HAMILTONIAN CYBERSECURITY

Jeff Kosseff[*]

Cyberattacks present existential challenges for U.S. national security and economic interests, yet Congress has failed to adopt a comprehensive regulatory framework to secure private-sector information and systems. To fill that gap, state legislatures have passed many laws that regulate data security, data breaches, and protection of personal data. The requirements of these laws vary significantly, are outdated, and sometimes conflict. This Article explains why this state-centric approach to cybersecurity is inadequate. First, the Article examines the Framers' desire for a uniform approach to commercial regulations and explains how the U.S. approach is scattered, outdated, and decentralized. A comprehensive federal cybersecurity statute would help to realize the Framers' vision. Second, the Article asserts that, given this prudential argument, the state approach to cybersecurity and data protection regulations may be unconstitutional under the Dormant Commerce Clause, which prohibits state laws that unduly burden interstate commerce or impose inconsistent regulations.

TABLE OF CONTENTS

* Assistant Professor of Cybersecurity Law, United States Naval Academy, Cyber Science Department. J.D., Georgetown University Law Center; M.P.P., B.A., University of Michigan. The views expressed in this Article are only the author's and do not reflect the views of the Naval Academy, Department of Navy, or Department of Defense. Many thanks to Jonathan Hilliard and the staff of *Wake Forest Law Review* for the indispensable feedback and careful editing.

I. INTRODUCTION

Cybersecurity vulnerabilities threaten the U.S. economy,[1] national security,[2] individual privacy and safety,[3] and even the fundamental underpinnings of our democracy.[4] Many of the most damaging incidents have targeted systems and information controlled by private companies.[5] Yet Congress has largely failed to enact national cybersecurity or data protection legislation.[6] Although

1. *See* Michelle Drolet, *What Does Stolen Data Cost [Per Second]*, CSO (Jan. 26, 2018, 10:34 AM), https://www.csoonline.com/article/3251606/data-breach/what-does-stolen-data-cost-per-second.html ("The 2017 Cost of Data Breach Study from the Ponemon Institute, sponsored by IBM, puts the global average cost at $3.6 million, or $141 per data record. That's a reduction on the average cost in 2016, but the average size of data breaches has increased. It's also worth noting that the average cost of a data breach in the United States is much higher at $7.3 million.").

2. *See* Ellen Nakashima, *White House Says Sony Hack is a Serious National Security Matter*, WASH. POST (Dec. 18, 2014), https://www.washingtonpost.com/world/national-security/white-house-says-sony-hack-is-a-serious-national-security-matter/2014/12/18/01eb8324-86ea-11e4-b9b7-b8632ae73d25_story.html.

3. *See* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 744–45 (2018) ("The number of people affected by data breaches continues to rise as companies collect more and more personal data in inadequately secured data reservoirs. Risk and anxiety are injuries in the here and now. Victims of data breaches have an increased risk of identity theft, fraud, and reputational damage. Once victims learn about breaches, they may be chilled from engaging in activities that depend on good credit, like house- and job-hunting.").

4. *See* Ellen Nakashima & Shane Harris, *How the Russians Hacked the DNC and Passed its Emails to Wikileaks*, WASH. POST (July 13, 2018), https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html ("While Russian hacking, especially for espionage purposes, is decades old, using digital tools to steal data and then release it to embarrass and stoke divisions—weaponizing information—was the innovation, one that U.S. spy agencies did not see coming until too late.").

5. *See* Sean Doherty, *Why Cyber Defense Ultimately Rests with the Private Sector*, FCW (Mar. 31, 2015), https://fcw.com/Articles/2015/03/31/Private-sector-cyber.aspx ("The private sector has been the hardest hit by cyberattacks and data breaches in recent years and is now seeking help from the federal government.").

6. *See* Brett V. Newman, Note, *Hacking the Current System: Congress' Attempt to Pass Data Security and Breach Notification Legislation*, 2015 J. L. TECH. & POL'Y 437, 438 (2015) ("Despite the wave of massive breaches and

some federal laws regulate sectors that handle particularly sensitive information, such as healthcare[7] and financial institutions,[8] the United States has no comprehensive statutory scheme to regulate the confidentiality, integrity, and availability of information, systems, and networks.[9]

The federal government's inaction has prompted states to fill the gaps. Since 2003, every state has passed at least one law that establishes rules for notifying victims of data breaches or securing private networks.[10] Some states have passed many laws that require companies to adopt specific cybersecurity safeguards.[11] These laws vary in scope and substantive requirements, and some even conflict with one another. The state laws typically apply based on the location of the data subject and not the company, meaning that a company with customers or employees nationwide must comply with the laws of all fifty states.[12]

This uncoordinated regulatory approach is ill-suited to any field and particularly to one as vital as cybersecurity. Cybersecurity regulation is determined by more than seven thousand state legislators,[13] and it is enforced by fifty governors and fifty state attorneys general and their staffs. This bouillabaisse of state cybersecurity laws makes it impossible for the United States to develop a cohesive strategy to secure itself from increasingly persistent and advanced cyber threats. Although new cybersecurity threats emerge daily, many state cybersecurity laws are more than a decade old and have not changed. These laws therefore address the

legislative action on the part of many states, there is no comprehensive federal law for data security and breach notification.").

7. 45 C.F.R. §§ 160.102, 164.104 (2018).

8. 15 U.S.C. § 6801 (2012).

9. *See Glossary*, NAT'L INITIATIVE FOR CYBERSECURITY CAREERS & STUD., https://niccs.us-cert.gov/glossary (last updated Nov. 28, 2018) (defining "cybersecurity" as "[s]trategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure").

10. *See Data Security Laws: Private Sector*, NAT'L CONF. ST. LEGISLATURES (Jan. 4, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx; *Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

11. *See Data Security Laws: Private Sector*, *supra* note 10.

12. *Id.*

13. *See Number of Legislators and Length of Terms in Years*, NAT'L CONF. ST. LEGISLATURES (Mar. 11, 2013), www.ncsl.org/research/about-state-legislatures/number-of-legislators-and-length-of-terms.aspx (tallying 7,383 state legislators in the United States).

threats of the mid-aughts rather than the threats of today. It does not have to be like this.

For the United States to even begin to address modern cybersecurity threats, it must develop effective regulations, cooperation, and assistance that ultimately leads to increased security of both the public *and* private sectors. This Article advances prudential and constitutional cases to replace our state-centric cybersecurity laws with a cohesive national system. Cybersecurity is an inherently interstate field that is ill-suited for a state-by-state regulatory scheme. In 1782, Alexander Hamilton wrote of the need for a "common direction" in commercial regulation.[14] For cybersecurity, that remains true today.

Cybersecurity threats are increasingly complex, constantly changing, and potentially devastating to the U.S. economy and national security. This is precisely the sort of field that requires the common direction that Hamilton envisioned. Yet the regulation of cybersecurity and the related field of data protection are often left to disparate state regulations. While well-intentioned, the states have demonstrated that they simply do not have the resources or expertise to keep pace with the new challenges by passing laws that mitigate the risks and harms.

Part II examines the U.S. history and rationale for regulating interstate commerce at the federal level. It examines the criticisms that Hamilton and James Madison leveled on the Articles of Confederation-era state regulation of commerce and their rationale for national commercial regulation.

Part III explains how cybersecurity law contravenes the Hamiltonian vision of commercial regulation, with power largely concentrated in the states. It highlights the practical difficulties of this state-centric regulatory regime, as predicted by Hamilton and Madison, and presents a prudential argument for uniform national cybersecurity regulations. I refer to this framework as "Hamiltonian Cybersecurity" because Hamilton had forcefully pushed for a common direction for commercial regulation, though Madison, John Jay, and other Framers also advocated for centralized laws. Congress should heed the Framers' call and pass a centralized national cybersecurity law that preempts the current state regulatory patchwork.

Part IV sets forth a constitutional argument against state cybersecurity regulation in light of the practical difficulties of state-by-state cybersecurity and data protection regulations. For many of the same reasons that state cybersecurity laws are impractical and contrary to the expectations of the Framers, there is a strong argument that at least some of the state laws violate the Dormant Commerce Clause.

14. 1 ALEXANDER HAMILTON, *The Continentalist No. V*, *in* THE WORKS OF ALEXANDER HAMILTON 267, 271 (Henry Cabot Lodge ed., G.P. Putnam's Sons 1904).

This Article does not argue against aggressive and meaningful regulation of cybersecurity. To the contrary, a major failure of many state laws is that they do not sufficiently deter reckless cybersecurity practices. For cybersecurity laws to adequately regulate and deter bad practices, they must address current threats. State cybersecurity laws largely have not accomplished that. A uniform federal system of cybersecurity laws would not only be closer to the Framers' vision of commercial regulation, but it also would be more effective at achieving the end goals of bolstering the security of systems and information.

II. HAMILTONIAN VIEW OF COMMERCIAL REGULATION

Hamilton and Madison envisioned a strong central government that broke down the barriers to commerce among states. This Part outlines the primary reasons for their strong preference for federal control over business regulations rather than the state-centric regulation that existed under the Articles of Confederation.

A. The Confederation's Failures and the Need for a "Common Direction"

The call for a unified and national commercial regulation traces back before the Constitution to the confederated government under the Articles of Confederation, which were ratified in 1781.[15] Among the confederation's shortcomings were the barriers to commerce created by disparate state regulations, and these shortcomings led Hamilton, Madison, and others to conceptualize centralized regulation. The Articles of Confederation established a "league of friendship" among the states.[16] The unicameral confederation under the Articles had a far weaker central government that was effectively incapable of taxing and regulating commerce.[17] The economy was in shambles.[18]

15. ARTICLES OF CONFEDERATION of 1781, art. III.

16. *Id.*

17. *See* Gregory E. Maggs, *A Concise Guide to the Articles of Confederation as a Source for Determining the Original Meaning of the Constitution*, 85 GEO. WASH. L. REV. 397, 408 (2017) ("No provision gave Congress power to regulate commerce, a power which was left to the states themselves."); Douglas G. Smith, *An Analysis of Two Federal Structures: The Articles of Confederation and the Constitution*, 34 SAN DIEGO L. REV. 249, 286–87 (1997) ("The most important additions to the list of enumerated powers [in the Constitution] were the power to levy taxes and the power to regulate interstate and foreign commerce. The Articles had proved inadequate since under the Articles it was up to the states to obtain funds to support the general government.").

18. Grant S. Nelson & Robert J. Pushaw, Jr., *Rethinking the Commerce Clause: Applying First Principles to Uphold Federal Commercial Regulations but Preserve State Control Over Social Issues*, 85 IOWA L. REV. 1, 22 (1999) ("Several related problems had plunged the economy into an abyss. Most obviously, the break from England ruptured America's umbilical commercial connection to the

The Confederation Congress rejected proposals that would have allowed it to regulate interstate and foreign commerce.[19] George William Van Cleve attributes these rejections to "sectional jealousies" among states with different trade interests.[20] "In both Massachusetts and Virginia, opponents were fearful that if Congress received such broad powers, their states would be harmed by other sections with conflicting interests," Van Cleve wrote in an authoritative history of the confederated government.[21] "Massachusetts's legislature instead initially advocated a national convention on Confederation reform, but the state's congressional leaders persuaded it to drop its proposal."[22]

This left the states to take very different approaches to their own commercial regulations. Many of these regulations were seen as onerous and counterproductive.[23] As Barry Friedman and Daniel T. Deacon summarized:

> By the mid-1780s many American politicians had come to see the proliferation of state laws under the Articles of Confederation as a threat both to the Union and to the grand experiment in republicanism with which it was intimately bound. As early as 1780, James Iredell called the laws of North Carolina, his home state, "the vilest collection of trash ever formed by a legislative body." William Plumer – a prominent New Hampshire politician – was even more direct, writing, "Our liberties, our rights & property have become the sport of ignorant unprincipled State legislators!" A slew of specific state enactments, from various forms of debtor-relief legislation to paper-money laws, were roundly condemned for violating the

mother country, with special harm flowing from the loss of colonial subsidies and preferences.").

19. GEORGE WILLIAM VAN CLEVE, WE HAVE NOT A GOVERNMENT: THE ARTICLES OF CONFEDERATION AND THE ROAD TO THE CONSTITUTION 102 (2017).

20. *Id.*

21. *Id.*

22. *Id.* at 102–03; *see also* Nelson & Pushaw, *supra* note 18, at 23 ("Independent state governments filled the political vacuum. They were usually dominated by radically democratic legislatures, which pursued disastrous commercial policies. Especially pernicious were debtor relief laws, which enabled borrowers to avoid their contractual obligations and authorized the emission of worthless paper money.").

23. *See* BARRY FRIEDMAN, THE WILL OF THE PEOPLE: HOW PUBLIC OPINION HAS INFLUENCED THE SUPREME COURT AND SHAPED THE MEANING OF THE CONSTITUTION 24 (2009) ("Prominent members of the community began to express disgust as state legislatures regularly enacted laws that were seen as violating fundamental rights. Among the more frequent and troubling abuses were paper money and tender laws, debtor relief laws, and violations of the common law right to a trial by jury.").

> spirit of the Union and for inhibiting the general welfare of the population.[24]

States also stepped in to regulate trade, as the Confederation Congress had refused to do so. Van Cleve wrote that the state regulations varied significantly. For example, some states "imposed import duties, and some of them were discriminatorily higher on British shipping, goods, or both."[25] Some state duties were "costly to citizens of other states," Van Cleve wrote.[26] He elaborated:

> A substantial part of New York's import revenues came from citizens of Connecticut and New Jersey, who received no discernible benefits in return. Rhode Island's and Virginia's import duties similarly beggared their neighbors. But these self-interested policies achieved no significant change in British trade policy or improvement in America's massive negative balance of trade with Britain.[27]

In fact, during the Articles of Confederation period, other countries tightened their trade policies with the states. Spain claimed exclusive navigation rights over the Mississippi River.[28] France prohibited certain American exports and imports.[29] The states could not respond effectively.[30] The American economy plunged into a recession.[31] Members of the Confederation Congress were largely powerless, only capable of declaring foreign protectionism as "contemptable."[32] The lack of concentrated congressional power prevented a forceful response.

The nation's leading political thinkers recognized the harms of this state-by-state approach to commercial regulation. State regulation, Hamilton reasoned, would make sense if the states had "distinct interests" that were "unconnected with each other."[33] But that was not the case for states that are "parts of a whole, with a

24. Barry Friedman & Daniel T. Deacon, *A Course Unbroken: The Constitutional Legitimacy of the Dormant Commerce Clause*, 97 VA. L. REV. 1877, 1884–85 (2011) (footnotes omitted).

25. VAN CLEVE, *supra* note 19, at 112.

26. *Id.* at 112–13.

27. *Id.* at 113.

28. *Id.*

29. *Id.*

30. *See id.* at 114.

31. *Id.* at 117 ("As of May 1785, economic conditions in Massachusetts were dismal. To protect jobs, artisans there organized to seek trade protection from the legislature for domestic goods such as shoes. Manufacturers of twenty types of goods also met and resolved to seek protection. And agitated merchants began a vigorous campaign to get Massachusetts and other states to take action to improve conditions by granting new Confederation commerce powers or by tougher state legislation.").

32. *Id.*

33. 1 HAMILTON, *supra* note 14.

common interest in trade, as in other things."[34] Those states need a "common direction," Hamilton wrote on April 18, 1782, in *The Continentalist*.[35] He wrote:

> It is easy to conceive that many cases may occur in which it would be beneficial to all the States to encourage or suppress a particular branch of trade, while it would be detrimental to either to attempt it without the concurrence of the rest, and where the experiment would probably be left untried for fear of a want of that concurrence.[36]

For Hamilton, this common direction would result in a net benefit to the nation by allowing a free flow of goods across state borders.

B. The Inefficiency of Disparate Regulation

The Framers were concerned that the dispersed system of commercial regulations ultimately harmed the economy. In April 1787, James Madison published *Vices of the Political System of the United States*, a point-by-point takedown of America's confederated system of government.[37] Among his many complaints was that the

> practice of many States in restricting the commercial intercourse with other States, and putting their productions and manufactures on the same footing with those of foreign nations, though not contrary to the federal articles, is certainly adverse to the spirit of the Union, and tends to beget retaliating regulations, not less expensive & vexatious in themselves, than they are destructive of the general harmony.[38]

Madison argued that this problem contributed to the poor economic climate of the time. By imposing various requirements on business, he argued, there would never be a free flow of goods among the states. "How much has the national dignity, interest, and revenue suffered from this cause?" Madison asked.[39] He wrote:

> Instances of inferior moment are the want of uniformity in the laws concerning naturalization & literary property; of provision for national seminaries, for grants of incorporation for national purposes, for canals and other works of general utility, wch.

34. *Id.*
35. *Id.*
36. *Id.*
37. *See generally* JAMES MADISON, *Vices of the Political System of the United States*, *in* JAMES MADISON: WRITINGS 69 (Jack N. Rakove ed., 1999).
38. *Id.* at 71.
39. *Id.*

> may at present be defeated by the perverseness of particular States whose concurrence is necessary.[40]

To Madison, state-by-state regulation of commerce would also be unduly burdensome, particularly on smaller states that do not necessarily have the same interests as the more powerful states. In a letter to Edmund Randolph, Madison wrote:

> Nor should it be overlooked that as uniform regulations of the Commerce of the different States, will so differently affect their different interests, such regulations must be a strong temptation to measures in the aggrieved States which may first involve the whole confederacy in controversies with foreign nations, and then in contests with one another.[41]

Madison also questioned "whether the commercial interests of the States do not meet in more points than they differ," in a letter to James Monroe.[42] "To me it is clear that they do: and if they do there are so many more reasons for, than against, submitting the commercial interest of each State to the direction and care of the Majority."[43] For instance, Madison questioned the utility of state regulation of weights and measures, and he suggested a federal standard:

> Such a scheme appears to be easily reducible to practice; & as it is founded on the division of time which is the same at all times & in all places & proceeds on other data which are equally so, it would not only secure a perpetual uniformity throughout the U.S. but might lead to Universal standards in these matters among nations.[44]

To Madison, like Hamilton, there was little overall social gain for enacting disparate commercial regulations. The states had common interests, and Madison believed that they could better accomplish these by harmonizing their requirements for businesses.[45] Hamilton and Madison also worried about the impact of decentralized commercial regulation on foreign trade. Under the confederated government, states used their commerce powers to regulate trade with other nations, often to gain an advantage over other states. As Friedman and Deacon summarized:

---

40. *Id.*

41. JAMES MADISON, *To Edmund Randolph*, *in* JAMES MADISON: WRITINGS, *supra* note 37, at 20, 22.

42. JAMES MADISON, *To James Monroe*, *in* JAMES MADISON: WRITINGS, *supra* note 37, at 36, 38.

43. *Id.*

44. Letter from James Madison to James Monroe (Apr. 28, 1785) (on file with the Library of Congress), https://www.loc.gov/resource/mjm.02_0375_0377/.

45. Brannon P. Denning, *Confederation-Era Discrimination Against Interstate Commerce and the Legitimacy of the Dormant Commerce Clause Doctrine*, 94 KY. L.J. 37, 49–50 (2005).

> Particularly irksome to national-minded politicians was the practice of some states of establishing duty-free ports, where foreign vessels were free to trade without paying onerous duties. Free ports were most likely to be found in states with lesser ports. These states hoped to attract a greater volume of trade at the expense of states, such as New York, with high tariffs on foreign goods. The existence of free ports substantially undercut the revenue-related value of state imposts by diverting trade away from states in which they existed and hindered the ability of the Union to effectively respond to Britain's discriminatory practices.[46]

Madison, Hamilton, and others had taken their concerns to the Confederation Congress with little success. They argued that a lack of centralized commerce powers undercuts the nation's ability to conduct trade with foreign nations.[47] An April 1784 congressional committee report predicted that "[u]nless the United States can act as a nation and be regarded as such by foreign powers . . . they can never command reciprocal advantages in trade and without such reciprocity our foreign Commerce must decline and eventually be annihilated."[48]

In May 1787, the Constitutional Convention began in Philadelphia.[49] Debate at the convention was centered on the Virginia Plan, which Madison drafted.[50] The plan, which favored larger states, urged the creation of a population-based national legislature with the power to pass laws "in all cases to which the separate States are incompetent: or in which the harmony of the United States may be interrupted by the exercise of individual legislation."[51]

At the Constitutional Convention, Noah Webster circulated a pamphlet, *An Examination Into the Leading Principles of the Federal Constitution*, which advocated for the adoption of a new Constitution.[52] Webster vociferously argued for a centralized national government that regulated commerce and performed other functions that states had not adequately handled, such as national

46. Friedman & Deacon, *supra* note 24, at 1888.

47. Denning, *supra* note 45.

48. VAN CLEVE, *supra* note 22, at 103.

49. *The New Nation, 1783-1815*, LIBRARY CONGRESS, http://www.loc.gov/teachers/classroommaterials/presentationsandactivities/presentations/timeline/newnatn/usconst/ (last visited Mar. 2, 2019).

50. *Virginia Plan (1787)*, OURDOCUMENTS.GOV, https://www.ourdocuments.gov/doc.php?flash=false&doc=7 (last visited Mar. 2, 2019).

51. *Transcript of Virginia Plan (1787)*, OURDOCUMENTS.GOV, https://www.ourdocuments.gov/doc.php?flash=false&doc=7&page=transcript# (last visited Mar. 2, 2019).

52. *See* NOAH WEBSTER, AN EXAMINATION INTO THE LEADING PRINCIPLES OF THE FEDERAL CONSTITUTION 50 (Prichard & Hall eds., 1787).

defense.[53] He wrote that a strong, centralized government was vital to the nation's survival.[54] He continued:

> Without powers lodged somewhere in a single body, fully competent to lay and collect equal taxes and duties—to adjust controversies between different states—to silence contending interests—to suppress insurrections—to regulate commerce—to treat with foreign nations, our confederation is a cobweb—liable to be blown asunder by every blast of faction that is raised in the remotest corner of the United States.[55]

Also at the Constitutional Convention, John Jay circulated an influential pamphlet entitled *An Address to the People of the State of New York* that made the case for a strong federal government.[56] Among his reasons was that the Confederation Congress' power to regulate business was weak.[57] "They may partly regulate commerce, but without authority to execute their ordinances," Jay wrote.[58] He implored New York citizens to consider the harm that the state's discriminatory taxation laws had on New Jersey and Connecticut.[59] "They cannot, they will not love you—they border upon you, and are your neighbours; but you will soon cease to regard their neighbourhood as a blessing," Jay wrote.[60] "You have but one port and outlet to your commerce, and how you are to keep that outlet free and uninterrupted, merits consideration."[61]

The Constitutional Convention concluded on September 17, 1787,[62] with the adoption of a constitution that contained the Commerce Clause, which provided Congress with power to "regulate Commerce with foreign Nations, and among the several States, and with the Indian Tribes."[63] Although the final text did not provide the same breadth of federal power as Madison had urged in the Virginia Plan, it generally addressed the Framers' concerns about disparate state regulations by entrusting Congress with the ability to regulate interstate commerce.[64] Then began an arduous process for states to

53. *Id.*
54. *Id.*
55. *Id.*
56. JOHN JAY, AN ADDRESS TO THE PEOPLE OF THE STATE OF NEW-YORK 8 (Samuel Loudon & John Loudon eds., 1788).
57. *Id.* at 16.
58. *Id.* at 6.
59. *Id.* at 16–17.
60. *Id.* at 17.
61. *Id.*
62. *The New Nation, 1783-1815*, *supra* note 49.
63. U.S. CONST. art. I, § 8, cl. 3.
64. *See* Scott Boykin, *The Commerce Clause, American Democracy, and the Affordable Care Act*, 10 GEO. J.L. & PUB. POL'Y 89, 94–95 (2012) ("The Framers adopted the Commerce Clause for narrow purposes. They intended the commerce power to enable the national government to conduct a uniform trade policy with foreign nations, to establish domestic free trade, and to reduce

ratify the new Constitution.[65] Many controversies created opposition, among them the regulatory power of Congress relative to the states.

C. "Neighbourly" Interstate Relations

After the Constitutional Convention, a chorus of anti-federalist voices emerged, opposing the ratification of the Constitution and its strong central government.[66] Hamilton, Madison, and Jay responded with a series of essays in newspapers. The eighty-five essays, published under the pseudonym "Publius" between October 1787 and May 1788, become known as the *Federalist Papers*.[67] The *Federalist Papers* cover many issues related to this new form of government, including separation of powers among the three branches, the structure of the military, and protection of individual liberties.[68] Among the *Federalist Papers*' complaints about the confederated government was its dispersed regulation of businesses.[69] Hamilton and Madison used their essays to argue for a unified commercial framework.

In *Federalist No. 22*, Hamilton wrote of his concern that the "prohibitions, restrictions and exclusions" of the "[s]everal States" had "frustrated every experiment of the kind."[70] Hamilton speculated that states had enacted regulations on commerce to bolster their own competitive advantages at the expense of other states:

> The interfering and unneighbourly regulations of some States, contrary to the true spirit of the Union, have in different instances, given just cause of umbrage and complaint to others; and it is to be feared that examples of this nature, if not restrained by a national controul, would be multiplied and extended till they became not less serious sources of animosity and discord, than injurious impediments to the intercourse between the different parts of the confederacy.[71]

Hamilton predicted that "the gradual conflicts of State regulations" would cause citizens of each state to "come to be considered and treated by the others in no better light than that of foreigners and

interstate political conflict. These were the Framers' intentions, and there is no legitimate basis in the historical record for ascribing any more ambitious purpose to the Commerce Clause than these.").

65. *The New Nation, 1783-1815*, *supra* note 49.

66. *The Federalist*, U.S. SENATE, https://www.senate.gov/reference/reference_item/federalist.htm (last visited Mar. 2, 2019).

67. *Id.*

68. *See id.* (describing the *Federalist Papers* as "an eloquent defense of constitutional government").

69. ALEXANDER HAMILTON, *The Federalist No. 22*, *in* ALEXANDER HAMILTON: WRITINGS 243, 243 (Joanne B. Freeman ed., 2001).

70. *Id.* at 244.

71. *Id.*

aliens."[72] Indeed, in *Federalist No. 7*, Hamilton predicted that state regulation of commerce in other states could cause war among the states:

> The spirit of enterprise, which characterises the commercial part of America, has left no occasion of displaying itself unimproved. It is not at all probable that this unbridled spirit would pay much respect to those regulations of trade, by which particular States might endeavor to secure exclusive benefits to their own citizens. The infractions of these regulations on one side, the efforts to prevent and repel them on the other, would naturally lead to outrages, and these to reprisals and wars.[73]

Hamilton also argued that vesting federal courts with the power to adjudicate commercial law is preferable to such disputes being adjudicated in state court, which could discriminate against out-of-state litigants: "In this case if the particular tribunals are invested with a right of ultimate jurisdiction, besides the contradictions to be expected from difference of opinion, there will be much to fear from the bias of local views and prejudices, and from the interference of local regulations," Hamilton wrote in *Federalist No. 22*, published on December 14, 1787, in *The New-York Packet*.[74] Four days later, the newspaper published Hamilton's *Federalist No. 23*, in which he argued that the federal government "must be empowered to pass all laws, and to make all regulations which have relation to them," and that "[t]he same must be the case, in respect to commerce, and to every other matter to which its jurisdiction is permitted to extend."[75]

Hamilton also recognized the advantages that national commerce regulation would present for foreign trade. In *Federalist No. 11*, he wrote of the need for states to stand together against commercial threats from Europe and the difficulty of doing so without a unified central government with jurisdiction over commerce and trade:

> Facts have too long supported these arrogant pretensions of the European: It belongs to us to vindicate the honor of the human race, and to teach that assuming brother moderation. Union will enable us to do it. Disunion will add another victim to his triumphs. Let Americans disdain to be the instruments of European greatness! Let the thirteen States, bound together in

72. *Id.*

73. ALEXANDER HAMILTON, *The Federalist No. 7*, *in* ALEXANDER HAMILTON: WRITINGS, *supra* note 69, at 183, 186; *see* DAN T. COENEN, THE STORY OF THE FEDERALIST: HOW HAMILTON AND MADISON RECONCEIVED AMERICA 70 (2007) ("For Hamilton and Madison, the drift toward disunion fostered by the Articles of Confederation all but ensured future armed clashes among the former allies of the Revolution.").

74. HAMILTON, *supra* note 69, at 250.

75. ALEXANDER HAMILTON, *The Federalist No. 23*, *in* ALEXANDER HAMILTON: WRITINGS, *supra* note 69, at 253, 255.

> a strict and indissoluble union, concur in erecting one great American system, superior to the controul of all trans-atlantic force or influence, and able to dictate the terms of the connection between the old and the new world![76]

Federalists argued that strengthening federal regulation of commerce and trade would cause a free flow of goods across state lines. In *Federalist No. 42*, Madison looked to Europe for examples of such unencumbered commerce:

> In Switzerland, where the union is so very slight, each canton is obliged to allow to merchandizes, a passage through its jurisdiction into other cantons, without an augmentation of the tolls. In Germany, it is a law of the empire, that the princes and states shall not lay tolls or customs on bridges, rivers, or passages, without the consent of the emperor and diet . . . . Among the restraints imposed by the union of the Netherlands, on its members, one is, that they shall not establish imposts disadvantageous to their neighbours, without the general permission.[77]

Madison asserted that centralized commercial regulation would be more efficient to the overall American economy. On June 11, 1778, Madison spoke to the Virginia Ratifying Convention of the "great saving of expence and time" under a strong federal regulatory system.[78] "The greatest calamity to which the United States can be subject, is a vicissitude of laws, and continual shifting and changing from one object to another, which must expose the people to various inconveniences," Madison said.[79]

> This has a certain effect, of which sagacious men always have, and always will make an advantage. From whom is advantage made? From the industrious farmers and tradesmen, who are ignorant of the means of making such advantages. The people will not be exposed to these inconveniences under an uniform and steady course of legislation.[80]

Although the Internet would not exist until nearly two hundred years after the ratification of the Constitution, there is little doubt that the Framers would have considered such technology to fall within the scope of interstate commerce best regulated at the federal level. Indeed, in his farewell address, George Washington associated

76. ALEXANDER HAMILTON, *The Federalist No. 11*, *in* ALEXANDER HAMILTON: WRITINGS, *supra* note 69, at 202, 208.

77. JAMES MADISON, *The Federalist No. 42*, *in* JAMES MADISON: WRITINGS, *supra* note 37, at 235, 239.

78. JAMES MADISON, *Speech in the Virginia Ratifying Convention on Direct Taxation*, *in* JAMES MADISON: WRITINGS, *supra* note 37, at 366, 379.

79. *Id.*

80. *Id.*

communications improvements with enhancements to commerce throughout the United States:

> The *East*, in a like intercourse with the *West*, already finds, and in the progressive improvement of interior communications, by land and water, will more and more find a valuable vent for the commodities which it brings from abroad, or manufactures at home. The *West* derives from the *East* supplies requisite to its growth and comfort, and, what is perhaps of still greater consequence, it must of necessity owe the *secure* enjoyment of indispensable *outlets* for its own productions to the weight, influence, and the future Maritime strength of the Atlantic side of the Union, directed by an indissoluble community of Interest as *one Nation*.[81]

When interpreting the scope of federal and state authority to regulate commerce, courts often look to the statements of Madison and Hamilton. For instance, in 1944, amid the expansion of federal commerce powers, Justice Black cited numerous *Federalist Papers* for the proposition that the "federal power to determine the rules of intercourse across state lines was essential to weld a loose confederacy into a single, indivisible Nation; its continued existence is equally essential to the welfare of that Nation."[82]

III. THE HAMILTONIAN CASE FOR CENTRALIZED CYBERSECURITY LAW

The United States has not fully realized the national system of commercial regulation that Hamilton and Madison envisioned. Of course, the federal government's commerce regulation is sweeping in many sectors, particularly since the New Deal.[83] States continue to regulate some commerce, provided that Congress has not either expressly or implicitly preempted the regulation with a federal law within Congress' Commerce Clause powers.[84] States often regulate local commerce, such as by licensing building contractors and hair

81. GEORGE WASHINGTON, *Farewell Address*, *in* GEORGE WASHINGTON: WRITINGS 962, 965–66 (John Rhodehamel ed., 1997).

82. *See, e.g.*, United States v. Se. Underwriters Ass'n., 322 U.S. 533, 552 (1944).

83. Jack M. Balkin, *Commerce*, 109 MICH. L. REV. 1, 3 (2010) ("Without the New Deal transformation in constitutional understandings about national power, we could not have a federal government that provides all of the social services and statutory rights guarantees that Americans have come to expect. The government could neither act to protect the environment nor rescue the national economy in times of crisis.").

84. *See id.* at 6 (articulating an approach to Commerce Clause analysis that "shows why there are still areas where federal commerce power does not extend–these are areas where Congress cannot reasonably claim that an activity produces interstate spillovers or collective action problems, and does not involve networks of transportation and communication").

stylists.[85] Cybersecurity regulation, however, is an inherently interstate endeavor, yet a patchwork of state regulations predominate. This Part first summarizes the current state of U.S. cybersecurity law and the related field of data protection. It then explains the practical burdens of this system and describes how it fails to satisfy the Framers' vision of a national commercial regulatory system. Congress can—and should—pass comprehensive cybersecurity legislation that preempts state-by-state efforts to regulate this inherently interstate field.

A. The Current State of U.S. Cybersecurity Regulation

To understand the current state of cybersecurity law, it is important to define what I mean by "cybersecurity law." The term has many meanings in technical and legal circles. Often, "cybersecurity law" is conflated with "data security law."[86] Cybersecurity law encompasses data security, but for this Article "cybersecurity law" is broader and includes security of systems and networks. Moreover, cybersecurity promotes not only (1) confidentiality but also (2) integrity and (3) availability (known in cybersecurity circles as the "CIA Triad").[87] In a recent *Iowa Law Review* article, after synthesizing the technical and legal authorities, I defined "cybersecurity law" as laws that promote "the confidentiality, integrity, and availability of public and private information, systems, and networks, through the use of forward-looking regulations and incentives, with the goal of protecting individual rights and privacy, economic interests, and national security."[88] This Article also includes the related but distinct concept of "data protection law." Data protection law has become particularly prominent since 2016 when the European Union

85. *See generally* W. Sherman Rogers, *Occupational Licensing: Quality Control or Enterprise Killer? Problems that Arise When People Must Get the Government's Permission to Work*, 10 BUS., ENTREPRENEURSHIP & L. 146 (2017) (describing various occupations subject to state licensing requirements).

86. Jason Fornicola, *Cybersecurity vs. Data Security: Government's Two-Pronged Challenge*, FED. NEWS NETWORK (Oct. 7, 2015, 10:01 AM), https://federalnewsradio.com/sponsored-content/2015/10/cybersecurity-vs-data-security-governments-two-pronged-challenge ("Many organizations, agencies and the private sector spend much of their resources on cybersecurity. And with the recent data breaches at the Office of Personnel Management, Target, JP Morgan Chase and a host of other large organizations, are agencies and companies focusing on the wrong issues? If you look at recent legislation, it's focused on information security, whether it's the federal information security management act or the cyber information sharing protection act or a host of other bills. Then what is cybersecurity and how does it relate to data security?").

87. Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 997 (2018).

88. *Id.* at 1010.

approved the General Data Protection Regulation ("GDPR"),[89] which provides individuals with broad rights to access, delete, and transfer their personal data.[90] Data protection is closely related to cybersecurity because it requires companies to implement extensive data security safeguards on personal data and to impose those data security requirements on any contractors or business partners that handle personal data.[91] Data protection law also provides individuals with the ability to hold companies accountable for data security failures.[92]

State and federal laws go beyond mere private-sector regulations. For example, laws also set minimum cybersecurity standards for government information systems[93] and establish mechanisms by which the private sector can exchange cyber threat information with the government and other companies.[94] However, this Article focuses on cybersecurity and data protection laws that regulate the private sector. Unlike other jurisdictions, such as the European Union and China, the United States lacks a broad law or regulation that regulates and promotes cybersecurity across sectors.[95] At the federal level, the United States has enacted data security statutes and regulations for particularly sensitive types of data. For instance, regulations promulgated under the Health Insurance Portability and Accountability Act of 1996 include a "Security Rule" that specifies technical, administrative, and physical safeguards that covered

89. Commission Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Council Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter General Data Protection Regulation].

90. *Id.* at 7.

91. Josh Eichorn, *Life Under #GDPR and What it Means for Cybersecurity*, INFOSECURITY (Apr. 25, 2018), https://www.infosecurity-magazine.com/opinions/life-gdpr-cybersecurity/ ("Since GDPR lends itself to the expectation of increased data privacy, this builds pressure on websites to tighten their cybersecurity and even integrate new practices.").

92. *See* General Data Protection Regulation, *supra* note 89, at 1, 81.

93. *See* 44 U.S.C. § 3551(1) (2012) (providing "a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets").

94. *See* 6 U.S.C. § 1505(b) (2012) ("No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the sharing or receipt of a cyber threat indicator or defensive measure under section 1503(c) of this title.").

95. *See generally* General Data Protection Regulation, *supra* note 89 (describing the European Union's expansive cybersecurity law); Kosseff, *supra* note 87 (describing the patchwork of U.S. cybersecurity laws and regulations related across various sectors); Liudmyla Balke, Note, *China's New Cybersecurity Law and U.S.–China Cybersecurity Issues*, 58 SANTA CLARA L. REV. 137 (2018) (discussing recent Chinese legislation that produced an expansive cybersecurity regulatory framework).

entities must apply to protected health information.[96] The Gramm-Leach-Bliley Act, a 1999 overhaul of the financial regulatory system, includes a "Safeguards Rule" that requires regulated financial institutions to "insure the security and confidentiality of customer records and information."[97] The Securities and Exchange Commission ("SEC") released guidance that suggests publicly traded companies have an obligation to disclose material cybersecurity risks and incidents to their shareholders in public SEC filings.[98]

The closest thing that the United States has to a national cybersecurity regulator is the Federal Trade Commission ("FTC"), though the FTC lacks a statute that explicitly provides it with the authority to regulate cybersecurity.[99] Rather, the FTC draws its data security authority from § 45 of the FTC Act, which declares illegal "unfair or deceptive acts or practices in or affecting commerce."[100] The FTC can bring an enforcement action against a company for a "deceptive" data security practice if a company misrepresents its safeguards (such as in a privacy policy).[101] "Unfairness" is more controversial,[102] as the FTC Act vaguely defines unfair trade practices as those 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."[103] In August 2015, the United States Court of Appeals for the Third Circuit affirmed the FTC's ability to bring data security actions under the FTC Act's unfairness prong.[104]

The FTC has brought about seventy data security-related enforcement actions since 2000.[105] The agency's enforcement authority has three primary shortcomings. First, the FTC rarely

96. *See, e.g.*, 45 C.F.R. §§ 164.308, 164.310, 164.312 (2017); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, § 1173(d)(2), 110 Stat. 1936, 2026 (1996) (codified at 42 U.S.C. § 1320d–2).

97. *See, e.g.*, 15 U.S.C. § 6801(b)(1) (2012); Gramm–Leach–Bliley Act, Pub. L. No. 106–102, § 501(b), 113 Stat. 1338, 1436–37 (1999) (codified at 15 U.S.C. § 6801).

98. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8166–72 (Feb. 26, 2018).

99. Kosseff, *supra* note 87, at 1010–11.

100. 15 U.S.C. § 45(a)(1) (2012).

101. *See* Kosseff, *supra* note 87, at 1012.

102. Glenn G. Lammi, *FTC Must Refocus on Harm to Consumers and Competition*, FORBES (Mar. 8, 2017, 2:03 PM), https://www.forbes.com/sites/wlf/2017/03/08/ftc-must-refocus-on-harm-to-consumers-and-competition ("What, in the context of a data breach, is unfair? The answer to that is quite troubling: enforcement targets can discover the term's meaning in the nearly 60 settlement agreements FTC has reached with other parties accused of unfair practices after a data breach.").

103. 15 U.S.C. § 45(n).

104. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015).

105. *See Data Security*, FED. TRADE COMMISSION, https://www.ftc.gov/datasecurity (follow "Cases" drop-down menu) (last visited Mar. 2, 2019).

issues fines for data security violations of the FTC Act.[106] Instead, it typically signs a consent decree with a company in lieu of pursuing a lawsuit, and under this agreement the FTC may fine the company if the company fails to improve its security or rejects the FTC's extensive oversight.[107] Although FTC investigations and agreements are inconvenient and can be costly, they do not necessarily have the same deterrent effect as large statutory fines.[108] Second, although the FTC has published guidance about best practices for data security,[109] these regulations are not binding and do not provide businesses with certainty that they will be in compliance if they adopt the safeguards. For instance, the FTC's guidance suggests that companies "may want to consider" authentication controls such as two-factor authentication.[110] Would that be sufficient to avoid an unfairness claim after a data breach? The answer is unclear because this guidance is not a binding regulation. Moreover, the FTC Act does not explicitly require companies to mitigate harm, such as by notifying victims and regulators.[111] Finally, the FTC simply does not have the resources to regulate the rapidly growing field of cybersecurity. Data security enforcement is performed by the Division of Privacy and Identity Protection, within the FTC's Bureau of Consumer Protection, and it is responsible not only for data

106. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 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. . . . When the FTC does include fines, they are often quite small in relation to the gravity of the violations and the overall net profit of the violators.").

107. *See* Michelle De Mooy, *How to Strengthen the FTC Privacy & Security Consent Decrees*, CTR. FOR DEMOCRACY & TECH. (Apr. 12, 2018), https://cdt.org/blog/how-to-strengthen-the-ftc-privacy-security-consent-decrees/.

108. *Id.* ("While the terms of FTC consent orders can appear quite detailed and privacy-protective, there is considerable evidence that consent orders 'lack teeth,' permitting companies tremendous flexibility to satisfy the terms of the consent order without improving privacy and security practices internally. When the FTC has enforced the terms of its consent decree, the resulting penalties can be so miniscule as to ensure the penalties are simply the cost of doing business. For instance, when Google agreed to pay a $22.5 million penalty for violating the terms of its consent order, this amounted to less than half a single day's revenue.").

109. *See generally* FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (suggesting practical guidance on how to reduce a variety of risks associated with maintaining sound security).

110. *Id.* at 5.

111. *See* Gregory James Evans, *Regulating Data Practices: How State Laws Can Shore Up the FTC's Authority to Regulate Data Breaches, Privacy, and More*, 67 ADMIN. L. REV. 187, 204 (2015).

security but privacy and identity theft.[112] That division, responsible for privacy, data security, and identity theft regulation nationwide, employed fifty-two full-time employees in the 2018 fiscal year.[113] The roughly seventy data security enforcement actions since 2000 represent a small fraction of the thousands of large data breaches that occur in the United States each year.[114] In June 2018, FTC Chairman Joseph Simons said that the FTC's limited data security authority is "something that's of serious concern to me," and that he is "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."[115]

The federal government's cybersecurity regulation is scattered and weak. States have recognized this problem and have passed their own statutes to regulate private-sector cybersecurity. Most pervasive are statutes that require companies to notify victims and regulators of data breaches. Every state and the District of Columbia have passed such statutes.[116] The statutes share some common requirements; for instance, the laws apply to a person's name combined with a social security number, driver's license or state identification, or full financial account information.[117] However, the laws contain several key differences. Some breach notice laws are triggered by disclosing other information, including medical

112. *Division of Privacy and Identity Protection*, FED. TRADE COMMISSION, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-privacy-and-identity (last visited Mar. 2, 2019).

113. FED. TRADE COMM'N, FISCAL YEAR 2019 CONGRESSIONAL BUDGET JUSTIFICATION 41 (2018), https://www.ftc.gov/system/files/documents/reports/fy-2019-congressional-budget-justification/ftc_congressional_budget_justification_fy_2019.pdf; *see 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 Rebecca Kelly Slaughter, Comm'r, FTC) ("We have excellent, expert, experienced staff who want nothing more than to hold law breakers accountable; we leverage them as effectively as possible. But we have more cases to bring every day, those cases have become more complex both legally and technologically, and they involve defendants with deep pockets and armies of attorneys. Our budget has not kept pace with these developments; to wit, we had more [full-time equivalents] in the Reagan administration than we do today.").

114. *See* IDENTITY THEFT RES. CTR., 2017 ANNUAL DATA BREACH YEAR-END REVIEW 6 (2018), https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf.

115. C. Ryan Barber, *FTC's Limited Data-Privacy Power Makes Chair Joe Simons 'Nervous'*, NAT'L L.J. (June 20, 2018, 5:27 PM), https://www.law.com/nationallawjournal/2018/06/20/ftcs-limited-data-privacy-power-makes-chair-joe-simons-nervous/.

116. For a complete list of state data breach notification statutes, see *Security Breach Notification Laws*, *supra* note 10.

117. *See* JEFF KOSSEFF, CYBERSECURITY LAW 38 (2017).

information, biometric data, and online account credentials.[118] North Dakota has the most sweeping breach notice law, requiring notification upon disclosure of birth date, mother's maiden name, employment identification number, and other types of personal data.[119] The laws do not apply if the compromised information was encrypted, though Tennessee briefly (and inexplicably) deleted this exception from its breach notice law.[120]

State breach notice laws also contain different notification requirements. Most states only require notification if the company determines that the breach poses a risk of harm to an individual,[121] though some "strict liability" states require notification even if the company determines that the breach poses no risk of harm.[122] Some statutes require notifications to contain particular elements, such as contact information for a state attorney general or the FTC.[123]

About a dozen states also have enacted separate data security laws.[124] Most laws are general and require companies to implement "reasonable" data security policies and procedures.[125] However, some are more specific. Oregon's data security statute provides examples of particular safeguards, such as employee training and risk assessments, to satisfy its reasonableness requirements.[126] Rhode Island requires a company's data security program to be "appropriate" to the company's size, the type of information, and the

118. *Id.* ("In addition to those three elements, a number of other states include elements that, combined with an individual's name, trigger a data breach requirement . . . .").

119. *Id.*

120. Andrew M. Ballard, *Tennessee to Clarify Breach Notice Encryption Exemption*, BLOOMBERG LAW (Mar. 28, 2017), https://www.bna.com/tennessee-clarify-breach-n57982085804/ ("Tennessee's 2005 breach notice law specifically provided an exception to providing notice if the breached data were encrypted. But in 2016, the law was amended to remove the specific exemption but still mentioned encryption as a means of protecting data. That change cast doubt for many on whether the breach notice encryption exception was still allowed under the Tennessee law. The new amendment would reinstate the encryption language in the statute to remove any doubt that companies need not give breach notice of encrypted data, unless the encryption key was also breached.").

121. *See* Rachael M. Peters, Note, *So You've Been Notified, Now What? The Problem with Current Data-Breach Notification Laws*, 56 ARIZ. L. REV. 1171, 1182–83 (2014).

122. *See id.*

123. *See* BAKERHOSTETLER, DATA BREACH CHARTS: JULY 2018, at 16–22 (2018), https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf.

124. For a list of these laws, see KOSSEFF, *supra* note 117, at 42–48.

125. *See* Philip N. Yannella, *What Does "Reasonable" Data Security Mean, Exactly?*, BALLARD SPAHR LLP (July 20, 2018), https://www.cyberadviserblog.com/2018/07/what-does-reasonable-data-security-mean-exactly/.

126. OR. REV. STAT. § 646A.622(2)(d)(A) (2017).

purpose for the information.[127] Nevada requires encryption for transferring its residents' personal information.[128]

Massachusetts has the most specific general data security law. Its Department of Consumer Affairs and Business Regulation has the statutory authority to develop regulations for protecting the confidentiality and security of the personal information of Massachusetts residents.[129] The regulations cover a wide range of specific administrative, physical, and technical safeguards. They require companies to designate an employee responsible for information security, disciplinary procedures for employees who violate data security policies, restrictions on physical access to stored data, and regular monitoring of compliance with data security policies.[130]

States also regulate the cybersecurity of specific industries, even if the federal government has enacted its own cybersecurity laws for those sectors. For instance, Connecticut requires health insurers to maintain a "comprehensive information security program to safeguard the personal information of insureds and enrollees."[131] And in 2017, the New York Department of Financial Services ("DFS") issued cybersecurity regulations for the financial institutions that it regulates.[132] The regulations require companies to regularly monitor and test their cybersecurity defenses[133] and to have security policies that cover at least fourteen enumerated topics, such as data classification, business continuity, and incident response.[134] The New York DFS also requires several specific technical safeguards, such as reporting data breaches within seventy-two hours, encryption of nonpublic information in transit at rest,[135] and multifactor authentication.[136] Regulated financial institutions pushed back on

127. 11 R.I. GEN. LAWS § 11-49.3-2(a) (2018).
128. NEV. REV. STAT. § 603A.215(2)(a) (2017).
129. MASS. GEN. LAWS ch. 93H, § 2(a) (2017).
130. 201 MASS. CODE REGS. 17.03(2) (LexisNexis 2018).
131. CONN. GEN. STAT. § 38a-999b(b)(1) (2018).
132. N.Y. COMP. CODES R. & REGS. tit. 23, § 500.0 (2018).
133. *Id.* § 500.5 ("The cybersecurity program for each covered entity shall include monitoring and testing, developed in accordance with the covered entity's risk assessment, designed to assess the effectiveness of the covered entity's cybersecurity program.").
134. *See, e.g.*, *id.* § 500.16 ("As part of its cybersecurity program, each covered entity shall establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event materially affecting the confidentiality, integrity or availability of the covered entity's information systems or the continuing functionality of any aspect of the covered entity's business or operations.").
135. *Id.* § 500.15(a) ("As part of its cybersecurity program, based on its risk assessment, each covered entity shall implement controls, including encryption, to protect nonpublic information held or transmitted by the covered entity both in transit over external networks and at rest.").
136. *Id.* § 500.12 ("Based on its risk assessment, each covered entity shall use effective controls, which may include multi-factor authentication or risk-based

the regulations as overly burdensome and convinced the New York DFS to scale back a few of the most onerous requirements.[137] Some cybersecurity and privacy professionals lauded the new rule, with one saying it was "designed to increase accountability and remove the fog of uncertainty that often surrounds breaches."[138] Another analysis dubbed it "one of the most, if not *the* most, prohibitive and burdensome cybersecurity regimes."[139] Regardless of where a company is headquartered, if it is subject to any regulation by the New York DFS, it must self-certify compliance and subject itself to potential enforcement actions for noncompliance.[140]

State common law also plays an increasingly important role in data security law. Data breach victims sue companies for failing to safeguard their personal information. The lawsuits, often filed on behalf of a large class, include claims under state law for breach of contract,[141] negligence,[142] breach of warranty,[143] and unjust enrichment.[144] For instance, the class action lawsuit filed against Target after its 2013 breach of payment card information was 126 pages, with claims arising under most states' common laws.[145] Although common-law claims share many of the same elements across state lines, their parameters are set by the highest court in

authentication, to protect against unauthorized access to nonpublic information or information systems.").

137. *See* Press Release, N.Y. State Dep't of Fin. Servs., DFS Issues Updated Proposed Cybersecurity Regulation Protecting Consumers and Financial Institutions (Dec. 28, 2016), https://www.dfs.ny.gov/about/press/pr1612281.htm; *see also* Jacob A. Lutz, III & Shannon VanVleet Patterson, *Revision to New York's Proposed Cybersecurity Regulations Reflect Risk-Based Approach*, TROUTMAN SANDERS (Jan. 17, 2017), https://www.troutman.com/revision-to-new-yorks-proposed-cybersecurity-regulations-reflect-risk-based-approach-01-17-2017/.

138. Nathaniel Fick, Opinion, *Cybersecurity Today is Treated Like Accounting Before Enron*, N.Y. TIMES (Jan. 8, 2018), https://www.nytimes.com/2018/01/08/opinion/cybersecurity-breach-spectre-meltdown.html.

139. Charles M. Horn & Mark L. Krotoski, *New York Department of Financial Services Modifies, Delays Implementation of Cybersecurity Rules*, NAT'L L. REV. (Jan. 11, 2017), https://www.natlawreview.com/article/new-york-department-financial-services-modifies-delays-implementation-cybersecurity.

140. N.Y. COMP. CODES R. & REGS. tit. 23, § 500.21 (2018) ("Covered entities will be required to annually prepare and submit to the superintendent a certification of compliance with New York State Department of Financial Services Cybersecurity Regulations . . . .").

141. *See, e.g.*, Sovereign Bank. v. BJ's Wholesale Club, Inc., 533 F.3d 162, 168 (3d Cir. 2008).

142. *See, e.g.*, *In re* Sony Gaming Networks & Customer Data Sec. Data Breach Litig., 996 F. Supp. 2d 942, 963 (S.D. Cal. 2014).

143. *See, e.g.*, *In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 613 F. Supp. 2d 108, 119–20 (D. Me. 2009), *aff'd in part, rev'd in part on other grounds sub nom. on other grounds*, Anderson v. Hannaford Bros. Co., 659 F.3d 151, 167 (1st Cir. 2011).

144. *See, e.g.*, Resnick v. AvMed, Inc., 693 F.3d 1317, 1328 (11th Cir. 2012).

145. *See* Consumer Plaintiffs' Consolidated Class Action Complaint at 113, 114, 118, *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154 (D. Minn. 2014) (No. 14-2522).

each state. Therefore, there is significant variation on issues, such as standard of care.[146]

In 2018, California passed what is perhaps the most sweeping state restriction on information, going far beyond the data security and privacy protections seen in other state or federal laws. The California Consumer Privacy Act of 2018 ("CCPA"), a ten-thousand-word statute, contains several restrictions on a company's ability to disclose and sell Californians' personal information[147] and requires that a company allow customers to access and delete their personal information.[148] The CCPA has some similarities to Europe's GDPR.[149] Although the CCPA, like the GDPR, is a data protection law and not explicitly confined to cybersecurity, it imposes significant cybersecurity obligations. Companies must "implement and maintain reasonable security procedures and practices appropriate to the nature of the information," and if they experience a data breach, they could face a lawsuit with statutory damages ranging from $100 to $750 per victim.[150] Data breach victims can sue under many of causes of action (such as negligence, breach of contract, and violation of state consumer protection laws) in all fifty states, but these laws typically allow recovery only of actual damages.[151] What is unique about the CCPA is that it permits statutory damages.[152] Imagine that a retailer with 100,000 California customers suffered a data breach and faced a class-action lawsuit. Even if a court awarded the lowest possible amount of statutory damages—$100 per victim—the company would be liable for $10,000,000. If a court awarded the highest amount of statutory damages—$750 per victim—the company would be liable for $75,000,000. This vastly increases the potential liability for companies, as actual damages from data breaches are difficult to prove absent identity theft.

B. U.S. Cybersecurity Law Lacks a Common Direction

State legislators and regulators have gone far beyond the limited cybersecurity requirements of federal law and imposed far more demanding standards on U.S. companies. These laws impose specific —and often difficult—requirements, and sometimes they are not in harmony with one another. The U.S. cybersecurity legal framework

146. *See, e.g.*, *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1171–76 (D. Minn. 2014) (presenting separate analyses of the economic loss doctrine in negligence claims for eleven states in a data breach lawsuit).

147. CAL. CIV. CODE § 1798.100 (Deering 2018).

148. *Id.* § 1798.105.

149. General Data Protection Regulation, *supra* note 89, at 87.

150. CAL. CIV. CODE § 1798.150.

151. *See, e.g.*, ALASKA STAT. §§ 45.50.471(b)(55), 45.50.531(a) (2018); S.C. CODE ANN. § 39-1-90 (2018).

152. *See* CAL. CIV. CODE § 1798.150.

is far from the common direction for commercial regulation that Hamilton and Madison envisioned.

Cybersecurity falls within the category of interstate commerce that Hamilton described as he articulated a nationwide common direction.[153] Save for the smallest businesses that have only a handful of customers in the state where the businesses are based, mid-sized and large companies generally have customers in all or most states. Cybersecurity laws generally apply based on the location of the data subject, regardless of where the company is based.[154] So a ten-employee company in Montana, for instance, could be subject to California's data security laws even if it only had one customer in California. Cybersecurity regulations require companies to spend money to secure data and may restrict how they store, use, and share that data. That is the essence of a commerce regulation, particularly in an era when many businesses' most important assets are the data they hold.

Some critics of federal commercial regulation have argued that the Framers defined "commerce" more narrowly than courts have interpreted it since the New Deal. After reviewing the text of the Constitution, statements at the Constitutional Convention, the *Federalist Papers*, ratification conventions, and other sources, Randy Barnett concluded that Hamilton and others believed that the Framers only intended to provide Congress with the

> power to specify rules to govern the manner by which people may exchange or trade goods from one state to another, to remove obstructions to domestic trade erected by states, and to both regulate and restrict the flow of goods to and from other nations (and the Indian tribes) for the purpose of promoting the domestic economy and foreign trade.[155]

Jack Balkin, in contrast, argues that "commerce" in the eighteenth century more broadly referred to "interaction and exchange between persons or peoples" and that the constitutional authority for Congress to "regulate commerce 'among the several states'" is intended "to give Congress power to legislate in all cases where states are separately incompetent or where the interests of the nation might be undermined by unilateral or conflicting state action."[156]

153. *See supra* Subpart II.A.

154. *See, e.g.*, CAL. CIV. CODE § 1798.140.

155. Randy E. Barnett, *The Original Meaning of the Commerce Clause*, 68 U. CHI. L. REV. 101, 101, 124 (2001) ("From these findings, we can conclude that if anyone in the Constitutional Convention or the state ratification conventions used the term 'commerce' to refer to something more comprehensive than 'trade' or 'exchange,' they either failed to make explicit that meaning or their comments were not recorded for posterity.").

156. Jack M. Balkin, *Commerce*, 109 MICH. L. REV. 1, 5–6 (2010) ("In particular, this approach justifies the constitutionality of federal regulation of labor law, consumer protection law, environmental law, and anti-discrimination

From Chief Justice Marshall's 1824 opinion in *Gibbons v. Ogden*[157] through the twenty-first century,[158] courts continued to apply an expansive view of interstate commerce. But the cybersecurity laws described above would even fall within the scope of Barnett's narrow interpretation of Congress' Commerce Clause power. Cybersecurity is inherently interstate, with the vast majority of businesses storing data on cloud services[159] that have absolutely no connection to their physical location.[160] Personal data stored on these services inherently has value[161] and is at the center of the business models of many companies.[162] Even if the act of securing a system or

law; it even shows why a federal mandate for individuals to purchase health insurance is constitutional.").

157. 22 U.S. 1, 189–90 (1824) ("Commerce, undoubtedly, is traffic, but it is something more: it is intercourse. It describes the commercial intercourse between nations, and parts of nations, in all its branches, and is regulated by prescribing rules for carrying on that intercourse. The mind can scarcely conceive a system for regulating commerce between nations, which shall exclude all laws concerning navigation, which shall be silent on the admission of the vessels of the one nation into the ports of the other, and be confined to prescribing rules for the conduct of individuals, in the actual employment of buying and selling, or of barter.").

158. *See* Nat'l Fed. of Indep. Bus. v. Sebelius, 567 U.S. 519, 536–37 (2012) ("The power over activities that substantially affect interstate commerce can be expansive. That power has been held to authorize federal regulation of such seemingly local matters as a farmer's decision to grow wheat for himself and his livestock, and a loan shark's extortionate collections from a neighborhood butcher shop.").

159. *See* Sharon Florentine, *Cloud Adoption Soars, but Integration Challenges Remain*, IDG COMM., INC. (Jan. 5, 2016, 3:00 AM), https://www.cio.com/article/3018156/cloud-computing/cloud-adoption-soars-but-integration-challenges-remain.html ("The cloud has quickly become a mainstay in IT departments, with recent research from cloud solutions provider RightScale showing 93 percent of businesses using cloud technology in some form or another.").

160. *See* Clive Longbottom, *How to Plan and Manage Datacentre Redundancy*, COMPUTERWEEKLY.COM (Aug. 2013), https://www.computerweekly.com/feature/How-to-plan-and-manage-datacentre-redundancy ("The overall availability of an IT platform means that an approach of a single application on a single physical server with dedicated storage and individual dedicated network connections is a strategy to oblivion. It is incumbent on IT to ensure that the IT platform can continue to operate through failures – as long as the cost of doing so meets the organisation's own cost/risk profile.").

161. *See* Tim Worstall, *Understanding the Economic Value of Your Personal Data*, COMPUTERWEEKLY.COM (May 2017), https://www.computerweekly.com/opinion/Understanding-the-economic-value-of-your-personal-data ("To know that any individual bouncing around Europe, taking an interest not in cat imagery but of posting the local cuisine to friends on their chosen social media – the sort of thing that could be gleaned is not valuable to anyone in the slightest. It is having that sort of information on hundreds of millions of people which has value. Data can then be mined and processed to, for example, inform menu decisions in a recipe book. What's our likely audience for deep-fried chocolate bars? One or two unhealthy Brits? Mediterranean diet it is, then.").

162. *See* Asunción Esteve, *The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA*, 7 INT'L DATA PRIVACY L. 36, 37 (2017).

information is not necessarily performed for a profit motive, cybersecurity laws still are a regulation of commerce because they are integral to the commercial flow of information.[163] Moreover, cybersecurity laws are inherently regulations of *interstate* commerce. Regulating how companies secure and protect this valuable commodity will inevitably regulate how the data flows across state lines.[164]

As described in Part II, Hamilton and Madison urged uniform commercial regulations among the states. In cybersecurity, however, these regulations are not harmonious. For instance, the Massachusetts data breach notification law prohibits a company from informing individuals about the circumstances that caused a data breach,[165] while other states require a description.[166]

Even if the regulations do not directly conflict with one another, they present the onerous burdens that Hamilton and Madison sought to avoid. For example, consider data security laws. Most states have no statutory requirements for data security. About a dozen states require "reasonable" security, as discussed above.[167] Yet Nevada requires encryption of its residents' personal information.[168] That requirement becomes the baseline for most companies nationally, provided that they at least have some customers in Nevada. Moreover, unless the companies can segregate their data handling by state of residence, the Nevada encryption requirement effectively applies to the data of all U.S. residents. Similarly, the detailed Massachusetts requirements for information security programs also become a national standard unless companies are able and willing to separate the data of Massachusetts residents from other data held by the company. Segregating systems by residence of data subjects is impractical and sometimes impossible.[169] Indeed, the most restrictive

163. *See* Edwards v. California, 314 U.S. 160, 172 n.1 (1941) (concluding that a state transportation law is a commerce regulation, and "[i]t is immaterial whether or not the transportation is commercial in character").

164. *See* Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 170 (S.D.N.Y. 1997) ("The Internet is wholly insensitive to geographic distinctions. In almost every case, users of the Internet neither know nor care about the physical location of the Internet resources they access. Internet protocols were designed to ignore rather than document geographic location; while computers on the network do have 'addresses,' they are logical addresses on the network rather than geographic addresses in real space.").

165. MASS. GEN. LAWS ch. 93H § 3(b) (2017).

166. *See* CAL. CIV. CODE § 1798.82(d)(2)(A) (Deering 2018).

167. *See supra* Subpart III.A.

168. *See* NEV. REV. STAT. § 603A.215 (2017) (prohibiting companies from transferring "any personal information through an electronic, nonvoice transmission other than a facsimile to a person outside of the secure system of the data collector unless the data collector uses encryption to ensure the security of electronic transmission").

169. For instance, when the European Union enacted its stringent data protection law, the GDPR, many companies applied the new protections to all customers regardless of their location because of the impossibility of segregating

state privacy and data security laws often become de facto national requirements.[170]

Some defenders of the current system have argued that data security laws are harmonious, as they are centered on the concept of "reasonableness." For instance, William McGeveran recently dismissed complaints about the current scattershot system of data security as "balderdash."[171] McGeveran asserted that "[e]xisting legal materials and private sector guidance about best practices provide data custodians with ample notice about legal responsibilities"[172] and that "public law and the private sector have converged on a clear understanding of the duty of data security owed by companies like Equifax when they store personal data."[173] To support this point, McGeveran pointed to fourteen different sources of data security rules, including state laws and industry standards.[174] Although McGeveran rightly observed that many are grounded in reasonableness and share some common requirements, it also is important to keep in mind that the governing authorities also have significant differences as described in Subpart III.A, such as requirements for multifactor authentication, encryption, and internal policies. A Chief Information Security Officer with a limited budget for technical safeguards and staffing will want some degree of assurance that the investments meet the expectations of regulators; if those regulators are in all fifty states and are applying different standards, it will be difficult for companies to know whether these investments are in line with those regulators' expectations. Moreover, some cybersecurity and data protection laws are

the data. *See How the E.U.'s New Online Privacy Laws Will Affect You*, FUTURITY (Apr. 30, 2018), https://www.futurity.org/general-data-protection-regulation-eu-1744912/ ("[T]he GDPR applies extraterritorially to those companies that process the personal data of any EU resident so the practical effect of the law is to force platforms and Internet companies around the globe to comply with GDPR requirements everywhere. The alternative would be for companies to create two separate systems and infrastructure to separate EU data, which simply isn't practical in an interconnected world.") (quoting Albert Gidari, Dir. of Privacy, Ctr. for Internet & Soc'y at Stanford Law Sch.).

170. *See* Hogan Lovells, *California Continues to Shape Privacy and Data Security Standards*, INT'L ASS'N PRIVACY PROFESSIONALS, (Oct. 1, 2013) https://iapp.org/news/a/california-continues-to-shape-privacy-and-data-security-standards/ ("One out of eight Americans live in California. These factors, and others, make California an important market for online services. And because California's standards are some of the strictest in the U.S., many companies adopt California's standards as part of their baseline standards for privacy and data security rather than adopting state-specific practices. In certain respects, therefore, California laws have set national standards for privacy and data security.").

171. William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1137 (2019).

172. *Id.* at 1140–41.

173. *Id.* at 1137.

174. *Id.* at 1139.

particularly onerous and set a new baseline standard that goes far beyond the expectations of other states or the federal government.

The CCPA is an extreme example of the burdens that a single state can impose on out-of-state businesses without significant operations in that state. The CCPA provides individuals with rights to access, amend, and delete their personal information that are unprecedented in the United States.[175] Many companies will need to entirely revamp their data storage and security to comply with the new law. Moreover, the CCPA creates a new cause of action for lawsuits against companies that have experienced data breaches, providing statutory damages of between $100 to $750 *per victim*, regardless of whether the plaintiffs (or class) suffered any actual damages.[176] The reach of the law goes far beyond California companies. The CCPA applies to any company that collects the personal information of any California resident, provided that it either (1) has annual revenues over $25 million; (2) annually receives or provides the personal information of at least fifty thousand Californians; or (3) receives at least half of its revenues from selling personal information.[177] The statute's definition of "personal information" is quite broad,[178] so a website that automatically logs the IP addresses of visitors—a common practice—could be subject to the onerous requirements if at least fifty-thousand Californians visit it within a year. The International Association of Privacy Professionals estimated that more than five hundred thousand U.S. companies will fall within the CCPA's requirements when it goes into effect in 2020.[179]

One might question if there is any actual harm in allowing a particularly cybersecurity-focused state to set a stringent national standard. As in the Articles of Confederation era, there remains a legitimate concern about the efficacy of state regulations of interstate commerce.[180] Although states have regulated cybersecurity in great

175. CAL. CIV. CODE § 1798.105 (Deering 2018).

176. *Id.* § 1798.150.

177. *Id.* § 1798.140(c)(1).

178. *Id.* § 1798.140(o)(1) (defining "personal information" as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household").

179. Rita Heimes & Sam Pfeifle, *New California Privacy Law to Affect More Than Half a Million US Companies*, INT'L ASS'N PRIVACY PROFESSIONALS (July 2, 2018), https://iapp.org/news/a/new-california-privacy-law-to-affect-more-than-half-a-million-us-companies/ ("The brand-new California Consumer Privacy Act of 2018, which swept through the California legislature last week with startling speed as a compromise measure preempting an even stricter ballot initiative, will apply to more than 500,000 U.S. companies, the vast majority of which are small- to medium-sized enterprises. These figures were derived by an IAPP examination of the language of the law as applied to U.S. census data about American businesses.").

180. *See supra* Subpart II.B.

quantity, the quality has not necessarily been high. By quality, I largely refer to the ability to keep pace with current cybersecurity threats. Consider the data breach notification laws described above.[181] California was the first state to require breach notice in 2003.[182] Most states followed within the next few years,[183] and by 2018, every state and the District of Columbia enacted a breach notice law.[184] The laws vary in requirements, but they are largely based on a framework from the 2003 California breach notice law.[185] The scope, magnitude, and character of cybersecurity threats differ vastly from what they were in 2003, yet states continue to cling to this outdated breach notice structure. Granted, states have modestly amended their breach notice laws in the past decade, but these amendments are not consistent among the states, and they often lag behind technological developments. For instance, every state breach notice law covers disclosure of an individual's name combined with driver's license, social security number, or full financial account information.[186] In the early-aughts as states followed California's lead and passed breach notice laws, these were likely the most critical categories of personal information, as identity theft and financial fraud was a primary concern.[187] However, the amount and character of personal information currently available is vastly different. For instance, no state breach notice law applies to disclosing precise geolocation data, which reveals intimate details and is widely accessible to hackers.[188] Likewise, few states require notification of unauthorized access to biometric data.[189] Although identity theft due to compromise of social security or driver's license numbers remains a significant problem and a legitimate concern, the laws also should account for newer forms of information that the average consumer likely would expect to be protected.

States have not seriously studied whether cybersecurity should focus more on prevention than on post-incident notification. The overall efficacy of state breach notice laws is debatable. A 2016 RAND survey found that eighty-nine percent of respondents continued to patronize a business after receiving a breach notice from it.[190] Rather than requiring companies to notify individuals only after their data

181. *See supra* text accompanying notes 171–73.

182. *See* Kim Zetter, *California Looks to Expand Data Breach Notification Law*, WIRED (Mar. 6, 2009, 6:07 PM), https://www.wired.com/2009/03/ca-looks-to-exp/.

183. *Id.*

184. *See Security Breach Notification Laws*, *supra* note 10.

185. *See* Zetter, *supra* note 182.

186. *See* KOSSEFF, *supra* note 117.

187. *See* Zetter, *supra* note 182.

188. *See* KOSSEFF, *supra* note 117.

189. *Id.*

190. LILLIAN ABLON ET AL., CONSUMER ATTITUDES TOWARD DATA BREACH NOTIFICATIONS AND LOSS OF PERSONAL INFORMATION ix–x (2016), https://www.jstor.org/stable/pdf/10.7249/j.ctt1bz3vwh.5.pdf.

has been stolen, laws should impose effective cybersecurity requirements that reduce the risk of attacks. Yet most states have no cybersecurity requirements.

Even the states that have "cybersecurity" requirements generally focus on protecting the confidentiality of personally identifiable information. This emphasis on "data security" is again a reflection of the early-aughts' concern about identity theft that is the driving force of state data security and breach notification laws. Government officials still should be concerned about identity theft and other harms resulting from compromises in the confidentiality of personal information. However, cybersecurity threats have evolved in the past two decades, and laws should more effectively address them. Breaches of sensitive corporate information—even if such information does not contain personally identifiable information—can lead to trade secret theft, a major economic problem for the United States.[191]

State laws do little to address the integrity and availability prongs of the CIA Triad.[192] Website defacement, for example, is a threat to integrity because an unauthorized person could change information on a website to cause confusion or damage.[193] Imagine, for instance, if a hacker altered the *New York Times* homepage to falsely report an incoming nuclear missile strike in the United States. Even if the newspaper were to quickly correct that story, the initial report likely would spread on social media and cause confusion and panic. Ransomware—in which an attacker encrypts information on a computer or system and refuses to decrypt unless the target pays ransom—is among the top modern cybersecurity challenges.[194] Yet state data security laws focus little on preventing such attacks.

191. Pamela Passman, *Trade Secret Theft: Businesses Need to Beware and Prepare*, FORBES (May 24, 2012, 10:27 AM), https://www.forbes.com/sites/ciocentral/2012/05/24/trade-secret-theft-businesses-need-to-beware-and-prepare/#6763dd891e65.

192. *See* Mike Gault, Opinion, *The CIA Secret to Cybersecurity That No One Seems to Get*, WIRED (Dec. 20, 2015, 7:00 AM), https://www.wired.com/2015/12/the-cia-secret-to-cybersecurity-that-no-one-seems-to-get/ ("The information security community has a model to assess and respond to threats, at least as a starting point. It breaks information security into three essential components: confidentiality, integrity, and availability. . . . Of these, integrity is the least understood and most nebulous. And what many people don't realize is it's the greatest threat to businesses and governments today.").

193. *See* Rashmi K. Verma & Shahzia Sayyad, *Implementation of Web Defacement Detection Technique*, 6 INT'L J. INNOVATIONS ENGINEERING & TECH. 134, 134 (2015) ("Web sites represent the image of a company or organization and these are therefore suffering significant losses due to defacement. Visitors may lose faith in sites that cannot promise security and will become wary of performing online transactions. After defacement, sites have to be shut down for repairs, sometimes for an extended period of time, causing expenses and loss of profit and value.").

194. *See Ransomware*, U.S. DEP'T HOMELAND SECURITY, https://www.us-cert.gov/Ransomware (last visited Mar. 2, 2019).

Just as Hamilton and Madison bemoaned the inefficacy of state commercial regulations under the confederated government, state cybersecurity regulations are lacking. The outdated nature of state cybersecurity laws is not surprising. State legislatures have general jurisdiction over many areas of law, and their staffs typically lack the same depth of expertise as those of Congress. Many state cybersecurity-related laws are administered by state attorneys general offices,[195] which have small staffs that are dedicated to cybersecurity-related issues. At the federal level, even though the FTC has limited enforcement authority, policy is shaped formally or informally by cybersecurity experts from the Department of Homeland Security, the National Institute of Standards and Technology ("NIST"), the National Security Agency, and other cyber-focused departments.[196] These agencies coordinate public-private partnerships, develop industry standards based on cybersecurity threats, and collect real-time intelligence about foreign and domestic cyber threats.[197] It would be unrealistic—and usually impossible—to expect each state to replicate the expertise of these federal agencies. Regulating cybersecurity and data protection at the federal level would enable both legislators and regulators to draw on the expertise of these agencies.

Regulating cybersecurity at the federal level would also allow for faster responses to emerging cybersecurity threats. Ransomware and attacks on cyber-physical systems, for instance, are among the top current cybersecurity concerns, but identity theft and fraud were more prominent until a few years ago. Modernizing legislation in Congress via amendments is difficult, as seen by its failure to pass a comprehensive cybersecurity regulatory bill.[198] However, modernizing state laws is even more difficult. Some state legislatures meet only every other year, causing even further delays. While some states may eventually update their cybersecurity laws to reduce the likelihood of modern threats, others simply would be unable to do so. The result would be the patchwork of laws that we currently see with breach notification.

Hamilton and Madison also argued that state-centric commercial regulation causes more difficulty in trade relations with other countries.[199] The same is true for cybersecurity and data protection, along with related privacy laws. For instance, the European Union's GDPR restricts the transfer of Europeans' personal information to another country or international organization unless the European

195. *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 748 (2016).

196. *See* KOSSEFF, *supra* note 117, at 243–58 (providing an overview of federal agencies' roles in cybersecurity).

197. *Id.*

198. Newman, *supra* note 6.

199. *See supra* Subpart II.B.

Commission "has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection."[200] The United States is not among the nations that Europe considers to offer "adequate" data protection, so U.S. companies must sign contracts or participate in programs before receiving Europeans' data.[201] Months before California passed the CCPA, some privacy experts suggested that California was seeking to obtain an adequacy decision from the European Commission by adopting stronger security and data protection regulations than the rest of the United States.[202]

While an adequacy decision might appear to benefit California, it is unclear how it would work in practice. There would be no barriers to transferring personal data between a company in Europe and a company in California. But that company could not transfer the data to its offices in any other states, unless those states also received an adequacy decision from the European Commission. This would create the uneven foreign trade advantages among states that Hamilton and Madison bemoaned. A federal data security and data protection regime would prevent such barriers among the states. If Congress determined that adequacy was a valid policy choice, it would pass legislation that requires adequate security and data protection across all fifty states. This would also allow the federal executive branch to negotiate particular terms of adequacy with the European Commission, rather than leaving such foreign affairs to individual state governors and attorneys general.

200. General Data Protection Regulation, *supra* note 89, at 61.

201. *Adequacy Decisions: How the EU Determines if a Non-EU Country Has an Adequate Level of Data Protection*, EUROPEAN COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en (last visited Mar. 2, 2019) (reporting that the European Union only recognizes the United States as providing limited "adequate protection" as to the Privacy Shield framework).

202. *See* Jason Peterson & Lydia de la Torre, *Is California on its Way to Going for 'Adequacy?'*, INT'L ASS'N PRIVACY PROFESSIONALS (Apr. 6, 2018), https://iapp.org/news/a/is-california-on-its-way-to-going-for-adequacy/ ("A U.S. state, for example California, could take advantage of this possibility and obtain adequacy determination from the European Commission even though the U.S. as a whole does not have an adequacy determination (the EU-U.S. Privacy Shield Framework provides a method for organizations to transfer data from the EU to the United States but only covers those entities that self-certify and remain compliant with the framework). A California adequacy decision could allow California-based organizations to transfer data from the EU without a need to be Privacy Shield certified, or use other appropriate safeguards (such as standard contractual clauses, or binding corporate rules).").

C. Federal Cybersecurity Law Would Establish Uniform National Policy

Congress could align U.S. cybersecurity laws with the Hamiltonian vision by passing a comprehensive data security and incident notification statute that applies across industries. The statute could expressly preempt state laws and therefore set a national standard.[203]

That is easier said than done. For more than a decade, members of Congress have introduced many bills that would have preempted state notice and security laws and established a national standard.[204] And in 2015, the Obama White House proposed a national breach notification and security bill.[205] Many such proposals have received hearings, but none became law.

In 2018, Representatives Blaine Luetkemeyer and Carolyn Maloney circulated a twenty-four-page draft bipartisan bill, the Data Acquisition and Technology Accountability and Security Act.[206] The bill requires companies to implement data security safeguards "that are reasonably designed to protect the security and confidentiality of personal information from unauthorized acquisition that is reasonably likely to result in identity theft, fraud, or economic loss."[207] Although the bill provides for some flexibility in safeguards, it requires certain elements such as employee training, risk assessment, and regular evaluations of threats.[208] The bill also establishes requirements for notifying federal law enforcement, credit bureaus, and individuals, depending on the size and potential harm of the breach.[209] The bill allows enforcement by the FTC and state attorneys general, though states may not sue if the FTC has already brought a civil action arising from the same breach.[210]

The bill broadly "preempts any law, rule, regulation, requirement, standard, or other provision having the force and effect of law of any State, or political subdivision of a State, with respect to securing information from unauthorized access or acquisition, including notification of unauthorized access or acquisition of

203. *See* Arizona v. United States, 567 U.S. 387, 399 (2012) ("There is no doubt that Congress may withdraw specified powers from the States by enacting a statute containing an express preemption provision.").

204. *See* Newman, *supra* note 6, at 446–52 (summarizing bills from the 113th Congress).

205. *See* Grant Gross, *Obama Calls for Data Breach Notification Law, Privacy Bill of Rights*, COMPUTERWORLD (Jan. 12, 2015, 11:08 AM), https://www.computerworld.com/article/2867839/obama-calls-for-data-breach-notification-law-privacy-bill-of-rights.html.

206. Data Acquisition and Technology Accountability and Security Act, H.R. ___, 115th Cong. (Discussion Draft, Feb. 16, 2018), https://financialservices.house.gov/uploadedfiles/03.07.2018_data_s_bill.pdf.

207. *Id.* § 3(a)(1).

208. *Id.* § 3(a)(3)(B)–(C).

209. *Id.* § 4(b)(1).

210. *Id.* § 5(a)–(b).

data."[211] This express preemption would establish a uniform data security and breach notice policy for every state, rather than subjecting companies to fifty-one different standards (for the fifty states and the District of Columbia).

Not everyone saw it that way. At a March 2018 House hearing on the bill, Sara Cable of the Massachusetts Attorney General's Office argued that the preemption provision would "expose American consumers to increased risks as a result of a new, less stringent national standard."[212] Later in March, thirty-two state attorneys general wrote a letter to Congress in which they argued that states "have proven themselves to be active, agile, and experienced enforcers of their consumers' data security and privacy."[213] Marc Rotenberg, the executive director of the Electronic Privacy Information Center, a privacy advocacy group, testified in February 2018 that federal breach notice and security bills "should be modified to establish a federal baseline and allow states to regulate upwards, providing more protection than federal law if their legislatures so decide."[214]

If critics of federal cybersecurity bills identify weaknesses in their protections, Congress could address those shortcomings and strengthen the protections. Yet the critics have identified no principle that would support state-by-state regulation of cybersecurity, which as described above is an inherently interstate endeavor.[215] But the continued opposition by states and consumer groups calls into question whether Congress can ever establish a uniform national policy on cybersecurity regulation.

To address some of the opposition from consumer groups, Congress should consider strong and specific cybersecurity

211. *Id.* § 6.

212. *Legislative Proposals to Reform the Current Data Security and Breach Notification Regulatory Regime: Hearing on H.R. 4028 and H.R. ___Before the Subcomm. on Fin. Insts. & Consumer Credit of the H. Comm. on Fin. Servs.*, 115th Cong. (2018) (prepared statement of Sara Cable, Assistant Att'y Gen. and Director, Data Privacy & Security, Consumer Protection Division, Office of the Massachusetts Attorney General) ("Now is not the time to dilute or preempt the tools regularly and successfully used by many states, including Massachusetts, to combat this crisis. Especially in light of breaches like Equifax, this is the time to build on and improve existing protections under federal and state law."), https://financialservices.house.gov/uploadedfiles/03.07.2018_fi_sara_cable_testimony.pdf.

213. Letter from Lisa Madigan, Ill. Attorney Gen., to Comm. Leaders, House Comm. on Fin. Servs. & House Subcomm. on Fin. Insts. & Consumer Credit (Mar. 19, 2018), http://www.illinoisattorneygeneral.gov/pressroom/2018_03/Committee_Leaders_letter.pdf.

214. *Examining the Current Data Security and Breach Notification Regulatory Regime: Hearing Before the Subcomm. on Fin. Insts. & Consumer Credit of the H. Comm. on Fin. Servs.*, 115th Cong. (2018) (prepared statement of Marc Rotenberg, President, Electronic Privacy Information Center), https://financialservices.house.gov/uploadedfiles/02.14.2018_marc_rotenberg_testimony.pdf.

215. *See supra* text accompanying notes 159–60.

regulations, such as breach notification requirements and specific safeguards that expert agencies, including NIST, believe are most effective at deterring modern threats. The Hamiltonian concerns about regulations do not arise from them being too onerous; the objections relate to the ability of a single state to regulate out-of-state commerce. Concrete and specific requirements at the federal level would be a vast improvement over the state-by-state approach that the United States applies to cybersecurity regulation.

A federal cybersecurity law would not be a panacea to U.S. companies that seek uniform regulations. If the companies process data of people located outside of the United States, they may be subject to even more burdensome laws of other countries, such as the European Union's GDPR. But some companies have already responded to particularly difficult cybersecurity and data protection laws by discontinuing business operations in those countries.[216] That is precisely the sort of corporate environment that Congress should avoid within the United States. An Oregon company, for instance, should not feel compelled to block its website from California residents because the company fears monstrous penalties under the CCPA. That is directly contrary to the unencumbered commerce envisioned by Madison and Hamilton.

IV. DORMANT COMMERCE CLAUSE AND STATE CYBERSECURITY LAWS

Even without congressional action, courts may eventually strike down state regulations of cybersecurity as unconstitutional under the Dormant Commerce Clause. Although few courts have directly addressed whether the Dormant Commerce Clause invalidates state cybersecurity and data protection regulations, the increasing burdens of these laws, combined with the varying approaches, raise legitimate questions about their constitutionality.

The Framers recognized that a centralized commercial regulatory system would, sometimes, prohibit state regulations. In *Federalist No. 32*, Hamilton wrote that the "exclusive delegation" of federal power and "alienation of State sovereignty," could

> only exist in three cases[:] [1] where the Constitution in express terms granted an exclusive authority to the Union; [2] where it granted in one instance an authority to the Union; and in another prohibited the States from exercising the like authority;

216. *See, e.g.*, Matt Novak, *Dozens of American News Sites Blocked in Europe as GDPR Goes Into Effect Today*, GIZMODO (May 25, 2018, 7:00 AM), https://gizmodo.com/dozens-of-american-news-sites-blocked-in-europe-as-gdpr-1826319542 ("The European Union's digital privacy law, known as the General Data Protection Regulation (GDPR), officially went into effect today. But some websites in the U.S. have decided to block their services entirely rather than adhere to the new regulations. Dozens of American newspapers are currently blocked in Europe and web services like Instapaper have suspended operations in the European Union for the foreseeable future.").

> and [3] where it granted an authority to the Union, to which a similar authority in the States would be absolutely and totally *contradictory* and *repugnant*.[217]

The Dormant Commerce Clause exists in the third prong of Hamilton's framework. For many of the same reasons that state cybersecurity laws fall short of the Framers' vision for federal commercial regulation, as described in Part III, they also may violate the Dormant Commerce Clause.

The Supreme Court and lower courts slowly articulated the boundaries for this Dormant Commerce Clause (also known as the "negative" Commerce Clause), to implement the Framers' vision of a centralized regulatory state.[218] In the 1824 case, *Gibbons v. Ogden*, the Supreme Court held that a federal law regulating navigation took priority over a conflicting New York law.[219] Chief Justice Marshall's majority opinion did not explicitly prohibit states from regulating any interstate commerce,[220] though Justice Johnson stated in a concurrence that the federal government has *exclusive* power of interstate commerce regulation.[221]

As Congress and state legislatures increased their regulatory efforts, the Supreme Court was forced to directly address the scope of constitutional limits on state commercial laws. Without using the phrase "dormant commerce clause," Justice Cardozo in 1935 struck down New York's imposition of minimum prices for milk imported from other states.[222] The Constitution, he wrote, "was framed upon the theory that the peoples of the several states must sink or swim together, and that in the long run prosperity and salvation are in union and not division."[223] In 1979, Justice Brennan observed that the Constitution was drafted to avoid "the tendencies toward economic Balkanization that had plagued relations among the

217. ALEXANDER HAMILTON, *The Federalist No. 32*, *in* ALEXANDER HAMILTON: WRITINGS, *supra* note 69, at 301, 301–02.

218. *See* Quill Corp. v. North Dakota, 504 U.S. 298, 312 (1992) ("Under the Articles of Confederation, state taxes and duties hindered and suppressed interstate commerce; the Framers intended the Commerce Clause as a cure for these structural ills. . . . It is in this light that we have interpreted the negative implication of the Commerce Clause. Accordingly, we have ruled that that Clause prohibits discrimination against interstate commerce . . . and bars state regulations that unduly burden interstate commerce . . . .").

219. Gibbons v. Ogden, 22 U.S. 1, 18 (1824).

220. *Id.* at 210.

221. *Id.* at 227 (Johnson, J., concurring) ("The power of a sovereign state over commerce, therefore, amounts to nothing more than a power to limit and restrain it at pleasure. And since the power to prescribe the limits to its freedom, necessarily implies the power to determine what shall remain unrestrained, it follows, that the power must be exclusive; it can reside but in one potentate; and hence, the grant of this power carries with it the whole subject, leaving nothing for the State to act upon.").

222. Baldwin v. G. A. F. Seelig, Inc., 294 U.S. 511, 527 (1935).

223. *Id.* at 523.

Colonies and later among the States under the Articles of Confederation," and therefore the Commerce Clause is not merely "an authorization for congressional action, but also, even in the absence of a conflicting federal statute," it is "a restriction on permissible state regulation."[224] Although some scholars argue that neither the text nor history of the Commerce Clause supports a "dormant" or "negative" reading that limits states,[225] the courts have disagreed.

The Dormant Commerce Clause does not prohibit *all* state litigation, statutes, and regulations that affect interstate commerce. Over the years, courts have been somewhat opaque as to precisely what types of state laws violate the Dormant Commerce Clause. Generally, the Dormant Commerce Clause restricts four types of state laws: (1) those that discriminate against out-of-state businesses;[226] (2) those that regulate conduct that occur outside of the state;[227] (3) nondiscriminatory regulations that excessively burden interstate commerce relative to the benefits that they confer;[228] and (4) inconsistent regulations across multiple states.[229]

For state cybersecurity regulations, the second, third, and fourth types are more likely to apply, as cybersecurity laws do not typically impose different duties on out-of-state companies.[230] Therefore, state

224. Hughes v. Oklahoma, 441 U.S. 322, 325–26 (1979).

225. *See, e.g.*, Martin H. Redish & Shane V. Nugent, *The Dormant Commerce Clause and the Constitutional Balance of Federalism*, 1987 DUKE L.J. 569, 571 (1987) ("With limited exceptions, the recent literature expends relatively little effort attempting either to find the textual source or to prove the legitimacy of the dormant commerce clause. Our position is that no such legitimate constitutional source exists: the simple fact is that there is no dormant commerce clause to be found within the text or textual structure of the Constitution.").

226. *See, e.g.*, Maryland v. Louisiana, 451 U.S. 725, 756 (1981) (invalidating a Louisiana natural gas tax on Dormant Commerce Clause grounds because it "unquestionably discriminates against interstate commerce in favor of local interests as the necessary result of various tax credits and exclusions"); Bos. Stock Exch. v. State Tax Comm'n, 429 U.S. 318, 331 (1977) (striking down a New York law that imposed a higher tax on out-of-state stock transfers because the "obvious effect of the tax is to extend a financial advantage to sales on the New York exchanges at the expense of the regional exchanges").

227. Healy v. Beer Inst., 491 U.S. 324, 336 (1989); Edgar v. MITE Corp., 457 U.S. 624, 642–43 (1982) (plurality opinion) ("The Commerce Clause also precludes the application of a state statute to commerce that takes place wholly outside of the State's borders, whether or not the commerce has effects within the State.").

228. *See* Pike v. Bruce Church, 397 U.S. 137, 142 (1970) ("Where the statute regulates even-handedly to effectuate a legitimate local public interest, and its effects on interstate commerce are only incidental, it will be upheld unless the burden imposed on such commerce is clearly excessive in relation to the putative local benefits.").

229. CTS Corp. v. Dynamics Corp. of Am., 481 U.S. 69, 88 (1987) ("This Court's recent Commerce Clause cases also have invalidated statutes that may adversely affect interstate commerce by subjecting activities to inconsistent regulations.").

230. *See* Citron, *supra* note 195, at 805 ("[B]reach notification laws would not violate the anti-discrimination principle.").

cybersecurity regulations are likely to face Dormant Commerce Clause challenges if they regulate activities entirely outside of the state, unduly burden interstate commerce, or impose inconsistent regulations.

Few written court opinions have ever considered the applicability of the Dormant Commerce Clause to cybersecurity laws. In 2014, the United States District Court for the District of Minnesota concluded that the Dormant Commerce Clause did not shield Target from a lawsuit arising under a Minnesota state law that required prompt disposal of credit card information because "it applies equally to the Minnesota companies' data retention practices with respect to in-state and out-of-state transactions."[231] However, that brief dismissal of the argument appeared to address whether the Minnesota law discriminated between in-state and out-of-state businesses, which was not the argument that Target had raised. Instead, Target had argued that the Minnesota law was unlawfully extraterritorial, though it only made the argument in a footnote to its motion to dismiss.[232] Because the case settled before either party had a chance to appeal, there was not a more thorough ruling on the applicability of the Dormant Commerce Clause to the statute.

Due to the lack of on-point caselaw, we must apply Dormant Commerce Clause precedent from other areas to state cybersecurity and data protection laws. The rest of Part IV examines Dormant Commerce Clause cases that apply to somewhat similar legal frameworks and analyzes how each of the three relevant strands of Dormant Commerce Clause caselaw might apply to state cybersecurity regulations.

A. Extraterritoriality

The "extraterritoriality" Dormant Commerce Clause cases are perhaps the most likely obstacles for state cybersecurity laws, though the law outlining the contours of this doctrine is not entirely clear. Under the extraterritoriality prong, a state regulation could violate the Dormant Commerce Clause if it regulates entirely extraterritorial behavior. This line of cases is less developed than the burdensome balancing test or nondiscrimination Dormant Commerce Clause cases, so there is uncertainty as to precisely how a court might apply the extraterritoriality Dormant Commerce Clause test.

The leading Supreme Court case to apply the extraterritoriality test is *Healy v. Beer Institute*,[233] a 1989 challenge to a Connecticut

231. *In re* Target Corp. Customer Data Sec. Breach Litig., 64 F. Supp. 3d 1304, 1313 (D. Minn. 2014).

232. Defendant's Memorandum of Law in Support of Motion to Dismiss the Consolidated Class Action Complaint at 30, n. 11, *In re* Target Corp. Customer Data Sec. Breach Litig., 64 F. Supp. 3d 1304 (D. Minn. 2014), MDL No. 14-2522 (PAM/JJK) (Sept. 2, 2014).

233. 491 U.S. 324 (1989).

statute that required beer suppliers to affirm that they did not ship beer into Connecticut at prices higher than those they charged to wholesalers in other states.[234] The Supreme Court concluded that this law violated the extraterritoriality test of the Dormant Commerce Clause.[235] Justice Blackmun wrote for the majority that a state law "that directly controls commerce occurring wholly outside the boundaries of a State exceeds the inherent limits of the enacting State's authority and is invalid regardless of whether the statute's extraterritorial reach was intended by the legislature."[236] The Court's job, Blackmun wrote, is to determine "whether the practical effect of the regulation is to control conduct beyond the boundaries of the State."[237] Courts should evaluate the impact of the state law, he wrote, "not only by considering the consequences of the statute itself, but also by considering how the challenged statute may interact with the legitimate regulatory regimes of other States and what effect would arise if not one, but many or every, State adopted similar legislation."[238]

Applying that extraterritoriality test, Blackmun concluded that the Connecticut law violated the Dormant Commerce Clause. The statute, he wrote, "has the undeniable effect of controlling commercial activity occurring wholly outside the boundary of the State."[239] When viewed in light of the many other state laws regarding beer pricing, Blackmun wrote, the Connecticut law would "create just the kind of competing and interlocking local economic regulation that the Commerce Clause was meant to preclude."[240] Applying this extraterritoriality doctrine, courts have invalidated a California law that required art dealers to pay a specified royalty to artists[241] and an Indiana law that mandated licensing of out-of-state lenders who do business with Indiana residents.[242]

234. *Id.* at 326.
235. *Id.* at 343.
236. *Id.* at 336.
237. *Id.*
238. *Id.*
239. *Id.* at 337.
240. *Id.*
241. Sam Francis Found. v. Christies, Inc., 784 F.3d 1320, 1323 (9th Cir. 2015) (en banc) ("For example, if a California resident has a part-time apartment in New York, buys a sculpture in New York from a North Dakota artist to furnish her apartment, and later sells the sculpture to a friend in New York, the Act requires the payment of a royalty to the North Dakota artist—even if the sculpture, the artist, and the buyer never traveled to, or had any connection with, California. We easily conclude that the royalty requirement, as applied to out-of-state sales by California residents, violates the dormant Commerce Clause.").
242. Midwest Title Loans, Inc. v. Mills, 593 F.3d 660, 667–68 (7th Cir. 2010) ("Suppose Illinois thinks title loans a good thing (and there is, as we pointed out earlier, some basis for that belief)—or at least, as the absence of an Illinois counterpart to the Indiana law makes clear, thinks they shouldn't be restricted in the way that Indiana thinks they should be. To allow Indiana to apply its law

The Supreme Court has imposed some limits on the extraterritoriality branch of the Dormant Commerce Clause. In a 2003 case, *Pharmaceutical Research & Manufacturers of America v. Walsh*,[243] the Court refused to invalidate a Maine law that required drug manufacturers to provide rebates for sales to low-income Maine residents.[244] Even though the drug manufacturers were located outside of Maine, the Supreme Court refused to strike down the law under the extraterritoriality doctrine.[245] Justice Stevens reasoned that the Maine law did not "regulate the price of any out-of-state transaction, either by its express terms or by its inevitable effect," nor did it "insist that manufacturers sell their drugs to a wholesaler for a certain price."[246] Therefore, he concluded, the *Healy* extraterritoriality doctrine did not apply.[247] And in some circuits, recent court opinions have limited the scope of the extraterritoriality doctrine. For instance, in a 2015 opinion by the United States Court of Appeals for the Tenth Circuit, then-Judge Gorsuch rejected a Dormant Commerce Clause challenge to a Colorado law that required at least twenty percent of electricity sold to Colorado residents to come from renewable sources.[248] Striking the law merely because it affects out-of-state companies, then-Judge Gorsuch wrote, would require the invalidation of a wide range of manufacturing and labeling safety regulations.[249] Then-Judge Gorsuch wrote that such an expansive invalidation of state regulations would not be supported by Supreme Court precedent.[250] He asserted that the *Healy* line of cases are limited to cases involving: "(1) a price control or price affirmation regulation, (2) linking in-state prices to those charged elsewhere, with (3) the effect of raising costs for out-of-state consumers or rival businesses."[251] Justice Gorsuch's position, however, represents the most limited view of the extraterritoriality doctrine, and one not shared by other circuits. The next year, the United States Court of Appeals for the Eighth Circuit rejected his interpretation, observing that "the Supreme Court has never so limited the doctrine, and indeed has applied it more broadly."[252]

against title loans when its residents transact in a different state that has a different law would be arbitrarily to exalt the public policy of one state over that of another.")

243. 538 U.S. 644 (2003).

244. *Id.* at 649, 670.

245. *Id.* at 669.

246. *Id.* (quoting Pharm. Research & Mfrs. of Am. v. Concannon, 249 F.3d 66, 81–82 (1st Cir. 2001)).

247. *Id.*

248. Energy & Env't Legal Inst. v. Epel, 793 F. 3d 1169, 1170–71 (10th Cir. 2015).

249. *Id.* at 1175.

250. *Id.*

251. *Id.* at 1173.

252. North Dakota v. Heydinger, 825 F.3d 912, 920 (8th Cir. 2016).

Reviewing the strand of extraterritoriality cases, Brannon Denning concluded that after *Walsh*, "the extraterritoriality principle looks to be quite moribund."[253] Still, Denning's assessment of the post-*Walsh* doctrine was more robust than Justice Gorsuch's. Denning concluded that the extraterritoriality doctrine survived in three areas: (1) linking prices between states; (2) "where it is clear that a statute seeks to enable State A to control activities occurring in State B, or . . . where State A is 'projecting' its legislation into State B"; and (3) "in certain cases dealing with early state regulation of the Internet."[254]

Even under the more limited, post-*Walsh* extraterritoriality framework, cybersecurity regulations may well fall within this strand of the Dormant Commerce Clause. For instance, in a 2017 case, *Legato Vapors, LLC v. Cook*,[255] the United States Court of Appeals for the Seventh Circuit concluded that, because of extraterritoriality concerns, an Indiana law that imposed stringent regulations on the manufacturing of liquid used in e-vapor cigarette-like devices was unenforceable against non-Indiana manufacturers of the devices.[256] For instance, the Indiana law required that manufacturers—even those located out of state—"take reasonable steps to ensure that all ingredients used in the production of e-liquid are stored in a secure area accessible only by authorized personnel."[257] Such security requirements "amount to direct and unconstitutional extraterritorial regulation of out-of-state e-liquid manufacturers' production facilities and their purchases of services in their home states," the Seventh Circuit concluded.[258]

Although state cybersecurity laws regulate a different subject matter than the Indiana statute, they have a similar reach. The Seventh Circuit found that the Dormant Commerce Clause violation occurred due to the onerous regulations that Indiana imposed on manufacturing that occurred entirely out of state. Likewise, state cybersecurity and data protection laws subject out-of-state companies to requirements for storing, transmitting, processing, and controlling access to personal information. As described in Subpart III.A, state laws that require specific cybersecurity safeguards apply based on the location of the data subject. For instance, consider a Los Angeles-based e-commerce company whose servers are in Los Angeles, Salt Lake City, and Chicago. All of its employees are in those three cities. If that company has even just one customer in Massachusetts, it must comply with Massachusetts' data security

253. Brannon P. Denning, *Extraterritoriality and the Dormant Commerce Clause: A Doctrinal Post-Mortem*, 73 LA. L. REV. 979, 979 (2013).
254. *Id.* at 992–93.
255. 847 F.3d 825 (7th Cir. 2017).
256. *Id.* at 827.
257. *Id.* at 832.
258. *Id.* at 834.

regulations, including the requirements for more than a dozen different internal security policies and encryption of data.[259] If the company happens to be a bank, insurance broker, or other financial company that is regulated by the state of New York, it must comply with New York's particularly detailed requirements, even if it does not have a single employee or contractor in New York.[260] These state laws require out-of-state companies to make significant investments and procedural changes in operations that occur entirely outside of the state that enacted the requirements.

The Dormant Commerce Clause's applicability to cybersecurity laws is supported by some courts' conclusions that certain state regulations of the Internet are impermissibly extraterritorial. This approach originated in a 1997 case, *American Libraries Ass'n v. Pataki*,[261] in which the United States District Court for the Southern District of New York invalidated a New York law that criminalized the following act:

> Knowing the character and content of the communication which, in whole or in part, depicts actual or simulated nudity, sexual conduct or sado-masochistic abuse, and which is harmful to minors, [to] intentionally use[ ] any computer communication system allowing the input, output, examination or transfer, of computer data or computer programs from one computer to another, to initiate or engage in such communication with a person who is a minor.[262]

Artists, booksellers, and others who sell content online objected to this law as an unconstitutional burden on their out-of-state activities. For instance, Oren Teicher, president of the American Booksellers Foundation for Free Expression ("ABFFE"), testified:

> [B]ooksellers conduct business over the Internet in a variety of ways. If the Act is not enjoined and ABFFE members are forced to self-censor rather than be subject to criminal liability, they will suffer immeasurable injury because they will lose significant sales and goodwill generated by their use of the Internet with respect to both censored and noncensored materials and resources. If a bookstore must self-censor certain books, it loses the profits from the sale of those particular books generated from the books' listing on the booksellers' Web sites. In addition, the bookstore will lose even more business because it will appear that the bookstore has an incomplete or inadequate listing of books in its inventory and Internet users will choose to buy their books elsewhere.[263]

259. *See supra* text accompanying notes 129–30.
260. *See supra* text accompanying notes 132–40.
261. 969 F. Supp. 160 (S.D.N.Y. 1997).
262. *Id.* at 163 (quoting amendment to N.Y. PENAL LAW § 235.21)
263. *Id.* at 174–75.

Relying on this testimony and other evidence, the district court concluded that it is "impossible to restrict the effects of the New York Act to conduct occurring within New York" due to the design of the Internet.[264] "An Internet user may not intend that a message be accessible to New Yorkers, but lacks the ability to prevent New Yorkers from visiting a particular Website or viewing a particular newsgroup posting or receiving a particular mail exploder," Judge Loretta Preska wrote.[265] "Thus, conduct that may be legal in the state in which the user acts can subject the user to prosecution in New York and thus subordinate the user's home state's policy—perhaps favoring freedom of expression over a more protective stance—to New York's local concerns," Judge Preska concluded.[266] The New York law is a per se violation of the Dormant Commerce Clause, she wrote, because "New York has deliberately imposed its legislation on the Internet and, by doing so, projected its law into other states whose citizens use the Net."[267] In her discussion of inconsistent regulations later in the opinion, Judge Preska applied a truly Hamiltonian approach to Internet regulation, writing that "the Internet is one of those areas of commerce that must be marked off as a national preserve to protect users from inconsistent legislation that, taken to its most extreme, could paralyze development of the Internet altogether."[268] Judge Preska emphasized the need for national uniformity in regulation of the Internet:

> The courts have long recognized that certain types of commerce demand consistent treatment and are therefore susceptible to regulation only on a national level. The Internet represents one of those areas; effective regulation will require national, and more likely global, cooperation. Regulation by any single state can only result in chaos, because at least some states will likely enact laws subjecting Internet users to conflicting obligations.[269]

Judge Preska's opinion immediately attracted attention and criticism. In an essay published in 2001, Jack Goldsmith and Alan Sykes argued that Judge Preska effectively made it impossible for states to impose any laws affecting the Internet.[270] Goldsmith and

264. *Id.* at 177.
265. *Id.*
266. *Id.*
267. *Id.*
268. *Id.* at 169.
269. *Id.* at 181.
270. *See* Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 YALE L.J. 785, 787 (2001) ("The decided cases have mostly involved pornography regulations and antispam statutes. But the logic of *American Libraries Ass'n* and the cases that follow its reasoning extends to state antigambling laws, computer crime laws, various consumer protection laws, libel laws, licensing laws, and many more.").

Sykes focused on Judge Preska's observation that the case did not involve New York's regulation of *obscene* online content.[271] "While the prohibitions differ in substance, as applied to the Internet their extraterritorial effects are identical: Both regulations affect the pricing decisions of Web content providers in other states, and this influence on price may affect consumers in permissive jurisdictions outside of New York," they wrote.[272] "Such differential treatment suggests that the court's extraterritoriality reasoning may be flawed," they concluded.[273]

Goldsmith and Sykes argued that Judge Preska—and other judges who quickly adopted her reasoning in other Internet-related Dormant Commerce Clause cases—overextended the extraterritoriality doctrine to invalidate state laws. The proper question, Goldsmith and Sykes argued, "is not whether they produce out-of-state costs, but rather whether they are properly calibrated to redress local harms."[274]

Yet even after Goldsmith and Sykes published this widely cited essay—and after the 2003 *Walsh* opinion—courts continued to find a wide range of Internet-related laws invalid if they regulated wholly out-of-state conduct.[275] In 2003, the United States Court of Appeals for the Second Circuit invalidated a Vermont law that prohibited the online distribution of material that is "harmful to minors," concluding that "internet regulation of the sort at issue here still runs afoul of the dormant Commerce Clause because the Clause 'protects against inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another State.'"[276] Two years later, the United States Court of Appeals for the Fourth Circuit affirmed the striking down of a Virginia law restricting online material that is harmful to minors, applying similar reasoning.[277]

271. *Id.* at 822.
272. *Id.*
273. *Id.* at 822–23.
274. *Id.* at 827.
275. *See* Denning, *supra* note 253, at 992.
276. Am. Booksellers Found. v. Dean, 342 F. 3d 96, 103–04 (2d Cir. 2003) (quoting Healy v. Beer Inst., Inc., 491 U.S. 324, 337 (1989)) ("A person outside Vermont who posts information on a website or on an electronic discussion group cannot prevent people in Vermont from accessing the material. If someone in Connecticut posts material for the intended benefit of other people in Connecticut, that person must assume that someone from Vermont may also view the material. This means that those outside Vermont must comply with [the Vermont statute] or risk prosecution by Vermont. Vermont has 'project[ed]' [the statute] onto the rest of the nation.").
277. PSINet, Inc. v. Chapman, 362 F.3d 227, 240 (4th Cir. 2004) ("The content of the Internet is analogous to the content of the night sky. One state simply cannot block a constellation from the view of its own citizens without blocking or affecting the view of the citizens of other states. Unlike sexually explicit materials disseminated in brick and mortar space, electronic materials are not distributed piecemeal."); *see also* Se. Booksellers Ass'n v. McMaster, 371 F. Supp. 2d 773, 787 (D.S.C. 2005) ("[T]he Act is invalid because it places an undue burden

Just as a state should not impose regulations on out-of-state companies merely because some online customers reside in the state, a state should not be able to regulate the details of a company's cybersecurity program merely because the company stores or processes the data of some customers who live in the state. There is an even greater case to be made for prohibiting states' extraterritorial cybersecurity regulations than there is for the regulations of Internet decency in *American Libraries Ass'n* and its progeny. In those cases, the act typically regulated by State A is the transmission of certain online content to customers located in State A. In the standard cybersecurity context, however, even that tenuous link is not present. Cybersecurity laws regulate the storage, handling, and further transfer of data once it is no longer located in State A. Such laws are even more extraterritorial in scope because their only link to the regulating state is the residency of the data subjects.

As explained in Subpart III.A, there are several reasonable approaches to regulating cybersecurity, such as requiring encryption or particular authentication procedures. Under the *Healy* line of cases, it likely is unconstitutional for a single state to determine how out-of-state companies should approach cybersecurity merely because they have some customers in that state. Accordingly, the strongest Dormant Commerce Clause challenge to state cybersecurity laws likely would emerge from the extraterritoriality precedent. Though the emerging circuit split on the scope of the extraterritoriality rule leaves open the possibility that a court would not strike a state cybersecurity law under this precedent. However, for the reasons articulated in Part III, the Seventh Circuit's more expansive prohibition on state regulation of extraterritorial business activities follows the Framers' vision of commercial regulation.

B. Excessive Burden

Although the *Healy* extraterritoriality doctrine is the most likely basis for a Dormant Commerce Clause challenge to state cybersecurity statutes, the laws also could face a challenge under a separate line of Dormant Commerce Clause cases that prohibits state regulation that excessively burdens interstate commerce.

The Supreme Court articulated the "excessive burden" analytical framework in 1970, in *Pike v. Bruce Church*.[278] In this case, an Arizona produce company challenged an Arizona state law that required most cantaloupes grown in Arizona to "be packed in regular compact arrangement in closed standard containers approved by the

on interstate commerce by regulating commerce occurring wholly outside of South Carolina."); Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606, 663 (E.D. Pa. 2004) ("A number of courts have concluded that the Internet should not be subject to state regulation.").

278. 397 U.S. 137, 142 (1970).

supervisor."[279] Arizona had used this law to prevent the company from shipping its cantaloupes to California for packing.[280] The company's costly packing and processing facility was thirty-one miles away from its Arizona operation, across the border in California.[281] Arizona claimed the statue was necessary to "promote and preserve the reputation of Arizona growers by prohibiting deceptive packaging."[282] The company challenged the Arizona law as violating the Dormant Commerce Clause, arguing it placed an excessive burden on interstate commerce.[283]

Writing for a unanimous Court, Justice Stewart agreed with the company. To determine whether a state law places an excessive burden on interstate commerce, the Court considers "the nature of the local interest involved, and . . . whether it could be promoted as well with a lesser impact on interstate activities," wrote Justice Stewart.[284] Applying this test, Justice Stewart concluded that Arizona placed a "straightjacket" on the company's operations without demonstrating a compelling justification for the requirement:

> Such an incidental consequence of a regulatory scheme could perhaps be tolerated if a more compelling state interest were involved. But here the State's interest is minimal at best—certainly less substantial than a State's interest in securing employment for its people. If the Commerce Clause forbids a State to require work to be done within its jurisdiction to promote local employment, then surely it cannot permit a State to require a person to go into a local packing business solely for the sake of enhancing the reputation of other producers within its borders.[285]

Unlike the extraterritorial strand of Dormant Commerce Clause precedent, which many courts have interpreted as a per se ban,[286] the excessive-burden cases require the application of a balancing test to

279. *Id.* at 138 (quoting ARIZ. REV. STAT. ANN. § 3–503C (Supp. 1969)).
280. *Id.*
281. *Id.* at 139.
282. *Id.* at 143.
283. *Id.* at 138.
284. *Id.* at 142; *see also* S. Pac. Co. v. Arizona ex rel. Sullivan, 325 U.S. 761, 770–71 (1945) ("Hence the matters for ultimate determination here are the nature and extent of the burden which the state regulation of interstate trains, adopted as a safety measure, imposes on interstate commerce, and whether the relative weights of the state and national interests involved are such as to make inapplicable the rule, generally observed, that the free flow of interstate commerce and its freedom from local restraints in matters requiring uniformity of regulation are interests safeguarded by the commerce clause from state interference.").
285. *Pike*, 397 U.S. at 146.
286. *See supra* Subpart IV.A.

determine whether the burden on interstate commerce is excessive in relation to the local benefits.[287]

In the 1997 *American Libraries Ass'n* case, Judge Preska concluded that the New York "harmful to minors law" was also invalid under the excessive-burden balancing test.[288] She acknowledged that New York had a valid interest in the "protection of children against pedophilia"[289] but concluded that the benefits of the New York law "are not overwhelming" when compared to the burdens on interstate commerce.[290] "Balanced against the limited local benefits resulting from the Act is an extreme burden on interstate commerce," Judge Preska wrote.[291] "The New York Act casts its net worldwide; moreover, the chilling effect that it produces is bound to exceed the actual cases that are likely to be prosecuted, as Internet users will steer clear of the Act by significant margin," Judge Preska concluded.[292]

Because the excessive-burden doctrine relies on a fact-dependent balancing test, it is difficult to predict with any degree of certainty whether a court would invalidate a state cybersecurity law.[293] Danielle Keats Citron argues, for instance, that state breach notification laws would survive such a challenge:

> Companies can readily identify the state citizens covered by the statutes and thus can provide notice according to each state's law. The cost of compliance is not excessive in light of the benefits to consumers. The state interest in ensuring notification of data breaches is strong. Without notice, consumers would not know to monitor their credit for fraud; companies might be inclined to skimp on data security since breaches would cost them nothing if hidden from the public and regulators.[294]

287. *See, e.g.*, Greater L.A. Agency on Deafness, Inc. v. Cable News Network, Inc., 742 F. 3d 414, 433 (9th Cir. 2014) (refusing to invalidate a California law that required closed captioning of television programs because it serves a "legitimate interest in providing hearing-impaired citizens equal access to online news videos and protecting its citizens from disparate discriminatory impact").

288. Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 177 (S.D.N.Y. 1997).

289. *Id.*

290. *Id.* at 178.

291. *Id.* at 179.

292. *Id.*

293. *See* Eric Goldman, *The Long-Term Promise of Privacy Federalism, Part 1*, TECH. & MKTG. L. BLOG (Sept. 1, 2015), https://blog.ericgoldman.org/archives/2015/09/the-long-term-promise-of-privacy-federalism-part-1-guest-blog-post.htm ("There is no way of knowing whether a state experiment is going to be successful without giving it time to unfold. Moreover, the *Pike* test is essentially about balancing: some state burdens upon interstate commerce can be upheld when they are designed to counter market inefficiencies (e.g. data privacy problems that the federal lawmaker is yet to address or that private companies face problems with when self-regulating).").

294. Citron, *supra* note 195, at 805.

Citron presents a compelling argument for upholding state data breach notification laws under the *Pike* balancing test, though the test provides courts with significant leeway to determine whether the burden is excessive. The more detailed and costly state cybersecurity laws, however, would be a closer call under the *Pike* test. For instance, the New York financial cybersecurity regulations impose stringent—and often expensive—requirements on companies that are regulated by the New York DFS.[295] The state might have difficulty demonstrating strong local benefits, as financial institutions also must comply with the Gramm-Leach-Bliley security requirements.[296] Likewise, California's new data protection law, the CCPA, will require many out-of-state companies to make substantial changes to their data processing and storage systems.[297] California would need to demonstrate countervailing local benefits to privacy and security that outweigh the potentially high costs of compliance.

States also might have difficulty justifying the local benefits of particularly outdated state cybersecurity laws. For instance, if ransomware and theft of geolocation data are a greater economic and national security threat than, for instance, identity theft, a state law that focuses on the confidentiality of Social Security numbers and financial account data might not have the same degree of local benefit than it had in the past.

C. Inconsistent Regulations

The least-developed line of Dormant Commerce Clause cases restricts the ability of states to impose inconsistent regulations. Although this sounds like an obvious mechanism by which to challenge state-by-state regulation of cybersecurity law, the doctrine under these cases is far from settled and likely more limited than the extraterritoriality or excessive-burden cases.

In 1986, the Supreme Court advanced this theory of the Dormant Commerce Clause when it invalidated a New York law that regulated the price that liquor producers, regardless of their location, charge to wholesalers in the state.[298] Besides concluding that the law had

295. *See supra* text accompanying notes 132–40.

296. *See* Matthew A. Schwartz & Corey Omer, *The Constitutionality of State Cybersecurity Regulations*, CLEARING HOUSE, https://www.theclearinghouse.org/banking-perspectives/2017/2017-q2-banking-perspectives/articles/constitutionality-cybersecurity-regulations (last visited Mar. 2, 2019) ("[T]he cybersecurity programs of the vast majority of financial services institutions operating in the United States – including state-chartered financial services institutions – are already subject to regulation and supervision by various federal authorities. Thus, in practice, state cybersecurity regulations may largely duplicate requirements already imposed on the same financial services institutions.").

297. *See supra* text accompanying notes 175–79.

298. *See* Brown-Forman Distillers Corp. v. N.Y. State Liquor Auth., 476 U.S. 573, 583–84 (1986).

impermissible extraterritorial effects,[299] the Court reasoned that "the proliferation of state affirmation laws following this Court's decision in *Seagram* has greatly multiplied the likelihood that a seller will be subjected to inconsistent obligations in different States."[300] New York's enforcement of its statute, the Court reasoned, could effectively "force those other States to alter their own regulatory schemes in order to permit appellant to lower its New York prices without violating the affirmation laws of those States."[301]

Goldsmith and Sykes argued that the inconsistent-regulations doctrine does not ban all state laws that are different from one another,[302] but instead the doctrine only applies if "nonuniform state regulations might impose compliance costs that are so severe that they counsel against permitting the states to regulate a particular subject matter."[303]

In *American Libraries Ass'n*, Judge Preska took a broader approach than that suggested by Goldsmith and Sykes and concluded that in addition to being extraterritorial and excessively burdensome, the New York decency law was unconstitutional because it subjected Internet use to inconsistent regulations.[304] Judge Preska pointed to laws imposed by other states that "selected different methods" to regulate content transmission.[305] The Internet, Judge Preska, observed, "requires a cohesive national scheme of regulation so that users are reasonably able to determine their obligations. Regulation on a local Level, by contrast, will leave users lost in a welter of inconsistent laws, imposed by different states with different priorities."[306]

Because there are few cases interpreting the inconsistent-regulations doctrine, it is impossible to predict with certainty whether state cybersecurity laws would survive a challenge for being inconsistent. If, as Goldsmith and Sykes suggested, the inconsistent-regulations doctrine is another balancing test that requires weighing the harms and benefits, critics of the state laws would increase their chances of success by demonstrating the burdens caused by the inconsistency. The CCPA, for instance, might survive

299. *Id.* at 581–83.
300. *Id.* at 583.
301. *Id.* at 584.
302. Goldsmith & Sykes, *supra* note 270, at 806 ("The inconsistent-regulations cases do not concern inconsistencies in the sense that acts required in one state are prohibited in another. Rather, they concern *different* regulations across states that heighten compliance costs for multijurisdictional firms. There is nothing unusual about nonuniform regulations in our federal system. States are allowed to make their own regulatory judgments about scores of issues.").
303. *Id.* at 806–07.
304. Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 169, 182 (S.D.N.Y. 1997).
305. *Id.* at 182.
306. *Id.*

an inconsistent-regulations challenge because there are no other state laws with which it directly conflicts.[307]

State data breach notification laws, in contrast, might face more scrutiny under the inconsistent-regulations test. It is difficult to conceive of the overwhelming benefits, for instance, of requiring companies to make their notification decisions based on different rules in every state. Moreover, there is little benefit in requiring different forms of data breach notice depending on the state of residency of the data subject or prohibiting a description of the breach to Massachusetts residents but requiring it for notices to Californians.[308] Companies might present a compelling case that the costs of complying with the fifty different requirements simply do not justify the burdens of the variance.

V. CONCLUSION

Securing the confidentiality, integrity, and availability of private-sector information and systems is among the most vexing challenges that the United States currently faces. As seen over the past decade, cyberattacks threaten U.S. economic interests, national security, and even the underpinnings of our democracy.[309] These challenges demand an effective and rigorous legal framework that reduces the likelihood of successful attacks and allows companies to more quickly mitigate harm and recover.

Unfortunately, we have yet to receive such a cybersecurity legal framework at the federal level.[310] Instead, we have a smorgasbord of state laws, some dating back nearly two decades.[311] Some of the state laws are more effective than others, some are harmonious, and some conflict.[312] Taken together, however, the state-by-state approach to cybersecurity results in a minimally effective regulatory morass that lacks a comprehensive national strategy. Hamilton's vision for a common direction for commercial regulation demands a more thoughtful national approach to such an important problem.[313] Congress can—and should—pass a tough and effective cybersecurity regulatory law that preempts the current state patchwork system. Absent such congressional action, it is increasingly likely that courts will apply Dormant Commerce Clause caselaw and find that at least some of the state laws are impermissibly extraterritorial, excessively burdensome, or inconsistent with one another.

307. *See supra* text accompanying 175–79.
308. *See supra* Subpart III.A.
309. *See supra* notes 1–4 and accompanying text.
310. Newman, *supra* note 6.
311. *See supra* Subpart III.B.
312. *See supra* Subpart III.B.
313. *See supra* Subpart II.A.