See e.g.*, Notification of Risk to Personal Data Act, S. 1350, 108th Cong. (2003), S. 115, 109th Cong. (2005), S. 751, 109th Cong. (2005), S. 1326, 109th Cong. (2005), H.R. 1069, 109th Cong. (2005), H.R. 5582, 109th Cong. (2006), S. 239, 110th Cong. (2007), Data Breach Notification Act, S. 139, 111th Cong. (2009); Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. (2007); Identity Theft Prevention Act, S. 1178, 110th Cong. (2007); Data Security Act of 2007, S. 1260, 110th Cong. (2007), H.R. 1685, 110th Cong. (2007); Data Accountability and Trust Act, H.R. 958, 110th Cong. (2007), H.R. 2221, 111th Cong. (2009).

107. Sasha Romanosky & Alessandro Acquisti, *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives*, 24 BERKELEY TECH. L.J. 1061, 1074 (2009).

108. *See e.g.*, 45 C.F.R. § 164.404 (2019).

109. *Security Breach Notification Laws*, NAT'L CONF. OF ST. LEGIS. (Sept. 29, 2018) http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [perma.cc/7B4V-USBR].

110. Oregon's data breach notification statute was first enacted in 2009, amended in 2015, and has received a subsequent amendment in 2018. Or. Rev. Stat. § 654A.600-628 (2018); *see* Daniel J. Moses, *Oregon Enacts Tougher Data Breach Notification Law*, THE SOC'Y FOR HUM. RESOURCE MGMT. (Apr. 25, 2018),

example, in 2006, Maine's Bureau of Insurance was the first insurance regulator to require insurance entities to notify the agency after suffering a data breach.[111] Numerous other states have followed suit, including Connecticut in 2010,[112] Washington in 2013,[113] and California in 2014.[114] Tennessee's 2016 amendment to its data breach statute illustrates the potential downside of state regulation: ill-contrived policy or patent errors in legislation.[115] Tennessee's 2016 amendment removed an exemption for personal information breaches traceable to employees, but it also removed Tennessee's encryption safe harbor which triggered a duty to notify regardless of whether breached information

---

https://www.shrm.org/resourcesandtools/legal-and-compliance/state-and-local-updates/pages/oregon-enacts-tougher-data-breach-notification-law.aspx [perma.cc/VL24-WXUY].

111. Maine Insurance Regulation Bulletin No. 345 provides that those licensed by the Superintendent – insurers, producers, adjusters, and third-party administrators – are required to notify the Superintendent of breaches that require notice under the notice of Risk to Personal Data Act. Me. Rev. Stat. Ann. 10 §§ 1346–1349 (2005). The notice should include a description of the breach; the number of Maine residences affected; a copy of the notice and other information sent to affected persons; a description of the curative steps taken; and the name and contact information for the person whom the Superintendent may contact. *Id.*

112. Pursuant to Bulletin IC-25, all licensees and registrants of the Connecticut Insurance Department are required to notify the Department of any information security incident which affects any Connecticut residents as soon as the incident is identified, but no later than five calendar days after the incident is identified. *Information Security Incidents*, STATE OF CONN. INS. DEPT. BULLETIN IC-25 (2010).

113. As adopted under notice filed as WSR 13-07-053, all licensees must notify the insurance commissioner within two business days of such licensee determining that notification regarding a security breach of personal health or private information under RCW 19.255.010 and 45 C.F.R. 164 is required to be made to consumers or customers. *Security Breach Notification*, WASH. OFF. OF THE INS. COMM'R WSR 13–07–053 (2013). The notification to the insurance commissioner must be in writing and include the number of customers or consumers potentially affected and what actions are being taken. *Id.*

114. On May 16, 2014, the California Department of Insurance, Legal Division, issued a bulletin to all admitted insurers, insurance producers and other interested persons informing them of California's improper personal information disclosure and security breach notification requirements. *Notification of Improper Personal Information Disclosures and Security Breaches*, CAL. DEPT. OF INS. NOTICE (2014). Per this bulletin, the California Insurance Commissioner requests all insurers, insurance producers, and insurance support organizations to provide to the Insurance Commissioner any notices or information submitted to the Attorney General's Office in accordance with Civil Code § 1798.82(f). *Id.*

115. Tenn. Code Ann. § 47–18–2107 (2017); Thomas Ritter, *Tennessee Amends Its Cybersecurity Law*, THOMPSON BURTON (2016), https://thompsonburton.com/cybersecurity-law/2016/04/14/tennessee-amends-its-cybersecurity-law/ [perma.cc/R9AD-6LLF].

was encrypted.[116] No other state had such a requirement.[117] Encrypted information is useless without an encryption key, so Tennessee's modification essentially imposed liability on entities despite a lack of potential harm to citizens. Tennessee's attempt to update the law by removing the encryption safe harbor was "undoubtedly a noble (and nationally unprecedented) idea," but in response to widespread criticism, the state quickly reinserted the safe harbor while "exhibiting an appropriate level of corrective action."[118] As illustrated by Tennessee, state action has the potential to result in poor policy decisions, but their response highlights states' capacity to quickly make corrective measures in response to national criticisms.

States have also pioneered regulations of private digital industry cybersecurity. "[T]he federal government's cybersecurity regulation [remains] scattered and weak,"[119] and numerous states have moved to impose heightened cybersecurity requirements on private entities.[120] In 2018, thirty-five states introduced "265 bills or resolutions related to cybersecurity."[121] Of those proposals, twenty-two states passed fifty-two heightened requirements.[122] Similar to the pioneering data breach notification regulations, "[s]tate approaches to cybersecurity regulation are providing the Federal government with models to consider as it crafts its own nation-wide laws."[123] One recent example includes South Carolina's regulation of its insurance industry.[124] The success or failure

116. Tenn. Code Ann. § 47–18–2107 (2017); *see* Ritter, *supra* note 115.

117. Ritter, *supra* note 115.

118. *Id.*

119. Jeff Kosseff, *Hamiltonian Cybersecurity*, 54 Wake Forrest L. Rev. 155, 174 (2019). "It may be surprising that an overarching federal cybersecurity law doesn't yet exist in the United States." Kayla Matthews, *Getting Familiar with Cybersecurity Laws: Four Regulations You Should Know*, GLOBAL SIGN GMO INTERNET GRP. (Jan. 10, 2019), https://www.globalsign.com/en/blog/four-cybersecurity-regulations-you-should-know/ [https://perma.cc/9TMF-A82L].

120. *See, e.g.*, COLO. CODE REGS. § 704–1 (2018); 201 MASS. CODE REGS. 17.00–17.04 2 (2019); N.Y. COMP. CODES R. & REGS. 23 § 500.00 (2017).; 3 COLO. CODE REGS., 704–1: R. 51–4.8; 3 COLO. CODE REGS. 704–1: R. 51 – 4.14 (IA) (2019); 4–4 CODE. VT. R. § 8: 8–4 (2019).

121. *Cybersecurity Legislation* 2018, NAT'L CONFERENCE OF ST. LEGIS. (Feb. 8, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx [perma.cc/3MP3-AY2M].

122. *Id.*

123. *How State Cybersecurity Regulations Drive Federal Action*, CORANET (July 10, 2018), https://www.coranet.com/state-cybersecurity-regulations/ [perma.cc/9QXT-P6XW].; Richard Hill, *N.Y. Rule Could Be Model for Cyber-Collaboration*, 108 BANKING REP. (BNA) 458 (Mar. 23, 2017) (discussing how New York's regulations could model similar regulations across the nation); Sabrina Galli, *NYDFS Cybersecurity Regulations: A Blueprint for Uniform State Statute?*, 22 N.C. BANKING INST. 235, 254 (2018) ("[T]he NYDFS regulation adds two more technical safeguards, encryption and multi-factor authentication, that do not currently exist within the FTC regulation.").

124. Insurance Data Security Act, S.C CODE ANN. § 38–99–10–100 (2019).

of South Carolina's pioneering effort, which itself contains a data breach notification requirement,[125] will inform future national regulation of insurance industry data security. New Hampshire recently followed South Carolina's lead by enacting its own data security requirements for insurance entities.[126]

Pioneering state efforts to regulate issues of privacy are particularly relevant here. California was the first regulator, at the federal or state level, to enact a statute requiring online services and websites to publish privacy policies.[127] Delaware followed when it recently enacted a substantially similar requirement, which was modeled after the California statute.[128] State regulators led the charge in addressing issues of online sexual privacy, which went unaddressed prior to the pioneering efforts of California in 2014 despite the rising privacy concerns and individual harm such practices cause.[129] Vermont's 2018 regulation of data brokers exemplifies a proactive state regulation in the area of digital privacy.[130] The data broker industry has long been criticized as an example of the federal government's failure to address informational privacy concerns.[131] Within the digital economy, data brokers function as upstream intermediaries[132] that aggregate and sell the personal information of individuals throughout the country.[133] The FTC investigated the informational privacy

125. § 38–99–40.

126. New Hampshire Senate Bill 194, LEGISCAN (Aug. 5, 2019) https://legiscan.com/NH/text/SB194/id/2037480 [perma.cc/34MM-ABRM]; Alysa Zetler Hutnik, Katie Townley & Lauren Myers, *New Hampshire Enacts New Insurance Data Security Law*, AD LAW SUCCESS (Aug. 14, 2019), https://www.adlawaccess.com/2019/08/articles/new-hampshire-enacts-new-insurance-data-security-law/ [perma.cc/E69C-TQMN].

127. *See* Cal. Online Privacy Prot. Act, Cal. Bus. & Prof. Code § 22575 (2016).

128. Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 764 (2016); *see* Press Release, *Internet Privacy and Safety Agenda Becomes Law with Governor's Signature*, OFF. OF THE ATT'Y GEN OF DEL. (Aug. 7, 2015), http://news.delaware.gov/2015/08/07/internet-privacy-and-safety-agenda-becomes-law-with-governors-signature/ [perma.cc/2C2Y-ZSNW].

129. *See* Citron, *supra* note 128, at 773–76; Danielle Keats Citron, *Revenge Porn Should Be a Crime in U.S.*, CNN (Aug. 29, 2013), http://www.cnn.com/2013/08/29/opinion/citron-revenge-porn/ [perma.cc/CNJ2-JGQW].

130. *See* 9 VT. STAT. ANN. § 2447 (2019) ("Data broker duty to protect information; standards; technical requirements").

131. Yael Grauer, *What Are 'DataBrokers,' and Why Are They Scooping Up Information About You?*, VICE, https://www.vice.com/en_us/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection(Mar. 27, 2018) [perma.cc/Z7YD-ADA2].

132. *See* Rob Frieden, *Two-Sided Internet Markets and the Need to Assess Both Upstream and Downstream Impacts*, 68 Am. U. L. REV. 713, 757–58 (2019).

133. In a 2015 investigation, federal regulators discovered that one single company had compiled "3000 data segments for nearly every U.S. consumer," another company stockpiled consumer data covering "one trillion dollars in consumer transactions," and yet another company added more than "three billion new records each month to its

threats data brokers posed throughout the 2000s.[134] The FTC first identified the need for legislation regulating the practice in 2011[135] and has reiterated that position numerous times.[136] Congress, however, has repeatedly failed to enact targeted regulation.[137] Vermont moved to address the regulatory vacuum in

databases." *Data Brokers: A Call for Transparency and Accountability*, FED. TRADE COMM'N (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [perma.cc/JJM3-4DQ3]; *see also* Ashley Kuempel, Comment, *The Invisible Middlemen: A Critique and Call for Reform of the Data Broker Industry*, 36 NW. J. INT'L L & BUS. 207, 210 (2016); Laura Palk & Krishnamurty Muralidhar, *A Free Ride: Data Brokers' Rent-Seeking Behavior and the Future of Data Inequality*, 20 VAND. J. ENT. & TECH. L. 779 (2018); Rebecca Lipman, *Online Privacy and the Invisible Market for Our Data*, 120 PENN ST. L. REV. 777 (2016).

134. *See, e.g.*, *What Information Do Data Brokers Have on Consumers, and How Do They Use It? Before the S. Comm. on Commerce, Sci., & Transp*., 113th Cong. (Dec. 18, 2013) (statement of Jessica Rich, Director of the Bureau of Consumer Protection, Fed. Trade Comm'n), http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-entitled-what-information-do-data-brokers-have-consumers/131218databrokerstestimony.pdf [perma.cc/2CGC-F3QN]; *Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information Before the S. Comm. on Banking, Hous., & Urban Aff.*, 109th Cong. (Mar. 10, 2005) (statement of Deborah Majoras, Chairman, Fed. Trade Comm'n), http://www.ftc.gov/os/testimony/050310idtheft.pdf [perma.cc/J7Q3-MYYJ]; *The Information Marketplace: Merging and Exchanging Consumer Data*, FED. TRADE COMM'N (Mar. 13, 2001), http://www.ftc.gov/bcp/workshops/infomktplace/index.shtml [perma.cc/43EF-ZF74]; *see also* Press Release, *Information Flows: The Costs and Benefits Related to the Collection and Use of Consumer Information*, FED. TRADE COMM'N (June 18, 2003), http://www.ftc.gov/news-events/press-releases/2003/06/ information-flows-costs-and-benefits-consumers-and-businesses [perma.cc/TZ3V-3R69].

135. *Legislative Hearing on H.R. 2221, the Data Accountability and Protection Act, and H.R. 1319, the Informed P2P User Act Before the H.R. Comm. on Energy & Commerce*, 111th Cong. (2009) (statement of Eileen Harrington, Acting Director of the Bureau of Consumer Protection, Fed. Trade Comm'n), http://www.ftc.gov/sites/default/files/documents/public_ statements/prepared-statement-federal-trade-commission-legislative-hearing-h.r.2221-data-accountability-and-protection-actand-h.r.1319-informed-p2p-user-act/p064504peertopeertestimony.pdf [perma.cc/S5WW-J6B5].

136. *The Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission Before the S. Comm. on Commerce, Sci., & Transp*., 112th Cong. (2012) (statement of Jon Leibowitz, Chairman, Fed. Trade Comm'n), http://www.ftc.gov/os/testimony/120509privacyprotections.pdf [perma.cc/FPF6-27QE]; *Data Brokers: A Call for Transparency and Accountability*, *supra* note 133; BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? UNDERSTANDING THE ISSUES, *supra* note 18.

137. *See* Data Broker Accountability and Transparency Act, S. 2025, 113th Cong. (2014); The Data Accountability and Trust Act of 2014, H.R. 4400, 113th Cong. (2014).

2017[138] and subsequently passed legislation in November of 2018,[139] implementing regulations in the following month.[140] The Vermont legislation specifies conduct related to the use and collection of personal information that is explicitly prohibited, such as acquiring personal information by fraud and using personal information for the purposes of engaging in fraud, harassment, or discrimination.[141] In addition, it requires "data brokers"[142] to establish and maintain "a comprehensive information security program" and register annually with the Vermont Attorney General.[143]

B. Synergistic Federalism: States Fill in Gaps of Existing Federal Regulations and Contribute to Ongoing Cooperative Efforts

States have played an important legislative gap-filling role to bolster existing federal privacy regulations in the digital sphere.[144] California, Texas, and Delaware have enacted legislation to strengthen federal privacy protections for children's data, bolstering the sectorial federal framework of COPPA.[145]

---

138. T.J. Donovan, Vermont Att'y Gen., *Data Brokers*, OFF. OF THE VT. ATT'Y GEN. (Dec. 5, 2017), https://ago.vermont.gov/blog/2017/12/05/data-brokers/ [perma.cc/K3JN-8QSQ] ("On June 8, 2017, the Governor signed S.72 into law. Section 2 of this bill mandates: On or before December 15, 2017, the Commissioner of Financial Regulation and the Attorney General, in consultation with industry and consumer stakeholders, shall submit [recommendations concerning data aggregator regulations].").

139. 9 Vt. Stat. Ann. §§ 2430, 2433, 2446 & 2447 (2018).

140. *Guidance on Vermont's Act 171 of 2018 Data Broker Regulation*, OFF. OF THE VT. ATT'Y GEN., (December 11, 2018), https://www.sec.state.vt.us/media/914592/2018-12-11-vt-data-broker-regulation-guidance.pdf [perma.cc/BK6G-YBHH].

141. *Id.* at 11; 9 VT. STAT. ANN. § 2431 (2019).

142. 9 VT. STAT. ANN. § 2433(4)(A) (2019) (defining a data broker as any "business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship.").

143. §§ 2446, 2447.

144. Bellia, *supra* note 7, at 882 (noting the "importance of federal leadership in information privacy problems, with the adoption of a federal statute creating the momentum for adoption of state law."); *see* State Laws Related to Internet Privacy, NAT'L CONF. OF ST. LEGIS. (Aug. 13, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx#ISPs [perma.cc/Q9JB-N37V].

145. 6 DEL. CODE ANN. § 1204C (2016); CALIF. BUS. & PROF. CODE §§ 22580–22582; Citron, *supra* note 129, at 780; *Children's Apps Collected Personal Information*, FOX SAN ANTONIO NEWS (Nov. 4, 2015), http://foxsanantonio.com/news/tech/childrens-apps-collected-personal-information-11-06-2015 [perma.cc/BTM6-JT3R] (discussing the Texas Attorney General's cases against children's app developers and agreements not to collect location data).

Delaware has also enacted legislation extending information privacy protections to digital book services ("e-books")[146] similar to those federally established over video viewership histories by the Video Privacy Protection Act.[147] More recently, New York promulgated a cybersecurity regulation for business entities operating within the financial industry, supplementing those provided by the federal Gramm-Leach-Bliley Financial Modernization Act.[148] State action may also occur in response to federal retrenchment of privacy protections. Two years after the Federal Communications Commission repealed the "net-neutrality" regulation of Internet Service Providers ("ISPs") in 2016, twenty-four states moved to enact legislation granting their citizens the ability to restrict ISPs' collection and use of personal information.[149] Nevada and Minnesota currently have such restrictions in place.[150]

Perhaps nowhere is the cooperation between state and federal regulators more apparent than in the activity of state attorneys general.[151] Inspired by the FTC,[152] state attorneys general enjoy "a synergistic relationship with federal agencies working on privacy and data security issues."[153] State attorneys general often collaborate together to address national privacy issues.[154] In the past decade, a majority of state attorneys general have participated in "one or more multistate investigations spearheaded by privacy pioneers."[155] For example, in 2012, thirty-nine state attorneys general participated in a unified action against Google to address digital privacy concerns.[156] State attorneys general have also played an increasingly important role in experimenting with enacting novel legislative regulatory frameworks within their states and beyond.[157]

---

146. 6 DEL. CODE ANN. § 1206C (2016).

147. *See, e.g.*, The Video Privacy Protection Act of 1988. 18 U.S.C § 2710 (2018); Baker Hostetler, *The Privacy Protection Act: Watching the Court Through Crossed Eyes*, DATA PRIVACY MONITOR (Mar. 7, 2018) https://www.dataprivacymonitor.com/information-governance-2/the-video-privacy-protection-act-watching-the-courts-through-crossed-eyes/ [perma.cc/X3EK-NWMU].

148. 23 N.Y. COMP. CODES R. & REGS. § 500, *et seq.* (containing the cybersecurity regulations promulgated by the New York State Department of Financial Services in March 2017).

149. 2018 Privacy Legislation Related to Internet Service Providers, NAT'L CONF. OF ST. LEGIS. (May 13, 2019) http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-internet-service-providers-2018.aspx [perma.cc/Z9N5-6HVW].

150. NEV. REV. STAT. ANN. § 205.498 (1999); MINN. STAT. §§ 325M.01–325M.09 (2019).

151. *See generally* Citron, *supra* note 128, at 747.

152. *Id.* at 755.

153. *Id.* at 791.

154. *Id.* at 793 (illustrating the unified action thirty-nine state attorneys general offices took against Google in 2012).

155. *Id.* at 758.

156. *Id.* at 793.

157. *Id.*

C. Preemptive Federal Privacy Legislation: The Consequences of Limiting States' Regulatory Capacity in the Digital Sphere

In 2004, the federal government expressly preempted thirty-three state regulations targeting spam emailing.[158] The Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 ("CAN-SPAM") set a ceiling for state regulations and preempted stricter state laws.[159] The purpose of CAN-SPAM was to harmonize variations in existing state spam laws.[160] However, the federal legislation excluded certain standards that were uniform across state laws and imposed much looser regulatory requirements.[161] In addition, while most preceding state regulations created a private cause of action for individuals,[162] the FTC was exclusively empowered with CAN-SPAM enforcement.[163] Because CAN-SPAM was enacted before the benefits and detriments of the various state law approaches became apparent, it ultimately hindered the effectiveness of national regulation in the area.[164] The legislation has failed to achieve its intended purposes,[165] and CAN-SPAM remains an important lesson that where "the federal law is weak and preempts the state law, we probably would be better off without it."[166]

States clearly have an important role in addressing the digital era's finicky privacy issues, but all previous state privacy regulations are dwarfed by the scope of California's Consumer Privacy Act of 2018. Now, the issue is whether the nature of the CCPA is fundamentally different than preceding state privacy actions, and if so, whether it is so different as to warrant federal occupation and potential preemption.

---

158. 15 U.S.C. § 7707(b) (2018); *see* 15 U.S.C. § 7701(a)(11) (2018).

159. § 7707(b).

160. Rita Marie Cain, *When Does Preemption Not Really Preempt? The Role of State Law After Can-Spam*, 3 J.L. & POL'Y FOR INFO. SOC'Y 751, 758 (2008).

161. *Id.*

162. *Id.* at 760.

163. *Id.* at 759.

164. *Id.* ("Therefore, there was never any meaningful opportunity to see if these remedies actually could make a difference in combating the spam problem before they were preempted by federal law.").

165. Daniel Nasaw, *Federal Law Fails to Lessen Flow of Junk E-Mail*, WALL ST. J. Aug. 10, 2004, at D2; *see* John Soma et al., *Spam Still Pays: The Failure of the CAN-SPAM Act of 2003 and Proposed Legal Solutions*, 45 HARV. J. ON LEGIS. 165, 171–74 (2008) (providing an overview of proposed non-legal solutions to the spam problem); David J. Rutenberg, *Silence of the Spam: Improving the Can-Spam Act by Including an Expanded Private Cause of Action*, 14 VAND. J. ENT. & TECH. L. 225, 245 (2011) (The federal anti-spam law has proven to be very ineffective in preventing spam.); *see also* Tom Zeller, Jr., *Law Barring Junk E-Mail Allows a Flood Instead*, N.Y. TIMES (Feb. 1, 2005); David McGuire, *A Year After Legislation, Spam Still Widespread; Technology Seen as Best Deterrent*, WASH. POST, Jan. 4, 2005, at E5.

166. Jordan M. Blanke, *"Robust Notice" and "Informed Consent:" the Keys to Successful Spyware Legislation*, 7 COLUM. SCI. & TECH. L. REV. 2, 81 (2006).

V. CALIFORNIA'S CONSUMER PRIVACY ACT OF 2018

The digital industry cannot remedy privacy concerns through competition alone,[167] and in response to federal inaction, state-level regulators have played an important role in addressing privacy concerns to the benefit of their citizens and the nation as a whole.[168] California enacted the CCPA within this context.[169] Alastair Mactaggart, the CCPA's primary backer,[170] drafted the CCPA with the intent to "slowly dry up the supply of personal information that companies could buy or trade on the open market" by forcing companies into compliance.[171] Mactaggart struggled during his initial campaign in January 2018[172] and faced strong opposition from Silicon Valley business interests.[173] The struggle ended months later, in March of 2018, when Facebook's Cambridge Analytica Scandal broke, catalyzing support for Mactaggart's bill. Following the largest privacy scandal in history,[174] "all [CCPA campaigners] had to say was data privacy" to receive support from concerned Californians.[175] The CCPA's expansive scope and provisions codifying tenets of information privacy control are novel to the landscape of United States privacy regulation.

---

167. Frank Pasquale, *Privacy, Antitrust, and Power*, 20 GEO. MASON L. REV. 1009, 1010 (2013); Schwartz, *supra* note 14, at 1697 ("As the industry is currently configured, it benefits from standards that accomplish the following: promote maximum disclosure of personal data; establish a poor level of transparency; offer no effective procedural or substantive rights; and establish hollow oversight.").

168. *See* John A. Rothchild, *Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (or Anywhere Else)*, 66 CLEV. ST. L. REV. 559 (2018).

169. CAL. CIV. CODE §§ 1798.100–1798.196 (2018).

170. Ben Alder, *California Passes Strict Internet Privacy Law With Implications For The Country*, NPR (June 29, 2017), https://www.npr.org/2018/06/29/624336039/california-passes-strict-internet-privacy-law-with-implications-for-the-country [perma.cc/ZTN9-RHE6].

171. Nicholas Confessore, *The Unlikely Activists Who Took On Silicon Valley — and Won*, N.Y. TIMES MAG. (Aug. 14, 2018) https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html [perma.cc/QJW7-DB9X].

172. *Consumer Data Privacy: Examining the European Union's General Data Protection Regulation and the California Consumer Privacy Act, Hearing before the U.S. Senate Committee on Commerce, Science, and Transportation*, 115th Cong. 8 at 2 (2018) (statement of Alastair Mactaggart, Chair, Californians for Consumer Privacy).

173. Confessore, *supra* note 171.

174. Christopher Wylie, *Cambridge Analytica a Year on: 'A Lesson in Institutional Failure'*, THE GUARDIAN (March 17, 2019), https://www.theguardian.com/uk-news/2019/mar/17/cambridge-analytica-year-on-lesson-in-institutional-failure-christopher-wylie [perma.cc/MB8K-EA8J]. The Cambridge Analytica Scandal represents a turning point in global perspectives on digital privacy. The scale of the incident, the public's reception, the widespread medical coverage, and the secrecy of the widespread practices at issue were unprecedented. *Id*.

175. Confessore, *supra* note 169.

A. CCPA's Informational Privacy Protections.

The CCPA overhauls the FTC's passive digital privacy regulation,[176] and it operationalizes the individual-centered "privacy-control" theories of Alan Westin's definition of informational privacy.[177] The CCPA empowers Californians with control over the collection and use of their data,[178] including: (1) the right to know what personal information is being collected about them;[179] (2) the right to delete any personal information collected by an entity;[180] (3) the right to know whether their personal information is sold or disclosed and to whom, and to opt-out of future sales;[181] (4) the right to access their personal information; and (5) the right to nondiscriminatory pricing for services and products while exercising their right to opt-out of data collection.[182]

The CCPA represents an unprecedented development in United States privacy law. It sweepingly, and in no terms precisely, establishes a framework to bolster individual privacy in the modern information economy.[183] Much of the CCPA's expansive scope is due to its broad definitions of the personal information and the entities and practices it subjects to compliance.

---

176. "Notice-and-choice is a procedural rule in that, as long as it follows the prescribed procedures, tendering notice and obtaining consent, a data processor may collect any private information and use it for any purpose. A substantive privacy rule, on the other hand, deems certain conduct impermissible even with notice and consent." Rothchild, *supra* note 166, at 564 (suggesting the substantive right that a "company should be forbidden to condition provision of a good or service to a consumer on the consumer's consent to collection or use of private information that is not required for provision of the good or service."); *see* Assemb. B. 375, 2017–18 Reg. Sess. § 2(i)–(5) (Cal. 2017) (enumerating rights).

177. *See* Westin, *supra* note 14; CAL. CIV. CODE § 1798.140(7)(g) (2018) ("'Consumer' means a natural person who is a California resident"); *see also* Cal. Civ. Code § 1798(2)(a) (2018).

178. *See* Assemb. B. No. 375, 2017–18 Reg. Sess. § 2(h) (Cal. 2017).

179. CAL. CIV. CODE § 1798.110(a), (b) (2018).

180. § 1798.105(a) ("consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer."); § 1798.105(b) ("Consumer rights regarding deletion of personal information collected by businesses; disclosure; deletion requests; exceptions.").

181. § 1798.120(a) ("A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information.").

182. § 1798.125(a)(1).

183. Chris Achatz, *California Consumer Privacy Act: What You Need to Know*, KO LAW FIRM (Jan. 15, 2019), https://kofirm.com/california-consumer-privacy-act-need-know [https://perma.cc/8RGS-3DMJ].

The CCPA's definition of personal information is broad and non-exclusive.[184] "[O]ne would be hard-pressed to conceive of any data that is not" included in the CCPA.[185] The types of information the CCPA covers "includes, but is not limited to" the following: physical characteristics or descriptions, "audio, electronic, visual, thermal, olfactory, or similar information," aliases, account names, postal addresses, purchasing histories, internet activity information, geolocation data, and "[i]nferences drawn [from these types of information] to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."[186] Information is only subject to the CCPA if it "identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household[.]"[187] However, it exempts "publicly available information that is lawfully made available to the general public from federal, state, or local government records."[188] At the cost of more confusion, it is sufficient to state that the CCPA "applies to a much broader data set than GDPR[189] or any United States privacy law to date,"[190] and for covered businesses, mere "GDPR prep is not going to be sufficient."[191]

---

184. § 1798.140 (incorporating personal information defined in CAL. CIV. CODE § 1798.80 (2010)).

185. Michael Hahn & Matthew Savare, *The California Consumer Privacy Act's Radical Impact on the Digital Ad Ecosystem*, BLOOMBERG NEWS AUTHORITY: INSIGHTS (Aug. 9, 2018), [perma.cc/EJA3-ZVVS].

186. This is a non-exclusive list of the CCPA's non-exclusive definition of "personal information." CAL. CIV. CODE § 1798.140(o)(1)(B) (2018) (incorporating personal information defined in CAL. CIV. CODE § 1798.80 (2018)).

187. § 1798.140(o)(1).

188. § 1798.140 (o)(2).

189. The General Data Protection Regulation, or GDPR, is the European Union's most recent omnibus personal digital privacy regulation which was enacted in 2016 and became effective in 2018. Council Directive 9398/15 of June 11, 2015, Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf [perma.cc/TYF9-J7YY].

190. *Sweeping New Compliance Obligations: The CCPA's Impact on Financial Services*, DAVIS WRIGHT TREMAINE LLP (Jan. 24, 2019), https://www.privsecblog.com/2019/01/articles/california-consumer-protection-act-ccpa/sweeping-new-compliance-obligations-the-ccpas-impact-on-financial-services/ [perma.cc/52VX-5E66] ("For most consumer-focused industries, the CCPA will be a game-changer – imposing costly compliance burdens, and creating significant enforcement and litigation risks.").

191. *Leveraging Your GDPR Compliance Investment for CCPA*, DAVIS WRIGHT TREMAINE LLP, https://www.privsecblog.com/2019/02/articles/california-consumer-protection-act-ccpa/leveraging-your-gdpr-compliance-investment-for-ccpa/ [perma.cc/SL3D-DB8F].

The range of business entities facing CCPA compliance are similarly expansive. The CCPA defines a "covered entity" as any business "that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California."[192] The CCPA also applies to any entity "that controls or is controlled by a [covered] business . . . and that shares common branding with [that] business."[193] In an attempt to limit third-party data trading, i.e. the data broker industry or simply trading consumer information between corporations or subsidiaries, the CCPA specifies that "collects" is defined as "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means," which "includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior."[194]

Some commentators predict the CCPA will demand compliance from "more than 500,000 U.S. companies . . . in virtually every sector."[195] Depending on an entity's activities, "a website might only need 137 unique visitors from California per day" to be subject to CCPA enforcement.[196] Many large out-of-state businesses will be subject to compliance for simply having a website,[197] causing many internet-accessible businesses to unintentionally subject themselves to enforcement actions in California. Though its current iteration is subject to change,[198] the CCPA grants the California Attorney General's of-

192. CAL. CIV. CODE § 1798.140(c)(1) (2018).

193. § 1798.140(c)(2) ("Control or controlled" means "ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. 'Common branding' means a shared name, servicemark, or trademark.").

194. § 1798.140(e).

195. Hahn & Savare, *supra* note 185.

196. Timothy Tobin et al., *California Consumer Privacy Act: The Challenge Ahead – The Impact of the CCPA on Data-Driven Marketing and Business Models*, HOGAN LOVELLS CHRONICLE OF DATA PROTECTION (Nov. 30, 2018), https://www.hldataprotection.com/2018/11/articles/consumer-privacy/california-consumer-privacy-act-the-challenge-ahead-the-impact-of-the-ccpa-on-data-driven-marketing-and-business-models/ [perma.cc/WL95-G4B5].

197. Out-of-state businesses who "do business in the State of California" and either have (a) annual gross revenues in excess of twenty-five million dollars, (b) the personal information of 50,000 or more California citizens, or (c) derives 50% or more of its annual revenues from selling consumers' personal information. *See* CAL. CIV. CODE § 1798.140(c)(1)(A)–(C) https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180AB375 [perma.cc/WAJ5-VT9L].

198. This is subject to change by recently proposed amendments. *See* S.B. 561 Leg., 2019–20 Reg. Sess. (Cal. 2019).

fice the exclusive enforcement of those rights by imposing $100 to $1000 penalties for each individual violation.[199] Most importantly, the CCPA's final version will likely allow a private right of action for qualified offenses.[200]

Official clarification of the CCPA remains forthcoming.[201] To date, California regulators have refused to answer public concerns over the CCPA's uncertainty with any specificity.[202] The California Attorney General's Office has made some optimistic assurances that the CCPA's details will be fleshed out when it publishes its proposed regulations "in Fall of 2019."[203] Those proposals were published on October 10, 2019, yet "it remains unclear how California's Attorney General will interpret and enforce key CCPA provisions."[204] That uncertainly has further complicated the task of CCPA compliance, which already demanded "significant preparation in advance of the effective date of January 1, 2020."[205] For comparison, businesses facing compliance with the GDPR were given two years to prepare for its requirements,[206] and even then,

199. *Id.*

200. *Id.*

201. *See* Alysa Z. Hutnik & Lauren Myers, *California Privacy Update: What We Heard at Friday's CCPA Hearing*, AD L. ACCESS (Jan. 28, 2019) https://www.adlawaccess.com/2019/01/articles/california-privacy-update-what-we-heard-at-fridays-ccpa-hearing/ [perma.cc/JX6F-4RSC] ("For businesses hoping for CCPA clarity and guidance soon, that seems unlikely. California Deputy Attorney General Lisa Kim initiated the hearing, emphasizing that the Attorney General's Office was in the beginning of its rulemaking process and noting that she anticipated the formal review process not to start until Fall 2019.").

202. *See California Consumer Privacy Act (CCPA): Current Rulemaking Activity*, OFF. OF THE CAL. ATT'Y GEN. (2019), https://oag.ca.gov/privacy/ccpa [perma.cc/6ZA5-GNZB].

203. *See California Consumer Privacy Act (CCPA): Today's Forum*, OFF. OF THE CAL. ATT'Y GEN. (2019), https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-forum-ppt.pdf? [perma.cc/55LU-NU3U]; Lauren Valenzuela & June Coleman, *California's Fifth Consumer Privacy Act Forum in Review*, INSIDEARM (Feb. 12, 2019), https://www.insidearm.com/news/00044735-californias-fifth-consumer-privacy-act-pu/ [perma.cc/B7QF-5B59].

204. Ashley S. Shively, Mark S. Melodia, Marissa C. Serafino, *California Attorney General Releases Draft Regulations on the California Consumer Privacy Act*, HOLLAND & KNIGHT (Oct. 31, 2019), https://www.hklaw.com/en/insights/publications/2019/10/california-attorney-general-releases-draft-regulations [perma.cc/GYZ4-UFUV]

205. Theodore P. Augustinos and Laura L. Ferguson, *CCPA Guide: Are You Covered by the CCPA?*, LOCKELORD (Jan. 14, 2019), https://www.lockelord.com/-/media/privacy_20190111_ccpa-guide-are-you-covered_augustinos.pdf?la=en&hash=F8B868DFD0C23188F41CF44138625F1E [perma.cc/GBQ5-VKYA].

206. Matt Burgess, *What is GDPR?: The Summary Guide to GDPR Compliance in the UK*, WIRED (Jan. 21, 2019), https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018 [perma.cc/VPX3-SYC9].

many businesses remained unprepared just weeks before it became effective.[207] Businesses facing CCPA compliance have an easier task and will benefit from the growing compliance-related service market,[208] but the effectiveness of compliance consultants will be limited by the lack of certainty and formal guidance.[209]

The latest proposed amendments to the CCPA are likely to add to the mounting skepticism surrounding the bill.[210] The pending California Senate Bill 561 ("SB 561") amendment would remove the California Attorney General's mandatory duty to respond to entities' compliance guidance requests, expand the CCPA's private cause of action, and remove the thirty-day immunity window entities have to cure alleged violations before facing enforcement.[211] SB 561 intends to alleviate the "unworkable obligations" placed on California's Attorney General[212] but risks aggravating the growing criticisms and uncertainties surrounding its effective date.[213] Critics state the CCPA is "internally inconsistent and full of ambiguities,[214] and rather than alleviating

207. Tiffany Robertson, *Study Finds Organizations are not Ready for GDPR Compliance Issues*, THOMPSON REUTERS INSIGHTS (Aug. 15, 2017), https://blogs.thomsonreuters.com/financial-risk/riskmanagement-compliance/study-finds-organizations-not-ready-gdpr-compliance-issues/ [perma.cc/N8M2-3WEG].

208. Mark Adams & David Kruger, *Global Data Compliance in 2019*, BPA SOLUTIONS (Jan. 24, 2019), https://www.bpa-solutions.net/blog/2019-data-compliance/ [perma.cc/XK2S-ME5R].

209. Letter from Eric Goldman, Professor, Santa Clara University School of Law, et al., to California State Legislature, *Dear Senators and Assembly Members* (Jan. 17, 2019) https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2886&context=historical [perma.cc/USX2-8LL5] (expressing concerns about the CCPA and the "urgent need for major changes.").

210. *See* Don Jergler, *California Bills Would Add More Punch to Consumer Data Protection Law*, INS. J. (mar. 6, 2019), https://www.insurancejournal.com/news/west/2019/03/06/519826.htm [perma.cc/F8UZ-NRZP].

211. *See* S.B. 561, 2019–20 Reg. Sess. (Cal. 2019).

212. Letter from Xavier Becerra, Attorney Gen. of Cal., to State Assembly Member Ed Chau and State Senator Robert M. Hertzberg (Aug. 22, 2018), https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2801&context=historical [perma.cc/68MD-22KP]; Cheryl Miller, *Becerra Rips Lawmakers for 'Unworkable' Provision in New Data Privacy Law*, THE RECORDER (Aug. 29, 2018), https://www.law.com/therecorder/2018/08/29/becerra-rips-lawmakers-for-unworkable-provisions-in-new-data-privacy-law/ [perma.cc/B7LJ-FY7D].

213. *See* Joseph J. Lazzarotti et al., *California AG Announces Amendment to the CCPA*, THE NAT'L L. (Feb. 26, 2019), https://www.natlawreview.com/article/california-ag-announces-amendment-to-ccpa [perma.cc/Y2U2-HK4H].

214. *See* Alan L. Friel & Taylor A. Bloom, *CCPA Expansion Proposed*, BAKERHOSTETLER DATA PRIVACY MONITOR (Feb. 27, 2019), https://www.dataprivacymonitor.com/ccpa/ccpa-expansion-proposed/ [perma.cc/4JUZ-J3GF] ("This is alarming as there are detailed obligations for achieving compliance under CCPA, and the act is internally inconsistent and full of ambiguities. Under SB 561, a well-meaning business that accidentally makes a mistake because it couldn't seek clarification from

those fears, SB 561 embodies the ad-hoc nature of the CCPA's grass-roots origins.[215]

The consequences of the CCPA's unprecedented scope, formidable enforcement via a private right of action, and uncertain compliance requirements make preemption by federal lawmakers a tempting alternative. At a glance, a new federal framework that balances privacy concerns with feasible industry practices may be a preferable compromise between the CCPA and the FTC's current federal regulation under Section 5, but as previously discussed, states play an important if not essential role in the area of informational privacy regulation. Addressing digital-era privacy in the United States is more nuanced than first impressions.

VI. STATE LABORATORY OR QUASI-FEDERAL ACTOR: ANALYZING THE FEDERALIST IMPLICATIONS OF CALIFORNIA'S CONSUMER PRIVACY ACT OF 2018

Digital industry representatives and advocacy groups strongly oppose the CCPA and continue to fight for its alteration.[216] Those interests have taken to Washington D.C., touting the need for greater consumer privacy protections while seeking to influence legislation at the federal level.[217] While those efforts are unsurprising,[218] they raise concerns given the costs of preempting states from regulating privacy in the digital sphere.[219]

---

the AG will no longer have a 30-day opportunity to resolve the issue before enforcement ensues. Further, unlike the AG that exercises prosecutorial discretion to direct limited resources toward bad actors, allowing private attorney general actions will subject businesses to 'gotcha' claims for even innocent technical violations. As a result, minor issues best handled by 'fix it' tickets could be met with expensive and socially inefficient class action lawsuits.").

215. *See* Confessore, supra note 171.

216. *See e.g.*, Issie Lapowsky, *The Fight Over California's Privacy Bill Has Only Just Begun*, WIRED (Aug. 29, 2018), https://www.wired.com/story/california-privacy-bill-tech-lobbying/ [perma.cc/L6XA-LFQQ].

217. Barry Friedman, *Valuing Federalism*, 82 MINN. L. REV. 317, 373–74 (1997); Robert A. Mikos, *Making Preemption Less Palatable: State Poison Pill Legislation*, 85 GEO. WASH. L. REV. 1, 14 (2017) ("Furthermore, the states commonly must compete with relatively powerful lobbying groups that *favor* preemption, including business and trade associations.").

218. Schwartz, *supra* note 7, at 941 ("At any rate, state legislative activities will continue and will drive a flight by businesses to Washington for federal solutions. Over the next decade and beyond, continuing waves of state privacy lawmaking will provoke industry activity to seek federal legislation.").

219. See *infra* Section IV.C.

The CCPA becomes effective in 2020,[220] and its impending effective date presents an ultimatum for Congress.[221] Federal legislators can either: (1) enact an express legislative mandate for the federal regulation of the digital industry's collection and use of personal information, potentially preempting future state attempts to regulate in the area, or (2) allow the CCPA to move forward and ignore the national consequences of California's actions. The present discussion has focused on the benefits of state-level activity in privacy regulations, so the remaining discussion is limited to the costs of federal "ceiling" preemption in the area, i.e., federal legislation would limit the ability of state regulators to experiment, pioneer, or police compliance with new or old approaches.[222] Recent congressional proposals have contained such a limitation, and previous federal regulations in the digital sphere have imposed ceilings on state enforcement capabilities.[223] The CCPA's enforcement via a private cause of action make this type of limitation more likely in any future federal action,[224] either by express congressional mandate[225] or subsequent agency decisions under the mandate.[226]

220. *See* CAL. CIV. CODE § 1798.198(a) (effective January 1, 2020).

221. *See* Heather K. Gerken, *Dissenting by Deciding*, 57 STAN. L. REV. 1745, 1746 (2005); Heather K. Gerken & Ari Holtzblatt, *The Political Safeguards of Horizontal Federalism*, 113 MICH. L. REV. 57, 82–83 (2014) ("States are sites where . . . dissenters can model policymaking alternatives to the dominant national view."); Friedman, *supra* note 214, at 403 (noting state legislative initiatives can "serve as an independent means of calling forth the voice of the people").

222. William W. Buzbee, *Asymmetrical Regulation: Risk, Preemption, and the Floor/Ceiling Distinction*, 82 N.Y.U. L. REV. 1547, 1548 (2007).

223. *See* Cain, *supra* note 160, at 770 ("Congress should reinstate all the private rights of action under state laws that were preempted by CAN-SPAM. Individual recipients could then pursue statutory damages from any sender of spam who ignores opt-out messages, not just senders whose messages violate the deception prohibitions. Alternatively, Congress should create a meaningful private cause of action for recipients in a revised CAN-SPAM Act.").

224. Schwartz, *supra* note 7, at 944 ("The problem with a monopoly on enforcement given to federal agencies is that it would assign these organizations too large a role in the regulatory dialogue.").

225. *See* Cain, *supra* note 160, at 757–58 (describing how the federal CAN-SPAM Act directly preempted state laws providing enforcement via individual causes of action).

226. Mikos, *supra* note 217, at 16 (describing the common power of federal agencies to "preempt state law anytime it conflicts with a congressional statute or an agency regulation, regardless of the damage done to state interests").

A. The National Costs of the CCPA

The CCPA definitively rejects Congress' practice of using "narrowly targeted laws and regulations that prevent the privacy abuse of new technologies."[227] California's law applies a new approach: trading durability for flexibility while emphasizing that privacy concerns are important, complex, abstract, subjective, and subject to change over time; that the fast-paced nature of the digital industry results in a continuous emergence of new privacy threats; and that static regulations are often outpaced by industry developments.[228] "It is difficult, after all, if not impossible, to predict the pace of technology innovation and how it will affect society."[229] California's legislature has eliminated the need to predict the future with the broad and generalized provisions of the CCPA.[230] Those same provisions impose costs for entities subject to CCPA compliance, and national entities will pass those costs on to consumers.[231]

Calling the CCPA a "state-level" regulation is a form of fiction: the California statute will impose national costs.[232] The CCPA purports to regulate entities conducting *any* level of activity within California, so long the business meets the minimum annual revenue requirements and its activities in the state generate some revenue.[233] It also claims to "regulate businesses with no nexus

---

227. Daniel Castro & Alan Mcquinn, *The Privacy Panic Cycle: A Guide to Public Fears About New Technologies*, INFO. TECH. AND INNOVATION FOUND. (Sept. 2015), http://www2.itif.org/2015-privacy-panic.pdf [perma.cc/88L3-BZDW].

228. *See, e.g.*, Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2012).

229. Castro & Mcquinn, *supra* note 227.

230. *Id.*

231. Letter from Eric Goldman to California Legislature, *California Consumer Privacy Act*, (Jan. 17, 2019) https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2886&context=historical [perma.cc/USX2-8LL5] ("[The CCPA] causes tremendous uncertainty and possibly wasted expenditures for businesses without real ties to California.").

232. *See, e.g.*, Bellia, *supra* note 7, at 895 (discussing California's heightened child data protection in 2004).

> Any website seeking to serve a national market will meet the general requirements of the California standard. The standard becomes a national, though not a federally adopted, standard, and it may create externalities even if no other state adopts a conflicting rule. The effect of California's regulation – if not the very goal – is to raise the website's costs. Customers nationwide bear these costs, regardless of whether non-California residents value privacy at the same level as California residents do.

Id. It should be noted, however, that most forms of state regulation have consequences outside of state boarders to some extent. *See* Gerken & Holtzblatt, *supra* note 218, at 80.

233. Goldman, *supra* note 231 (expressing concerns about the CCPA and the "urgent need for major changes.")

with California other than being affiliates."[234] The CCPA undoubtedly causes "uncertainty and possibly wasted expenditures for businesses without real ties to California."[235]

State regulations are not *per se* unjustified simply because they impose extra-territorial costs. The magnitude of the regulation's costs and benefits must be considered along with the location where those consequences are felt. The costs imposed by a state-level privacy regulation will increase with the volume of activity regulated. That is to say, the most burdensome scenario occurs when large states impose broad regulations. The inverse holds that sectorial state-level privacy regulations that are less burdensome for the national industry may be justifiable despite extra-territorial costs. Illinois' regulation of biometric information illustrates a state-level privacy regulation that is permissible despite such national costs. The market for biometric technology, while growing, occupies only a small portion of the digital-technology industry.[236] Following its emergence less than a decade ago, biometric technologies elicited strong reactions from the public due to their potential surveillance applications.[237] Within that context, Illinois enacted the Biometric Information

---

> For example, the $25M threshold equally applies to businesses that receive all revenues from California residents and businesses that receive only $1 of revenue from California residents. If so, a business without any ties to California must comply with the CCPA (at substantial expense) the moment it accepts a single dollar from a California resident.

Id.; *see also* Stephen J. Astringer, *The Endless Bummer: California's Latest Attempt to Protect Children Online Is Far Out(Side) Effective*, 29 NOTRE DAME J.L. ETHICS & PUB. POL'Y 271, 288 (2015) (discussing California's previous child privacy legislation).

234. Goldman, *supra* note 231.

235. *Id.*

236. One source predicts the entire U.S. biometric technology market will reach 14.7 dollars in 2024, up from 2.3 billion in 2013. Arne Holst, *Size of the Biometrick Market in the United States from 2013 to 2024 (in Billion U.S. Dollars)*, STATISTA (Feb. 21, 2018) https://www.statista.com/statistics/761249/biometrics-market-size-in-us/ [perma.cc/5SXK-V7AB]. In contrast, the total value of U.S. big data industry was 19.6 billion dollars in 2013. Shanhong Liu, *Forecast of Big Data Market Size, Based on Revenue, from 2011 to 2027 (in Billion U.S. Dollars)*, STATISTA (Aug. 9, 2019) https://www.statista.com/statistics/254266/global-big-data-market-forecast/ [perma.cc/FL44-V2LF].

237. Rachel L. German & K. Suzanne Barber, *Current Biometric Adoption and Trends*, UNIV. OF TEX. AT AUSTIN CTR. FOR IDENTITY (Sept. 2017) https://identity.utexas.edu/assets/uploads/publications/Current-Biometric-Adoption-and-Trends.pdf [perma.cc/6J67-72JL]. Even with the downturn in general public concern, privacy fundamentalists from advocacy groups like the Electronic Privacy Information Center continue to warn against the "profound threats to privacy and financial security" posed by biometric data use and non-regulation. Claire Gartland, *Biometrics Are a*

Protection Act in 2008 ("BIPA"),[238] which heightened the state's regulation of biometric information by granting Illinois citizens privacy protections.[239] Few states have followed since then, and none of those provide a private right-of-action like Illinois' BIPA.[240]

The localized-consequences of BIPA illustrate why state-level privacy regulations are workable when limited in scope. BIPA is the strictest state-level regulation of biometric data, but rather than establish a new national standard, companies can chose to: (1) ensure compliance by foregoing use of potentially beneficial biometric technologies; (2) attempt compliance while using such technologies by altering their practice and risking potential liability; or (3) evade the forum entirely.[241] Like the CCPA, national companies that continue to subject themselves to BIPA liability "pass along the costs to consumers."[242] However, the magnitude of the activity regulated by BIPA is minimal due to its sectorial nature and limited territorial scope, and much of its costs are suffered within the state[243] by restricting its citizens' access to such

---

Grave Threat to Privacy, N.Y. TIMES (July 5, 2016) https://www.nytimes.com/roomfordebate/2016/07/05/biometrics-and-banking/biometrics-are-a-grave-threat-to-privacy [perma.cc/A5Y7-W5HK].

238. *Biometric Privacy Litigation: The Next Class Action Battleground*, WINSTON & STRAWN LLP (Jan. 12, 2018), https://www.winston.com/en/thought-leadership/biometric-privacy-litigation-the-next-class-action-battleground-1.html [perma.cc/9DL4-FQZW].

239. *See* Biometric Info. Privacy Act, 740 Ill. Comp. Stat. 15(b)(1) (2008).

240. Illinois and Texas have active legislation heightening regulations for biometric data. Biometric Information Protection Act (BIPA), 740 ILL. COMP. STAT. ANN. 14/1-99 (2018); Capture or Use of Biometric Identifier Act (CUBI), TEX. BUS. & COM. CODE ANN. § 503.001 (2017). Four other states have pending biometric data legislation. H.B. 72, 30th Leg., Reg. Sess. (Alaska 2017); H.B. 5522, 2017 Gen Assemb., Reg. Sess. (Conn. 2017); H.B. 523, 2017 Reg. Sess. (N.H. 2017); H.B. 1493, 65th Leg., Reg. Sess. (Wash. 2017).

241. *See, e.g.*, Jack Nicas, *Why Google's New App Won't Match Your Face to Art in Some States*, WALL ST. J. (Jan. 18, 2018), https://www.wsj.com/articles/why-google-wont-search-for-art-look-alike-in-some-states-1516194001 [https://perma.cc/4J7Q-QBTN]; Erin Marine, *Biometric Privacy Laws: Illinois and the Fight Against Intrusive Tech*, FORDHAM J. CORP. & FIN. L. (Mar. 20, 2018), https://news.law.fordham.edu/jcfl/2018/03/20/biometric-privacy-laws-illinois-and-the-fight-against-intrusive-tech/ [perma.cc/Z5U7-ZMKT]; Glosson, *supra* note 7, at 431 ("Several commentators suggest that modern geolocation capabilities lower the burden that state laws place on interstate commerce by enabling them to block citizens of states in which they do not wish to do business . . . .").

242. Todd Maisch, *Guest View: Don't Strangle Tech Industry in Illinois* (Oct. 22, 2017) https://qctimes.com/opinion/columnists/guest-view-don-t-strangle-tech-industry-in-illinois/article_1145bf96-5d7a-5cea-b0d5-405d35ecd724.html [perma.cc/ZC4D-AP5U].

243. Amy Korte, *The Flood of Biometric Privacy Litigation Engulfing Tech Companies and Employers Should Make the General Assembly Think Twice Before Passing New Regulations that Could Increase Costs and Compliance Burdens for Companies*,

technologies,[244] "making [it] a less attractive place for business investment and hurting [its] ongoing ability to attract and keep a tech workforce."[245] BIPA does impose extraterritorial costs: states other than Illinois would benefit from a completely unregulated biometric technology market.[246] However, the costs BIPA imposes on national innovation in the area are negligible, as ample alternative state forums are available for regulated entities to development regulated products and market such goods and services. State privacy regulations that are limited in scope like BIPA are largely justified because the costs and benefits of these experiments "hit home."[247]

None of the characteristics limiting the national consequences of BIPA are shared by the CCPA. While BIPA narrowly targets biometric information,[248] the CCPA broadly applies to most types of personal information.[249] In addition, though Illinois has a large economy, the comparative economic might of California makes avoiding the regulated activity extremely costly for national entities with internet platforms.[250] National companies that use fingerprint security scanners may forgo using them in their Illinois offices, but the same company with a website and $25,000,000 of annual revenue would be hit hard by avoiding all business operations within California. "At bottom, data privacy laws affect far more commerce than any obscenity statute or car dealership regulation ever has because privacy laws impact businesses of all shapes and sizes."[251] The cumulative and indirect effects of those costs are passed on to consumers throughout the nation, and they are not negligible.[252] Modern

---

ILL. POL'Y (Oct. 27, 2017) https://www.illinoispolicy.org/while-illinois-courts-amazon-privacy-litigation-threatens-tech-firms-illinois-employers/ [perma.cc/8SJL-B4LN].

244. Nicas, *supra* note 241.

245. Maisch, *supra* note 242.

246. *See ABI Research Predicts Fingerprint Sensors, Facial Recognition, and Biometric Surveillance to Propel the Global Biometrics Industry to $30 Billion by 2021*, ABI RES. (Mar. 17, 2016), *https://www.abiresearch.com/press/abi-research-predicts-fingerprint-sensors-facial-r/* [perma.cc/W3SF-H4Y9] ("[T]he global biometrics market will reach more than $30 billion by 2021, marking an impressive 118% increase from 2015.").

247. Greve, *supra* note 99.

248. Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/10 (2018).

249. Goldman, *supra* note 231 ("Most US privacy laws are 'sectoral-based,' i.e., they are optimized for the needs of specific industries. In contrast, the CCPA applies across all industries, with only limited exceptions. Because of the CCPA's rushed approval process, the California legislature did not hear from thousands of different industries affected by the CCPA.").

250. Hogan Lovells, *California Continues to Shape Privacy and Data Security Standards, International Association of Privacy Professionals Privacy Tracker*, IAPP (Oct. 1, 2013), https://iapp.org/news/a/california-continues-to-shape-privacy-and-data-security-standards/ [perma.cc/ZJ9H-TWEM].

251. Glosson, *supra* note 7, at 433.

252. *Id.* at 431, 433.

interstate commerce is tied to digital technologies. The digital industry has proven its ability to yield paradigm-shifting benefits through innovation and entrepreneurship, and nearly all non-digital entities retain some form of digital platform in its operations.

Federal preemption may be justified "to displace a law that has national consequences but that has not been subject to the national political process."[253] The national costs of the CCPA pose serious concerns and presently favor such intervention. Further, the case for judicial invalidation of the CCPA under the Dormant Commerce Clause, a higher and more concrete burden than the present policy conjecture, is plausible given the CCPA's extraterritorial effects.[254] By purporting to regulate activity wholly outside of California's borders, the CCPA "raises substantial Constitutional concerns."[255] Constitutionality aside, the recent actions of other states may lessen concerns raised by the CCPA's national costs.

B. States are Following the CCPA's Lead

Numerous states have begun following California's lead, alleviating some of the concerns that the CCPA will overburden non-Californians. As we have seen in previous areas of digital industry regulation, like data breach notification statutes, widespread state adoption and occupation of a regulatory field can negate concerns regarding the national costs imposed by a state pioneering the area. This is true despite the risk that the strictest state approach may impose "de facto national requirements."[256] In such situations, however, significant inconsistencies between state requirements also support federal action to occupy and potentially preempt state regulations.[257]

Ten states have already proposed CCPA-like legislation that would broadly regulate the collection and use of personal information.[258] Missis-

253. Bellia, *supra* note 7, at 899.

254. *See* Glosson, *supra* note 7, at 409 (approaching the issue with constitutional analysis under the Dormant Commerce Clause).

255. *See* Eric Goldman, *41 California Privacy Experts Urge Major Changes to the California Consumer Privacy Act*, TECH. & MARKETING LAW BLOG (Sept. 21, 2019), https://blog.ericgoldman.org/archives/2019/01/41-california-privacy-experts-urge-major-changes-to-the-california-consumer-privacy-act.htm [perma.cc/K45A-5XS5].

256. Kosseff, *supra* note 119, at 181–82.

257. Bellia, *supra* note 7, at 894.

258. Rachel Marmor et al., *"Copycat CCPA" Bills Introduced in States Across Country*, DAVIS WRIGHT TREMAINE LLP (Sept, 21, 2019), https://www.privsecblog.com/2019/02/articles/california-consumer-protection-act-ccpa/copycat-ccpa-bills-introduced-in-states-across-country/ [perma.cc/95HD-6X72]; *see also* Rachel Marmor et al., *Short State Law Chart*, DAVIS WRIGHT TREMAINE LLP (Sept. 21, 2019) https://www.dwt.com/files/Uploads/Documents/Advisories/02.07.19_CCPA%20Short%20State%20Law%20Chart.pdf [perma.cc/95HD-6X72].

sippi's bill died in committee, and New Jersey's has not moved out of committee.[259] Successful enaction of the bills pending in Hawaii,[260] Maryland,[261] Massachusetts,[262] New Mexico,[263] Rhode Island,[264] New York,[265] North Dakota,[266] and Washington[267] would alleviate arguments supporting CCPA preemption due to national costs, especially considering five of the proposals support enforcement via a private cause of action. Criticism of the federal CAN-SPAM Act bolsters the case for allowing such state-level regulation to continue.[268] However, state occupation of the field poses the additional problem of inconsistencies arising between states. Such inconsistencies make state-by-state compliance a costly and inefficient task for entities operating in multiple states. The potential for inconsistencies is particularly apparent in Washington's recent proposal: the Washington Privacy Act ("WPA"), currently pending as SB 5376.[269] The WPA shares the informational privacy characteristics of the GDPR and the CCPA, however, it is more closely modeled after the GDPR. Among its differences with the CCPA, the WPA would require "opt-in" consent for data "processing" and empower Washington citizens with additional rights related to the correction, alteration, and disclosure of collected personal information.[270]

C. Analyzing the Potential Case for Preemption of the CCPA

There are many benefits and costs of federal preemption.[271] As a general rule, however, "Congress should preempt state law only when the benefit it derives from doing so exceeds the cost that preemption imposes upon the state."[272] Additionally, preemption may be ideal "to displace a law that has

259. Marmor et al., *supra* note 255.
260. *Id.* (discussing Hawaii SB 418).
261. *Id.* (discussing Maryland SB 0613).
262. *Id.* (discussing Massachusetts SD 341).
263. *Id.* (discussing New Mexico SB 176).
264. *Id.* (discussing Rhode Island S0234).
265. *Id.* (discussing New York S00224).
266. *Id.* (discussing North Dakota HB 1485).
267. *Id.* (discussing Washington SB 5376).
268. *See supra* section IV.A.
269. Nancy Libin & Rachel Marmor, *Washington Privacy Act, as Introduced in the Washington Legislature; A Rapid Q & A, State Across Country*, DAVIS WRIGHT TREMAINE LLP (Sept. 21, 2019) https://www.dwt.com/Washington-Privacy-Act-as-introduced-in-the-Washington-Legislature-A-Rapid-QA-02-06-2019/ [perma.cc/QF2L-PNQ2].
270. *Id.*
271. *See* Bellia, *supra* note 7.
272. Mikos, *supra* note 217, at 11; *see generally* Robert Cooter & Neil Siegal, *Collective Action Federalism: A General Theory of Article I, Section 8*, 63 STAN. L. REV. 115 (2010); Friedman, *supra* note 217, at 317; Edward L. Rubin & Malcolm Feeley,

national consequences but that has not been subject to the national political process."[273] Common justifications for exercising federal preemptive power to centralize state regulations include: correcting regulations that create a "race to the bottom"; correcting for an inefficiency caused by the extraterritorial externalities of a state's regulation; and capturing the benefits uniform regulations yield.[274] Concerning state privacy regulations, "[t]here certainly has been no race to the bottom."[275] However, the latter two concerns are relevant.

Centralizing regulation at the federal level can prevent externalities "whenever a state governmental policy, law, or activity imposes costs or confers benefits on residents of other states."[276] Negative externalities occur when the cost of one state's regulation spillover to another state that receives none of the benefits. The preceding Section detailed the CCPA's great national costs, and these spillover burdens arguably provide the largest justification for federal preemptive action. However, in the context of state-level internet regulations, extraterritorial costs may simply account for heterogeneity in values and burdens of different states.[277] Specifically, state regulations can facilitate efficiency by imposing extraterritorial costs to address disproportionate harms suffered within their specific forum.[278] Known as the "matching principle," that justification appears in state air-pollution regulations to support the efficiency of state regulations despite their disproportionate spillover effects.[279] In other words, it may be economically beneficial for states to impose spillover costs that compensate for the disproportionate harms a national practice imposes within their forum. Such economic considerations are difficult here given the inherent subjectivity of privacy. One could argue that Californian's do suffer disproportionately from the privacy harms caused by widespread industry practices. California is the only state which constitutionally provides for an inal-

---

Federalism: Some Notes on a National Neurosis, 41 UCLA L. REV. 903 (1994); Catherine M. Sharkey, *Inside Agency Preemption*, 110 MICH. L. REV. 521 (2012); David C. Vladeck, Preemption and Regulatory Failure, 33 PEPP. L. REV. 95 (2005).

273. Bellia, *supra* note 7, at 895, 899 ("Customers nationwide bear these costs, regardless of whether non-California residents value privacy at the same level as California residents do.").

274. *See* Friedman, *supra* note 217, at 406–09.

275. Schwartz, *supra* note 7, at 940–41 ("In other words, California privacy initiatives have not encouraged Nevada or other states, neighboring or otherwise, to enact weaker regulations in the same area.").

276. Steven G. Calabresi, *"A Government of Limited and Enumerated Powers": In Defense of United States v. Lopez*, 94 MICH. L. REV. 752, 782 (1995).

277. Goldsmith & Sykes, *supra* note 100, at 796; Greve, *supra* note 99, at 1 ("State-based policy innovation also facilitates adaptation to local needs, circumstances, and preferences.").

278. Goldsmith & Sykes, *supra* note 100, at 796.

279. *See, e.g.*, Daniel C. Esty, *Revitalizing Environmental Federalism*, 95 MICH. L. REV. 570, 587 (1996); *see also* Bellia, *supra* note 7, at 893.

ienable right of privacy against both state and private actors, so the greater proportionate value California places on privacy is apparent.[280] Moreover, even without considering the state's heightened privacy values, California suffers greater harm from privacy abuses because "[o]ne out of eight Americans live in California."[281] Accordingly, one could plausibly argue that California suffers disproportionately from the nation's under-regulation of the collection and use of personal information, and the CCPA may therefore be justified as a function of the matching principle. The same considerations support more abstract arguments for state-level privacy regulations. Such a system would enable states to enact privacy laws catered to their constituents' unique values, facilitating democratic self-governance.[282] Federal preemptive action would restrict the ability of states to govern autonomously in accordance with those values.[283]

The second argument for federal preemption is the need for uniformity. Assuming states follow the CCPA, inconsistencies between state regulatory requirements could raise compliance costs in favor of federal regulation,[284] especially when such inconsistencies impose "high costs and little policy payoff."[285] In such circumstances, "centralization and uniformity . . . can reduce social cost."[286] In the context of digital industry, the "burden of potentially inconsistent regulations from other states is a very real concern."[287] The existence of variations does not render state regulatory landscapes inefficient *per se*.[288] As mentioned above, the matching principle's considerations are applicable here. Whether or not such inconsistencies warrant federal occupation has yet to be seen. As the preceding Section discusses, states have begun moving into the area, but the potential for future variations between states cannot presently warrant preemption.

The potential benefits of federal preemption must be weighed against the considerable costs. The flexible experimentation of states, in addition to their

280. CAL. CONST. art. I, § 1; Sheehan v. S.F. 49ers, 201 P.3d 472, 479 (Cal. 2009) (holding the right to privacy applies to state actors and private parties).

281. Lovells, *supra* note 250.

282. Friedman, *supra* note 217, at 389 ("States, and their substate local governments, are closer to the people and provide an opportunity for greater citizen involvement in the functional process of self-government."); *see* Deborah Jones Merritt, *The Guarantee Clause and State Autonomy: Federalism for a Third Century*, 88 COLUM. L. REV. 1, 3–10 (1988) (arguing that state governments provide political and cultural diversity).

283. Friedman, *supra* note 217, at 403 ("Whatever the shifts in regulatory authority from the states to the national government, the fact is that the states remain independent political fora, with popular assemblies capable of expressing popular sentiment. The states have performed this function throughout history.").

284. Bellia, *supra* note 7, at 894.

285. Schwartz, *supra* note 7, at 942.

286. Calabresi, *supra* note 282, at 780.

287. Glosson, *supra* note 7, at 431.

288. Goldsmith & Sykes, *supra* note 101, at 796 ("The mere fact that measures undertaken by one jurisdiction have effects on citizens elsewhere, however, is by itself no objection to them."); *but see* Kosseff, *supra* note 119, at 162–66.

capacity for rapid regulation, has been paramount for national regulation in the area of digital privacy. Those costs are exacerbated by the risk of a preemptive federal mandate ossifying in the fast-paced digital industry. Sunsetting provisions can ameliorate those concerns, but the historical lack of federal involvement in digital privacy fields is apparent.

VII. CONCLUSION

The CCPA marks the beginning of states broadly regulating the digital industry's collection and use of personal information. Pioneering state regulation of the digital industry is nothing new, and state government's regulatory activity in the area has numerous benefits for healthy regulation at the national level. Future efforts to centralize such regulation under a federal mandate should not restrict the flexibility state regulators provide without adequate justification. The benefits of any preemptive measure should be carefully compared to the costs of in-state capabilities and autonomy. As of now, congressional action to occupy the area may be premature. The next decade will show if the CCPA is gangbusters or just busted.