FEDERALIZING DATA BREACHES

EDWARD PERCARPIO

INTRODUCTION

The Equifax data breach affected 147 million people (almost half the country) and ultimately cost Equifax $380 million.[1] Luckily for plaintiffs, and unfortunately for Equifax, Equifax is headquartered in Georgia, whose federal courts have recognized a duty to safeguard personal data under Georgia common law.[2] If Equifax were instead headquartered in Illinois (e.g., if the same incident had happened to Walgreens), plaintiffs would have likely received nothing.

Data breaches are so common that they are now merely a cost of doing business on the internet.[3] Their ubiquity and penchant for headlining newspapers has placed increasing pressure on states and Congress to recognize a universal duty to safeguard personal information. After more than seven years of congressional waffling,[4] some state legislatures have taken the lead.[5] Other states, through legislative silence, have left the decision to the courts. This state of affairs creates a disjointed set of obligations, where Equifax must

1. *See In re* Equifax Customer Data Sec. Breach Litig., No. 1:17-md-2800-TWT, 2020 U.S. Dist. LEXIS 118209, at *145, *149 (N.D. Ga. Mar. 17, 2020) (approving settlement).

2. Georgia's state courts have been less eager to recognize such a duty. *See infra* Part I.A.

3. Data breaches are often confused with data incidents. Data incidents, which do not have to be reported and are seldom litigated, refer to events that compromise the integrity, confidentiality, or availability of information. Data breaches, on the other hand, are data incidents that result in a confirmed disclosure of data to an unauthorized party. *See* VERIZON, 2020 DATA BREACH INVESTIGATIONS REPORT 4 (2020), https://www.verizon.com/business/resources/reports/2020-data-breach-investigations-report.pdf [https://perma.cc/BJ2K-33VE] [hereinafter VERIZON 2020 DBIR]. While the number of discrete breaches dropped in 2020, the number of compromised records continues to climb. *See* Lance Whitney, *2020 Sees Huge Increase in Records Exposed in Data Breaches*, TECHREPUBLIC (Jan. 21, 2021, 10:50 AM), https://www.techrepublic.com/article/2020-sees-huge-increase-in-records-exposed-in-data-breaches/ [https://perma.cc/U8QY-3UN5].

4. *See* Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*, 127 YALE L.J.F. 614–16 (2018) (describing the lifecycle of breach, bill introduction, and congressional inaction since 2013).

5. These include California, Virginia, Massachusetts, and Ohio. *See* discussion *infra* Part I.E.

pay hundreds of millions of dollars, and Walgreens can count its blessings for hailing from the Land of Lincoln.

Some will say that this beautiful mess is why we have federalism. Heterogeneity bespeaks a diverse national populace and allows the federal government to observe the regulatory experimentation across states. Others will decry the inefficiency, the unfairness, the randomness. This Note interrogates both positions, asking, "is it time to federalize a duty to safeguard personal information?" This central question necessarily raises two first-order questions: (1) When is it appropriate to federalize anything? (2) If we do find that it is the right time to federalize, then how, institutionally, should that be actualized? These two questions guide the second half of the Note, while the first half focuses on describing our current decentralized framework and its practical impact.

Another question also inevitably arises during this inquiry: what form does the duty to safeguard personal information take, when it is recognized? States, and the FTC, tend to go after the low-hanging fruit when litigating on this point (e.g., unreasonable safeguards equal no encryption, no firewalls, and no security features).[6] As a result, grey area abounds on the topic of reasonable care. Academics and practitioners also avoid directly answering the question.[7]

Part I of this Note examines how states are approaching a duty to safeguard personal information. Parts I.A to I.C focus on three states—Georgia, Illinois, and California—whose courts and legislatures have taken notably diverse approaches to recognizing this duty. Part I.D synthesizes the findings with an eye towards the relationship between state and federal courts. Part I.E contextualizes the case studies within the national patchwork of other state regimes.

---

6. *See Symposium: The California Consumer Privacy Act*, 54 LOY. L.A. L. REV. 157, 195 (2020) (noting that state attorneys general tend to litigate by finding "scofflaws"—companies "who have done essentially nothing to comply."); Julie E. Cohen, *How (Not) to Write a Privacy Law*, KNIGHT FIRST AMEND. INST. AT COLUM. UNIV. 17–18 (2021), https://s3.amazonaws.com/kfai-documents/documents/306f33954a/3.23.2021-Cohen.pdf [https://perma.cc/2SXQ-JNV2] (describing the inefficacy of public enforcement litigation, particularly through the FTC, to deter privacy violations among tech companies).

7. For example, in a symposium on the California Consumer Privacy Act (CCPA), one speaker said: "One of the big focuses in these sorts of [data breach law] provisions is what the heck does 'reasonable' security practices mean, but I will leave that to Professor Wu to start to spell that out." To which the audience laughed, and Professor Wu never spelled it out. No one did. *Symposium: The California Consumer Privacy Act*, *supra* note 6, at 190.

With the caveat of a very limited sample size, Part I offers four central findings:

First, state approaches to recognizing a duty to safeguard personally identifiable information (PII) are extremely diverse. The case studies, while chosen to demonstrate heterogeneity, understate rather than exaggerate the disparity across the country.

Second, state appellate court opinions on data breaches are few and far between. And when state appellate courts do weigh in, they are often unhelpful in resolving the question of duty. Notably, this may be by design—many court opinions express the sentiment that the issue of duty is better resolved by the legislature than by traditional tort law.

Third, federal courts are the predominant forum for dealing with the duty to safeguard in the event of a data breach. Given the paltry backdrop of state court opinions on the topic, some federal courts have taken it upon themselves to generate a federal common law interpreting the nature of the duty and how/whether it aligns with the state's common law principles. The case law is non-binding, but it is proving influential in subsequent state court opinions on the topic.

Finally, whether a case is brought in state or federal court may determine the outcome. This is likely true for Georgia, but unlikely for Illinois or California.

Part II examines how these findings bear on the question of whether to federalize the duty. Specifically, this Note argues that the divergent approaches to recognizing and enforcing a duty to safeguard personal data have created an inefficiency and unfairness that militates in favor of at least *some* comprehensive federal regime. Assuming, then, that some amount of federalization is in order, Part II examines what an optimal path to federalization might look like, and how much federalization is best. Part II.A provides a brief background on federalism and federalization literature. Part II.B uses that literature to argue that, at this time, there is still some tangible benefit from federalism in this space, and therefore, complete federalization is not the optimal approach.

Part II.C asks and answers, if some federal regulation is needed, how do we know how much, and by whom? This section applies several factors from academic literature to determine the optimal mix of liability rules (from courts) versus regulation (from Congress and agencies) to the context of data breaches. This Note argues that a cooperative hybrid model would be optimal in this context, and federal courts should defer to agency standard-setting and determinations of preemption.

Part II.D identifies a snag in this plan: the lack of an on point expert agency and skepticism regarding whether the current enforcer—the FTC—is best positioned to regulate the field. Part II.D considers the role of insurance as an alternative option, given the skepticism that neither businesses nor agencies are well-positioned to provide the optimal risk-risk analysis in designing standards.

I.
STATE APPROACHES

A. Georgia

The Georgia state legislature has not taken a position on whether to recognize a duty to safeguard personal data in the event of a data breach. Georgia state courts have seen two data breach cases, and the Georgia Supreme Court first addressed the matter only in 2019.[8] In contrast, federal courts applying Georgia state law have been grappling with data breach cases for over a decade.[9]

Until 2016, Georgia federal courts had found that defendant businesses do not have an independent duty under Georgia tort law to implement reasonable protections against data breaches.[10] The

8. Except where noted otherwise, all statistics are as of April 2021. Searching "data breach" on LexisNexis and filtering the jurisdiction to include all Georgia state courts yields twelve hits. Six hits correspond to the same two data breach cases, *McConnell* and *Collins* (although at different levels of appeal), discussed at length in this Part. All other hits have no bearing on the issue. For example, four hits do not refer to data breaches at all but rather discuss contract claims arising from companies with "Data" in their names or were flagged merely due to the repetition of the word "breach." Another case, *Butler v. Equifax, Inc.*, dealt with a motion to dismiss regarding a parallel class action certification proceeding in state court, which was stayed pending the resolution of the federal multi-district litigation matter. No. 2017CV295644, 2018 Ga. Super. LEXIS 4502 (Bus. Case Div. July 26, 2018). A different case, *State ex rel. Carr v. Retrieval-Masters Creditors Bureau, Inc.*, is a consent order with no precedential value or admission of any facts or liability. No. 2021CV346830, 2021 Ga. Super. LEXIS 2215 (Apr. 22, 2021).

9. *See, e.g.*, Badish v. RBS Worldpay, Inc., No. 1:09-CV-0033-CAP, 2010 U.S. Dist. LEXIS 145301, at *16, *18 (N.D. Ga. Feb. 5, 2010) (finding standing and applying Georgia choice of law analysis to an identity theft class action suit in the wake of a data breach); *In re* Choicepoint, Inc., No. 1:05-CV-00686-JTC, 2006 U.S. Dist. LEXIS 97903 (N.D. Ga. Nov. 19, 2006) (discussing a federal securities class action suit following a data breach).

10. *See, e.g.*, Willingham v. Global Payments, Inc., No. 1:12-CV-01157-RWS-JFK, 2013 U.S. Dist. LEXIS 27764, at *61 (N.D. Ga. Feb. 5, 2013) (finding no duty of care because there was no direct relationship between plaintiff and defendant and dismissing Georgia state law negligence and Georgia Unfair and Deceptive Trade Practices Act (UDTPA) claims); Silverpop Sys. v. Leading Mkt. Techs., Inc., 641 F. App'x 849, 852 (11th Cir. 2016) (denying defendant's negligence counterclaim on the grounds that even if a duty existed, there was an insufficient showing

Home Depot data breach class action litigation, however, marked a turning point; the Northern District of Georgia held that an independent duty existed under Georgia state tort law based on the premise that parties owe a duty "to all the world not to subject [others] to an unreasonable risk of harm."[11] It borrowed the language and the proposition from *Bradley Center, Inc. v. Wessner*, in which the Georgia Supreme Court found that a mental hospital's legal duty to protect third parties from harm caused by its patients arose not from privity but rather from an independent duty to prevent a party under its control from harming others where it is or should be known that the party is likely to cause harm.[12]

The court in *Home Depot* did not attempt to analogize Home Depot's actions to those of the mental hospital in *Bradley Center*. Instead, it latched onto the *Bradley Center* court's broad proposition that defendants owed a duty to the world and extended its policy argument:

> To hold that no such duty existed would allow retailers to use outdated security measures and turn a blind eye to the ever-increasing risk of cyber attacks, leaving consumers with no recourse to recover damages even though the retailer was in a superior position to safeguard the public from such a risk.[13]

A month after the *Home Depot* decision, a Georgia appellate court decided *McConnell v. Department of Labor*, its first data breach case.[14] There, a Department of Labor employee had accidentally sent a spreadsheet of 4,000 Georgia residents' applications for unemployment benefits to 1,000 people on the spreadsheet.[15] The appellate court recognized that *Home Depot* had recently found a duty in a similar data breach case under Georgia law, but it decided not to follow the federal district court's lead. It distinguished *Home Depot* on the grounds that unlike in *Home Depot*, the plaintiffs had

---

of the applicable standard of care or, in the alternative, that defendant owed no duty under the economic loss rule).

11. *In re* Home Depot, Inc., No. 14-2583, 2016 U.S. Dist. LEXIS 65111, at *28 (N.D. Ga. May 18, 2016) (citing Bradley Ctr., Inc. v. Wessner, 296 S.E.2d 693, 695 (Ga. 1982)).

12. *Bradley Ctr.*, 296 S.E.2d at 696. For this proposition, the court relied on Section 319 of the Restatement (Second) of Torts: "One who takes charge of a third person whom he knows or should know to be likely to cause bodily harm to others if not controlled is under a duty to exercise reasonable care to control the third person to prevent him from doing such harm." RESTATEMENT (SECOND) OF TORTS § 319 (AM. L. INST. 1965).

13. *Home Depot*, 2016 U.S. Dist. LEXIS 65111, at *29.

14. 787 S.E.2d 794 (Ga. Ct. App. 2016).

15. *Id.* at 796.

not alleged that the Department of Labor had any knowledge or awareness of the risk of a data breach.[16] It also remarked that *Bradley Center*—and the *Home Depot* court's interpretation of it—was inapplicable to data breaches because the duty in *Bradley Center* was premised on the creation of a special relationship.[17]

Two years later, the Northern District of Georgia dealt with the Arby's data breach litigation.[18] In spite of *McConnell*, the district court reaffirmed both *Bradley Center*'s applicability and *Home Depot*'s assertion of an independent common law duty to safeguard personal information against data breaches.[19] The district court distinguished *McConnell* on three grounds. First, it noted that the *McConnell* decision had been vacated on other grounds and thus was not binding.[20] Second, the "Georgia Court of Appeals in *McConnell* did not overrule the Georgia Supreme Court's recognition in [*Bradley Center*] of a general duty of care."[21] Third, the facts as alleged in *McConnell* did not assert that there were any known security deficiencies or that the employee's inadvertent disclosure was foreseeable; yet in both *Arby's* and *Home Depot*, both defendants were aware of security risks, thereby creating the duty to implement reasonable security measures in response.[22]

By the time the Northern District of Georgia issued its opinion in *In re Equifax Customer Data Security Breach Litigation*,[23] *McConnell* had reached the Georgia Supreme Court, been remanded, and

16. Specifically, the *McConnell* court noted:

> [T]he district court found a duty to protect the personal information of the defendant's customers in the context of allegations that the defendant failed to implement reasonable security measures to combat a substantial data security risk of which it had received multiple warnings dating back several years and even took affirmative steps to stop its employees from fixing known security deficiencies. There are no such allegations in this case.

Id. at 797 n.4.

17. *Id.*

18. *In re* Arby's Rest. Grp. Litig., No. 1:17-cv-0514-AT, 2018 U.S. Dist. LEXIS 131140 (N.D. Ga. Mar. 5, 2018).

19. *Id.* at *18 ("Georgia courts recognize a 'general duty one owes to all the world not to subject them to an unreasonable risk of harm.'" (quoting Bradley Ctr., Inc. v. Wessner, 296 S.E.2d 693, 695 (Ga. 1982))); *see also id.* at *23 ("Under Georgia law and the standard articulated in *Home Depot*, allegations that a company knew of a foreseeable risk to its data security systems are sufficient to establish the existence of a plausible legal duty and survive a motion to dismiss.").

20. *Id.* at *25.

21. *Id.* at *26.

22. *Id.* at *25–26.

23. *In re* Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295 (N.D. Ga. 2019).

been decided again at the appellate level.[24] This time, the court of appeals affirmed its prior decision, making no mention of *Home Depot* or *Arby's* despite their potential conflict with its holding that the defendant owed no duty.[25] The *Equifax* court reasoned that this silence "suggests a tacit approval" of the distinction the *Arby's* court had made between the *McConnell* line of cases and the *Arby's/Home Depot/Equifax* cases where the defendant had been aware of the foreseeable risk.[26]

In the wake of *Equifax*, the Georgia Supreme Court granted certiorari on *McConnell* to clarify the common law negligence issue, among others. Perhaps in direct response to the *Arby's* court's interpretation of the court of appeals, the Georgia Supreme Court explicitly condemned any reliance on *Bradley Center* to find a common law duty to safeguard personal information.[27] However, it stayed silent on *Arby's* third argument distinguishing the foreseeability component. In a footnote, it narrowed its holding so as to seemingly avoid overruling this argument or any of the federal court cases: "[w]e also do not consider whether a duty might arise on these or other facts from any other statutory or common law source, as no such argument has been made here."[28] The footnote did not, however, allow for the conclusion that the Georgia Supreme Court's silence on the federal courts' line of cases should be read as a tacit approval of their holdings.

In *Collins v. Athens Orthopedic Clinic*, decided seven months later, the Georgia Supreme Court continued to avoid the question of duty.[29] The court framed the issue as solely focused on the cognizable injury portion of Georgia's standing doctrine,[30] and held that

24. McConnell v. Dep't of Labor, 814 S.E.2d 790 (Ga. Ct. App. 2018).

25. *Id.* at 797–99 (finding "no source in Georgia statutory law or case law" that supported a common law duty to safeguard personal information).

26. *In re Equifax, Inc.*, 362 F. Supp. 3d at 1325.

27. Dep't of Labor v. McConnell, 828 S.E.2d 352, 358 (Ga. 2019) ("[W]e hereby disapprove *Bradley Center* to the extent that it created a general legal duty 'to all the world not to subject [others] to an unreasonable risk of harm.' We therefore reject McConnell's reliance upon *Bradley Center*." (citation omitted) (quoting Bradley Ctr., Inc. v. Wessner, 296 S.E.2d 693, 695 (Ga. 1982))).

28. *Id.* at 358 n.5.

29. Collins v. Athens Orthopedic Clinic, P.A., 837 S.E.2d 310, 311 (Ga. 2019). There, a plaintiff damages class of 200,000 current and former patients of a medical clinic sued the clinic after its patient records were hacked into and offered for sale on the dark web. *Id.* at 311–12.

30. *Id.* at 312 ("We granted the plaintiffs' petition for certiorari to consider whether the Court of Appeals erred in holding that the plaintiffs failed to allege a legally cognizable injury. We conclude that the plaintiffs *did* allege a cognizable injury.").

the injury is sufficiently cognizable where a plaintiff alleges that the PII had been stolen by a criminal.[31] In arriving at this conclusion, the court indicated it was influenced by "[r]ecent persuasive federal district court decisions applying Georgia law" that had found standing despite stricter Article III standing requirements.[32] But while the facts of the case aligned more closely with the federal cases, the court neglected to resolve the ambiguity around duty, which it left open for resolution on remand.[33]

Where does this leave Georgia's state and federal courts after a decade of case law? Despite two opportunities, the Georgia Supreme Court has avoided deciding whether there is a common law duty to safeguard personal information. It has also neglected to accept or reject federal court decisions that found a duty to safeguard personal information where the defendant was aware of a risk to its security systems. Yet by rejecting any reliance on *Bradley Center*, the Georgia Supreme Court has undercut those federal courts' foundations in Georgia common law for finding such a duty. This leaves federal courts in an odd position: to continue finding a duty to safeguard personal information, they have ample federal case law to rely on but no grounding in state common law.

If the balance is untenable and precarious at best, then what are Georgia's appellate courts waiting for? The legislature, it seems. The court of appeals in *McConnell* put it plainly:

> Given the General Assembly's stated concern about the cost of identity theft to the marketplace and to consumers, as well as the fact that it created certain limited duties with regard to personal information (e.g., the duty to notify affected persons of data breaches and the duty not to intentionally communicate information such as social security numbers to the general public), it may seem surprising that our legislature has so far not acted to establish a standard of conduct intended to protect the security of personal information, as some other jurisdictions have done in connection with data protection and data breach notification laws. It is beyond the scope of judicial authority, however, to move from aspirational statements of

31. *Id.* at 316 ("[Plaintiffs'] allegation that the criminal theft of their personal data has left them at an imminent and substantial risk of identity theft is sufficient at this stage of the litigation [to show injury].").

32. *Id.* at 316–17.

33. *Id.* at 315–16 ("[S]howing injury as a result of the exposure of data is easier in a case like this [given the criminal component] . . . . But that easier showing of injury may well be offset by a more difficult showing of breach of duty." (referencing Dep't of Labor v. McConnell, 828 S.E.2d 352 (Ga. 2019))).

> legislative policy to an affirmative legislative enactment sufficient to create a legal duty.[34]

The following year (2019), the Georgia Supreme Court in *Collins* echoed the call for the state legislature to resolve the problem, albeit in a footnote:

> We recognize that this case involves a fairly new kind of injury. As a court, we discharge our duty to apply traditional tort law to that injury. But that traditional tort law is a rather blunt instrument for resolving all of the complex tradeoffs at issue in a case such as this, tradeoffs that may well be better resolved by the legislative process.[35]

Until the legislature acts, it appears that Georgia state courts will either continue to pass the buck to future courts or eventually find there is no duty to safeguard personal information, as Illinois has done.[36] Given the robust body of federal case law on this point, leading, in the aggregate, to billions of dollars transferred by defendants across hundreds of millions of tort claimants under the auspices of a potential duty to safeguard personal information in Georgia tort law, recognizing that duty would make quite the splash.

B. Illinois

The Illinois legislature has enacted various privacy laws,[37] but, like Georgia, it has not spoken on a general duty to safeguard personal information. Also similar to Georgia, the state case law is extremely sparse and incredibly stale: there is only one relevant appellate court decision, and it dates back to 2010. Yet that appellate court case, *Cooney v. Chicago Public Schools*,[38] solidified the precedent in federal court that Illinois provides no duty whatsoever for

34. McConnell v. Dep't of Labor, 814 S.E.2d 790, 799 (Ga. Ct. App. 2018).

35. *Collins*, 837 S.E.2d at 316 n.7.

36. *See infra* Part I.B.

37. Like every state, Illinois has a data breach notification law. *See* 815 ILL. COMP. STAT. ANN. 530/10 (LexisNexis 2023) (requiring businesses who own or license personal information to notify residents in the event of a data breach). But Illinois also recently enacted the novel Illinois Biometric Information Privacy Act (BIPA). 740 ILL. COMP. STAT. ANN. 14/1 (LexisNexis 2023). In 2020, a national class action successfully reached a $550 million settlement with Facebook for violations of BIPA's privacy requirements. *See* Natasha Singer & Mike Isaac, *Facebook to Pay $550 Million to Settle Facial Recognition Suit*, N.Y. TIMES (Jan. 29, 2020), https://www.nytimes.com/2020/01/29/technology/facebook-privacy-lawsuit-earnings.html [https://perma.cc/WBZ7-JXD8].

38. 943 N.E.2d 23 (Ill. App. Ct. 2010).

companies to safeguard personal information in the event of a data breach.

The facts of *Cooney* parallel *McConnell* in that they both tell the story of a public employee's (or contractor's) careless mistake, rather than the more common data breach tale of criminal theft.[39] In *Cooney*, a Chicago public school contractor accidentally failed to redact sensitive health insurance information when it mailed an insurance enrollment letter to 1,700 former employees.[40] When the school board found out, it asked the recipients to return or destroy the list and offered them a year of free credit protection services; a class action lawsuit ensued.[41] Plaintiffs, finding no case to support their theory, urged the court to recognize a "new common law duty to safeguard personal information," particularly since the case dealt with such sensitive information.[42] The court denied them, reasoning—as Georgia appellate courts did in *McConnell* and *Collins*—that the creation of a new legal duty was beyond their purview. This was particularly so because the legislature had "specifically addressed this issue" by providing a data breach notification duty and refusing to extend any further duties.[43] Thus, finding no duty for companies to safeguard personal information under Illinois statute or common law, the court dismissed the case.

Federal courts sitting in diversity and adjudicating data breaches under Illinois law have relied on *Cooney* as the sole authority on whether Illinois provides a duty to safeguard personal information.[44] Indeed, most federal courts have interpreted *Cooney* to stand for the proposition that a general duty analysis under traditional negligence theory cannot accommodate data breaches with-

39. Verizon's 2020 Data Breach Investigations Report found that around 80% of breaches in North America are due to phishing attacks. VERIZON 2020 DBIR, *supra* note 3, at 88. In contrast, errors were involved in 22% of all breaches, and only 8% involved misuse by authorized users, as in the *Cooney* and *McConnell* cases. *Id.* at 7.

40. *Cooney*, 943 N.E.2d at 27.

41. *Id.*

42. *Id.* at 28–29.

43. *Id.* at 29 ("[W]e do not believe that the creation of a new legal duty beyond legislative requirements already in place is part of our role on appellate review. As noted, the legislature has specifically addressed the issue and only required the Board to provide notice of the disclosure.").

44. *See* Cmty. Bank of Trenton v. Schnuck Mkts. Inc., 887 F.3d 803, 816–17 (7th Cir. 2018). There, the court noted that "[t]hough duty is a basic concept in tort law, the Illinois Supreme Court has not directly spoken to this question in the context of data breaches." *Id.* at 816. The Seventh Circuit then considered Illinois appellate decisions on the topic and arrived at *Cooney* as its sole source of authority. *Id.* at 816–17.

out the creation of a new duty (which *Cooney* bars).[45] In *Community Bank of Trenton v. Schnuck Markets Inc.*, the Seventh Circuit also expanded *Cooney*'s coverage to govern essentially all data breach cases in the absence of an Illinois Supreme Court opinion that distinguished certain facts as relevant in a court's duty analysis.[46]

The resulting litigation climate is a state of somewhat settled law, at least in federal courts. After *Community Bank of Trenton*, any post-data-breach tort suit premised on Illinois common or statutory law will fail in federal court regardless of the facts. Until an Illinois appellate court hears a case on it (which they somehow have avoided for over a decade), there is no duty for companies to safeguard personal information in Illinois.

C. California

1. California's "Reasonable Data Security Law"

The California legislature has recognized a duty to safeguard personal information for almost twenty years. A statute enacted in 2003, introduced and passed as Senate Bill 1386, added a breach notification law,[47] a reasonable data security requirement,[48] and a private right of action to recover (actual) damages.[49] The data security provision provides, in part, that "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security proce-

45. *See In re* Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447, 478 (D. Md. 2020). There, the district court dismissed plaintiffs' negligence claims under Illinois law, acknowledging that:

> [A]n Illinois court could find a duty here [under traditional tort principles] . . . [h]owever, they do not escape the conclusion that any such finding would establish a 'new duty' regarding data security in Illinois that *Cooney* declined to establish. Without further authority, I cannot conclude that the Illinois Supreme Court would disagree with the analysis in *Cooney*.

Id.; *see also Cmty. Bank of Trenton*, 887 F.3d at 816 (noting that "[t]he [*Cooney*] opinion reads as a more general statement that no duty to safeguard personal information existed, regardless of the kind of loss").

46. *Cmty. Bank of Trenton*, 887 F.3d at 816 ("In the absence of some other reason why the Illinois Supreme Court would likely disagree with the Cooney analysis on this issue of duty under the common law, . . . we predict that the state court would not impose the common law data security duty the plaintiff banks call for here." (citing Anicich v. Home Depot U.S.A., Inc., 852 F.3d 643, 649 (7th Cir. 2017))). The relevant portion of *Anicich* referenced by the court described exceptions to the general lack of duty to prevent third party criminal acts. 852 F.3d at 649.

47. CAL. CIV. CODE § 1798.82 (Deering 2023).

48. *Id.* § 1798.81.5.

49. *Id.* § 1798.84.

dures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[50]

The definition of personal information under the data security provision (Section 1798.81.5) is narrow. It only includes breaches that disclose first and last name in combination with one or more of a select few types of sensitive personal information.[51] In 2015, the legislature expanded the definition of personal information to include a username and email address in combination with a password that could compromise an account.[52] This addition does little to align the definition of personal information, as it relates to the duty, with the broader, more colloquial understanding of personal information.[53] Consequently, some federal courts in California have allowed data breach cases to proceed under common law theories of negligence while rejecting the statutory claim on definitional grounds.[54]

The duty to safeguard personal information has been enforced in state and federal courts by both consumers and the California

50. *Id.* § 1798.81.5(b).

51. *See id.* § 1798.81.5(d)(1) (defining the additional personal data types to encompass only social security number, driver's license number, account or debit card number in combination with a password to access the account, and medical information).

52. *See* Heather Egan Sussman et al., *California Governor Signs CCPA and Breach Notification Statute Amendments into Law*, ORRICK (Oct. 18, 2019), https://blogs.orrick.com/trustanchor/2019/10/18/the-end-of-the-california-legislative-session-which-ccpa-amendments-passed/ [https://perma.cc/6KUG-YB8E] (describing the legislative history of Section 1798.81.5).

53. This is particularly striking given the fact that this broad understanding of personal information is enshrined elsewhere in the Civil Code. *See, e.g.*, CAL. CIV. CODE § 1798.3(a) (defining "personal information" as "any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, the individual's name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history . . . [and] statements made by, or attributed to, the individual"). The obvious distinction between the two is that the latter applies only to agencies while the former, narrower definition applies to businesses.

54. *See, e.g.*, Corona v. Sony Pictures Ent., Inc., No. 14-CV-09600, 2015 U.S. Dist. LEXIS 85865 (C.D. Cal. June 15, 2015). There, the court allowed a data breach class action to proceed on a common law negligence theory and further found that a special relationship existed between employees and Sony which avoided the economic loss rule bar. *Id.* at *12–13. The court, however, denied plaintiffs' Section 1798.81.5 ("Customer Records Act") theory because, as employees, they were not customers. *Id.* at *16–18. Also, neither the court nor the plaintiffs explicitly used Section 1798.81.5 as a hook to establish negligence, which suggests the existence of the duty outside statutory enshrinement. *Id.* at *7–9.

Attorney General (AG).[55] The most concrete development in understanding what it means to provide "reasonable" data security came not from litigation but from then-Attorney General of California Kamala Harris's influential 2016 Data Breach Report.[56] The report compiled statistics on the 657 data breaches that had been reported to the AG from 2012 to 2015, and declared that it would peg its enforcement of a minimum reasonable security standard to the 20 security controls developed by the nonprofit Center for Internet Security.[57] Failure to implement all controls would constitute unreasonable data security and subject the entity to an enforcement action.[58]

Count Connections	Know the hardware and software connected to your network. (CSC 1, CSC 2)
Configure Securely	Implement key security settings. (CSC 3, CSC 11)
Control Users	Limit user and administrator privileges. (CSC 5, CSC 14)
Update Continuously	Continuously assess vulnerabilities and patch holes to stay current. (CSC 4)
Protect Key Assets	Secure critical assets and attack vectors. (CSC 7, CSC 10, CSC 13)
Implement Defenses	Defend against malware and boundary intrusions. (CSC 8, CSC 12)
Block Access	Block vulnerable access points. (CSC 9, CSC 15, CSC 18)
Train Staff	Provide security training to employees and vendors with access. (CSC 17)
Monitor Activity	Monitor accounts and network audit logs. (CSC 6, CSC 16)
Test and Plan Response	Conduct tests of your defenses and be prepared to respond promptly and effectively to security incidents. (CSC 19, CSC 20)

Figure 1: Security controls undergirding the California AG's "reasonable" security standard.[59]

55. At the time of writing (April 2021), filtering LexisNexis by Section 1798.81.5 in California state courts shows four (published) distinct cases: three brought by the Attorney General of California and one brought by an individual plaintiff. The individual consumer case, *Acosta v. Board of Chiropractic Examiners*, failed on the grounds that the information disclosed (name and email address in association with a drug test) did not satisfy the definition of personal information. No. 19ST-cv-06135, 2020 Cal. Super. LEXIS 1841, at *5 (Feb. 27, 2020). The AG cases are final judgments and consent orders of multistate actions against large companies. *See* People v. Target Corp., No. CGC-17-559105, 2017 Cal. Super. LEXIS 1631 (May 23, 2017); People v. Equifax, Inc., No. CGC-17-561529, 2017 Cal. Super. LEXIS 6771 (Dec. 21, 2017); People v. Uber Techs., No. CGC-18-570124, 2018 Cal. Super. LEXIS 5119 (Sept. 26, 2018). Federal district courts in California, on the other hand, have seen thirty-eight cases dealing with Section 1798.81.5, none of which have been brought by the AG.

56. CAL. DEP'T JUSTICE, CALIFORNIA DATA BREACH REPORT (Feb. 2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf [https://perma.cc/DRH4-8C8C].

57. *Id.* at 30.

58. *Id.*

59. *Id.* at 32. The full list can be found in Appendix A of the Report. *Id.* at 39.

2. The CCPA and the Duty to Safeguard Personal Information

When the California legislature enacted the California Consumer Privacy Act (CCPA) in 2018, it incorporated the previously existing standard of reasonable data security indq; data to the Act.[60] The CCPA does not provide guidance beyond this description of the duty, i.e., what "reasonable security procedures and practices" might entail. But it does allow businesses to "seek the opinion of the Attorney General for guidance on how to comply with the provisions" of the statute.[61] Notably, however, the California Attorney General has not initiated any rulemaking or issued any interpretive guidance to flesh out what a "reasonable" security program looks like,[62] despite the public outcry for guidance on this point during public hearings.[63] That said, perhaps the AG's silence merely indicates that its position on compliance has not changed since the 2016 Data Breach Report.

Despite containing a textually identical duty, the CCPA raises the stakes of compliance by allowing for statutory damages. The AG can seek injunctive relief and penalties up to $2,500 per violation (increased to $7,500 if the violation is intentional).[64] Consumers can also seek legal and equitable relief in the form of actual damages, statutory damages between $100 and $750 per consumer per incident, and injunctive or declaratory relief.[65] Given the per-violation count and the ease of collecting massive amounts of personal data, these statutory penalties could quickly amount to bet-the-company litigation.[66]

---

60. CAL. CIV. CODE § 1798.100(e) (Deering 2023) ("A business that collects a consumer's personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Section 1798.81.5.").

61. *Id.* § 1798.155(a).

62. The California AG promulgated six regulations to date, none of which speak to the reasonableness standard. *See* CAL. CODE REGS. tit. XI, § 999.300–37.

63. *See* Michael Osakwe, *Public Comments Show Lingering Problems with California's Data Privacy Law*, VENTUREBEAT (Dec. 18, 2019), https://venturebeat.com/2019/12/18/hearings-show-lingering-problems-with-californias-data-privacy-law/ [https://perma.cc/GL5V-AK67] (reporting on the uncertainty around "core terms" including "reasonable security measures" at the Los Angeles public hearing).

64. CAL. CIV. CODE § 1798.155(b).

65. *Id.* § 1798.150(a)(1).

66. *See* Nicholas Schmidt, *Top 5 Operational Impacts of CCPA: Part 5 – Penalties and Enforcement Mechanisms*, IAPP (Aug. 21, 2018), https://iapp.org/news/a/top-5-operational-impacts-of-cacpa-part-5-penalties-and-enforcement-mechanisms/ [https://perma.cc/E2RT-VF9L] (commenting that had the CCPA been in place

The private right of action still has a few important limiting provisions. First, in keeping with the text of Section 1798.81.5 of the California Civil Code, the right only applies to data breaches where the breached personal data was nonencrypted and nonredacted or was a combination of an email and a password or security question such that the attacker could access an account.[67] The California Attorney General, clarifying on this point, explained that the personal information stolen must include the individual's first name (or first initial), last name, and an additional type of personal information;[68] all of the information must also be nonencrypted and nonredacted.[69]

Second, the cause of action is limited to this statutory provision and cannot be extended to any other statutory, common law, or constitutional claim.[70] Third, before any individual or class action for statutory damages can proceed, the consumer must provide the business written notice "identifying the specific provisions" of the law that the consumer alleges were violated.[71] If the business cures the violations within thirty days and "provides the consumer an express written statement that the violations have been cured and that no further violations shall occur," then any action against the business is barred.[72]

A final limitation to obtaining statutory damages lies in the scope of the CCPA. Section 1798.140(c) of the California Civil Code describes that the CCPA only applies to (1) for-profit busi-

during the Cambridge Analytica scandal, Facebook could have faced penalties of $61.6 billion or $184.7 billion depending on whether the violation was intentional or unintentional); *see also* Danny Bradbury, *California's CCPA Gets Enforcement Teeth Today*, INFOSECURITY (July 1, 2020), https://www.infosecurity-magazine.com/news/californias-ccpa-gets-teeth-today/ [https://perma.cc/7RVU-4DJX] (quoting a CTO of the IAPP warning that "[w]ith companies collecting data about millions of California residents, the numbers add up quickly to sums that could dwarf the FTC's $5 billion settlement with Facebook").

67. CAL. CIV. CODE § 1798.150(a)(1).

68. Additional forms of personal information include social security numbers, unique government-issued identification numbers (e.g., driver's license number, tax identification number, passport), financial accounts or credit card numbers (if combined with required password or security code), medical or health insurance information, or biometric data. *See* California Consumer Privacy Act (CCPA), CAL. OFF. ATT'Y GEN., https://oag.ca.gov/privacy/ccpa [https://perma.cc/2EBW-V8FW]. As of 2020, this list reflects the types of PII covered under the California data breach notification law. CAL. CIV. CODE § 1798.81.5.

69. CAL. OFF. ATT'Y GEN., *supra* note 68.

70. CAL. CIV. CODE § 1798.150(c).

71. *Id.* § 1798.150(b).

72. *Id.* Consumers can enforce any breaches of the business's express written statement and pursue statutory damages for each breach of the written statement.

nesses that (2) collect California residents' personal information or determine the purpose or means of processing their PII, (3) do business in California, and either (a) have a gross revenue of over $25 million, (b) buy, receive, or sell PII of more than 50,000 California residents, or (c) derive 50% or more of their revenue from selling California residents' PII.[73]

3. Interest Group Politics, Prop 24, and the CPRA Amendments

The CCPA underwent a massive overhaul before it even went into effect.[74] Tugging at opposing threads of the legislation were the lobbyists for the Silicon Valley tech companies, and a coalition of privacy groups including the American Civil Liberties Union and the Electronic Frontier Foundation.[75] The tech companies feared a massive overhaul to their operations and wanted carveouts for certain common forms of data processing. The privacy groups saw those carveouts as loopholes that would defang the bill.[76] In the end, both sides got some of what they wanted. The tech lobby got a thirty-day cure provision, a limitation of the private right of action to the data breach provision only, and an exemption from providing any of the enumerated consumer rights if the data processing or transfer was for a "business purpose," among other concessions. The privacy groups got the bundle of consumer rights, a private right of action with large statutory damages (for data breaches only), and the passage of the most stringent omnibus data protection law in the country.[77]

As with any good compromise, no one was happy. Mary Stone Ross, one of the three key drafters of the CCPA, disavowed the law and has since publicly advocated for a federal privacy law.[78] Another drafter, Alastair Mactaggart, decided to try to amend the CCPA through a ballot proposition.[79] The proposition, (Prop 24)

73. CAL. CIV. CODE § 1798.140(c).

74. *See, e.g.*, Gilad Edelman, *The Fight Over the Fight Over California's Privacy Future*, WIRED (Sept. 21, 2020), https://www.wired.com/story/california-prop-24-fight-over-privacy-future/ [https://perma.cc/LZ54-FJMU].

75. *See* Issie Lapowsky, *Tech Lobbyists Push to Defang California's Landmark Privacy Law*, WIRED (Apr. 29, 2019), https://www.wired.com/story/california-privacy-law-tech-lobby-bills-weaken/ [https://perma.cc/EJ4D-5WDF].

76. *Id.*

77. *See* Edelman, *supra* note 74.

78. Mary Stone Ross, *I Helped Draft California's New Privacy Law. Here's Why it Doesn't Go Far Enough*, FAST COMPANY (Jan. 3, 2020), https://www.fastcompany.com/90444501/i-helped-draft-californias-new-privacy-law-heres-why-it-doesnt-go-far-enough [https://perma.cc/G8V5-C2GJ].

79. *Id.*

would create the California Privacy Rights Act (CPRA) and patch the holes created by the tech lobby and legislative compromise.[80] Importantly, Prop 24, as written, created a "one-way ratchet" that would allow the legislature to amend the Act by simple majority but only if it increased privacy protections.[81] Prop 24 passed in November 2022 and took effect on January 1, 2023.[82]

The CPRA makes one major change to the enforcement structure. It shifts the rulemaking and enforcement burden from the Attorney General to a newly created California Privacy Protection Agency (CalPPA).[83] CalPPA functions like a state analog to a federal administrative agency: led by a five-member board of experts, it can issue rules and pursue enforcement actions to carry out the purposes of the CPRA through hearings, orders, and penalties, overseen by its own administrative law judges.[84] It can subpoena witnesses,[85] audit businesses,[86] and advise the legislature on privacy-related legislation.[87] To fund the agency, the CPRA establishes a budget of $10 million per year flowing from the California General Fund, supplemented by the proceeds of any penalties brought by CalPPA which are placed in a separate Consumer Privacy Fund within the General Fund.[88]

---

80. Proposition 24, The California Privacy Rights Act of 2020 § 2(D) (as amended Nov. 4, 2019), https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf [https://perma.cc/JU2N-Q4HN] ("Even before the CCPA had gone into effect, the Legislature considered many bills in 2019 to amend the law, some of which would have significantly weakened it. Unless California voters take action, the hard-fought rights consumers have won could be undermined by future legislation.").

81. Cal. Const. Ctr., *How California Lives with Two Legislatures*, SCOCA BLOG (updated Aug. 5, 2020), http://scocablog.com/how-california-lives-with-two-legislatures/ [https://perma.cc/7ZCM-Y7LK].

82. Cal. Prop 24 § 21(22)(d).

83. *Id.* § 17 (amending CAL. CIV. CODE § 1798.155 to add CalPPA as an additional administrative enforcement mechanism); *id.* § 24 (amending CAL. CIV. CODE § 1798.199.10 et seq. to establish CalPPA); *see also* CAL. CIV. CODE § 1798.155 (amended Nov. 3, 2020 by Prop. 24 § 17; operative Jan. 1, 2023, pursuant to Prop. 24 § 31); *id.* § 1798.199.10 (added Nov. 3, 2020 by Prop. 24 § 24.1; operative Dec. 16, 2020, pursuant to Prop. 24 § 31).

84. CAL. CIV. CODE § 1798.199.55. Penalties are unchanged from the CCPA: Section 1798.199.55(a)(2) provides that penalties shall be no more than $2,500 per violation or $7,500 per each intentional violation.

85. *Id.* § 1798.199.65.

86. *Id.* § 1798.199.40(f).

87. *Id.* § 1798.199.40(g).

88. *See id.* § 1798.160; *see also id.* § 1798.199.55(a)(2) (designating fines to flow to the Consumer Privacy Fund); *id.* § 1798.155(b) (describing that all fines are intended to offset the costs incurred by the courts, the AG, and the CalPPA).

Aside from the creation of a new enforcement body, there are few changes on the duty and enforcement side relevant to the purposes of this Note. The CPRA does not alter any of the statutory damages figures, nor does it touch any of the limiting provisions to the private right of action. It made one small adjustment to the cure provision, clarifying that "[t]he implementation and maintenance of reasonable security procedures and practices pursuant to §1798.81.5 following a breach does not constitute a cure with respect to that breach."[89] In other words, the negligence inquiry focuses on the company's pre-breach security program, not on subsequent remedial measures. Other than that, the CPRA's main contribution (for the narrow purposes of this Note) is the establishment of a CalPPA and the hope that it will generate guidance on compliance through its expertise.

4. Litigation Post-CCPA

Bearing in mind the recency of the CCPA's enactment, three trends are emerging from the first wave of litigation. First, most if not all cases are being brought in federal court as class actions.[90] Second, those class actions allege both a nationwide and (usually in the alternative) a California class or subclass. Third, plaintiffs are all customers suing companies for data breaches, nearly all of which resulted from criminal hacking.[91] Despite these commonalities, the dispositions thus far have diverged: one settled (*Barnes*), one was dismissed by the court (*Rahman*), and another was voluntarily dismissed by the parties (*Fuentes*).

Another curious difference is that despite the enactment of a privacy law with massive potential damage awards, not every plaintiff is taking the opportunity to leverage the CCPA to seek them. In *Barnes v. Hanna Andersson*, for example, plaintiffs reserved the right to amend their class action complaint to seek damages under the CCPA.[92] Their negligence claim instead grounded the duty argu-

89. *Id.* § 1798.150.

90. *E.g.*, Class Action Compl., Barnes v. Hanna Andersson, LLC, No. 20-cv-00812 (N.D. Cal. Feb. 3, 2020); Fuentes v. Sunshine Behav. Health Grp., LLC, No. 8:20-cv-00487, 2020 U.S. Dist. LEXIS 198900, at *1 (C.D. Cal. Oct. 26, 2020); Rahman v. Marriott, Int'l, Inc., No. 8:20-cv-00654, 2021 U.S. Dist. LEXIS 15155 (C.D. Cal. Jan. 12, 2021); Atkinson v. Minted, Inc., No. 3:20-cv-03869, 2021 U.S. Dist. LEXIS 244257 (N.D. Cal. Dec. 17, 2021).

91. The one exception is *Fuentes v. Sunshine Behavioral Health Group*, where the cloud-based system used to store patient health information was inadvertently set up so as to make the records publicly accessible on the internet. Class Action Compl. at 5, *Fuentes*, 2020 U.S. Dist. LEXIS 198900.

92. Class Action Compl. at 24, *Barnes*, No. 20-cv-00812.

ment in Section 1798.81.5 of the California Civil Code; Section 5 of the Federal Trade Commission Act; and industry standards (PCI DSS).[93] (Plaintiffs did not cite the 2016 Data Breach Report.) Some suggest that the caution around adding a direct CCPA cause of action involves precisely some of the limitations of the private right of action mentioned earlier.[94] For example, what if the defendant encrypted the information and only after exfiltration did the hackers decrypt the PII? Would that defeat standing under the CCPA's narrow definition of personal information?[95] If the defendants had removed the malware within thirty days, would that constitute a cure and prevent the class action? These unanswered questions have significant consequences for the strength of a plaintiff's case. Safer, then, to leave room to add the CCPA claim after some discovery.

D. Data Breaches and the Relationship Between State and Federal Courts

The three state case studies were meant to canvass the spectrum of state approaches to recognizing a tort duty to safeguard personal information. Accordingly, the purpose of this Part has been descriptive. To that end, we can make a few global observations based on how these states have dealt with the duty.

First, state courts do not see many data breach cases. The Georgia Supreme Court has seen two, and only very recently, and perhaps only in response to significant federal district court cases delving into uncertain areas of Georgia state law. Illinois has seen one, well over ten years ago.

Second, even when state courts of appeals (at least in Georgia and Illinois) hear data breach cases, they are reluctant to recognize an independent duty to safeguard personal information founded in common law tort principles. Rather, their opinions indicate (often explicitly) that the legislature is the appropriate institution to recognize the duty. This (tentative) trend among the judiciary casts

93. *Id.* at 17. While the reliance on Section 1798.81.5 of the California Civil Code and Section 5 of the Federal Trade Commission Act are common (as is reliance on California's UDAP law, CAL. BUS. & PROF. CODE § 17200), reliance on industry standards is not. It is typically cabined to payments processing platform-related breaches, as they are governed by Payment Card Industry Data Security Standard (PCI DSS).

94. *See, e.g.*, *The First Wave of CCPA Allegations Makes Its Way into a New Data Breach Class Action Against Salesforce and Hanna Andersson*, MINTZ (Feb. 6, 2020), https://www.mintz.com/insights-center/viewpoints/2826/2020-02-05-first-wave-ccpa-allegations-makes-its-way-new-data [https://perma.cc/6VMD-J7SB].

95. Note: this argument could also be leveraged against the Section 1798.81.5 claim.

doubt on the efficacy of certain proposals urging judicial rather than legislative solutions for recognizing and enforcing a duty through common law tort principles.[96]

Third, Georgia, California, and Illinois federal courts have seen many data breach cases, far more than state courts.[97] They have also been more willing to comment on whether the state common law recognizes a duty. Perhaps this is because their precedent is nonbinding and thus less impactful on shaping state law than that of a state appellate court. Or perhaps federal courts feel the need to decide the issue because they face immense pressure to resolve such massive cases. Additionally, it is possible that both the plaintiffs and the locus of the harm were so detached from Georgia itself that the district court felt less tethered to Georgia's common law. Indeed, *Home Depot* and *Arby's* aggregated tens of thousands of people; *Equifax* had tens of millions. Punting the issue is impossible (as a district court) and waiting for the legislature to act may appear less feasible given the relative frequency with which Georgia district courts see data breach issues. Although, one must query why it did not certify the question to the state supreme court.

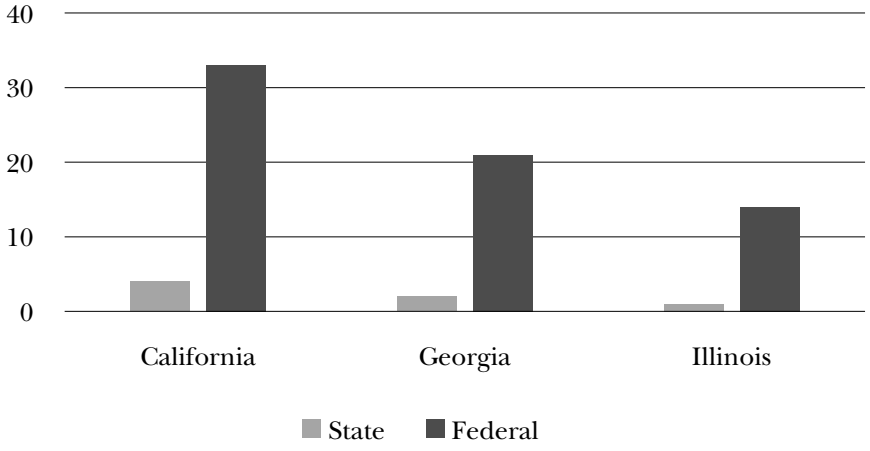

Figure 2: Proportion of data breach cases dealing with duty to safeguard PII in state and federal courts.

96. *E.g.*, Solow-Niederman, *supra* note 4; Jack Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11, 21 (2020); Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793 (2022).

97. Particularly those of Georgia and California. *See infra* Figure 2. The relative dearth in Illinois federal courts could be due to the repercussions of the Seventh Circuit's strong stance against recognizing a duty in *Community Bank of Trenton*.

Figure 2 documents the proportion of cases in federal versus state courts that discuss a duty to safeguard PII. The data and methodology behind Figure 2 were discussed sporadically throughout the individual state case studies but are worth briefly consolidating and elaborating. Since California has a specific statute dealing with the duty to safeguard personal data (Section 1798.81.5 of the California Civil Code), I searched LexisNexis by this statutory provision and filtered California state courts and federal courts sitting within California (Ninth Circuit and district courts) in turn. This generated forty-seven cases in federal court and six cases in state court as of April 2021. Since Georgia and Illinois do not have a statute on point, I searched "data breach."[98] Then, I removed duplicative and unpublished cases as well as cases that did not mention or analyze whether the defendant had a duty under that state's statutory or common law to safeguard the personal information exposed due to the breach. This latter interpretive component is a shortcoming in the reliability/replicability of the Georgia and Illinois figures and could benefit from replication through a more standardized methodology.[99]

That said, the limitations of the methodology err toward understating the magnitude of the disparity rather than exaggerating it. Three out of the four California state cases merely reflect consent orders with the Attorney General. In other words, the state court did not, and did not have to, perform any actual tort analysis, and the case generated no binding precedent because it was a settlement. Additionally, the share of federal court cases in the sample is under-representative because other federal courts interpret Georgia state law.[100]

98. For Georgia, this returned seven hits in state courts and ninety-three hits in the Eleventh Circuit and district courts sitting in Georgia. For Illinois, this returned eleven hits in state courts and 119 hits in the Seventh Circuit and district courts sitting in Illinois.

99. Casting a wide net through a broad search parameter leads to more false positives, which puts more weight on manual filtration on the back end. Searching "data breach" leads to an array of case types: customer negligence claims, shareholder derivative suits, criminal suits against employers who failed to disclose the breach, and breach of contract claims, among others, in combination or alone. I included only cases that engaged in legal analysis (including flippant rejections) of a duty to safeguard personal information. Cases excluded often involved breach of contract claims where the analysis dealt exclusively with contract interpretation, or criminal cases where the analysis centered not on the breach but on the defendant's conduct and mens rea with regards to covering it up.

100. On the other hand, there are limitations to using LexisNexis. (Pacer would have been ideal, but I did not have access.) There may be a significant share of state court cases whose complaints were filed and then settled out before mak-

Fourth, and finally, whether the claim is brought in a state or federal forum may determine the outcome of data breach cases involving common-law negligence claims. This is not the case in California and Illinois, where the state and federal courts sitting in diversity jurisdiction are aligned, at least on the narrow issue of duty. But the Georgia case study reveals a discord between the *Home Depot*, *Arby's*, and *Equifax* line of federal court cases that recognize a duty, and the state law cases, *McConnell* and *Collins*, which are, at best, hesitant to recognize such a duty and, at worst, (through their dicta) inclined not to recognize a common law tort duty. Granted, the case law has not completely diverged, but a plaintiff bringing a negligence claim in a Georgia district court will be able to cite a foundation of supporting cases in the same forum while a Georgia state court might be less persuaded.[101] An alternative conceptualization of this observation is that there is a lag time effect where federal district courts are able to build a body of case law before the state appellate courts are willing (or forced) to weigh in.

E. Zooming Out: Case Studies as Representative of National Heterogeneity

One major limitation of this Note is the small and targeted sample. Three state case studies are a far cry from a representative sample of state approaches, and the sample was far from random: Georgia, Illinois, and California were picked *because* they were different from each other. But the risk this Note runs by using a small sample and narrow topic is not to overexaggerate the heterogeneity of our fifty-state framework but to grossly underemphasize it. If we zoom out, the state of the nation is a far more fraught and complicated patchwork of legal perspectives than that reflected by three case studies, arranged on a spectrum from whether the state does or does not provide a duty, using a binary conception of duty.

Consider the states whose legislatures have, like California, recognized a tort duty to safeguard personal information. California, Massachusetts, Ohio, and Virginia, for instance, all have non-trivi-

---

ing it into Lexis. But again, this has no bearing on the development of binding law and often has no bearing on whether the court had to engage with any of the legal issues.

101. *See* Samuel Issacharoff & Florencia Marotta-Wurgler, *The Hollowed Out Common Law*, 67 UCLA L. REV. 600, 628 (2020) (noting that "rulings of federal courts sitting in diversity jurisdiction are treated as a one-off development, without binding effect on state courts or other courts"). *But see* Collins v. Athens Orthopedic Clinic, P.A., 837 S.E.2d 310, 315 n.4 (Ga. 2019) (explicitly stating its influence on federal district court decisions).

ally different definitions of personal information,[102] covered entity thresholds,[103] and substantive compliance requirements.[104] Their enforcement provisions also vary (typically around whether to provide a private right of action and statutory damages) such that a business's litigation risk and the expected value of the suit will be wildly different depending on the jurisdiction.[105] As a result, if we

102. *See* CAL. CIV. CODE § 1798.81.5(d)(1)(A) (Deering 2023) (requiring unencrypted first and last name in combination with a social security number, unique government-issued identification number (e.g., driver's license number, tax identification number, passport), financial account or credit card number (if combined with required password or security code), medical or health insurance information, or biometric data); VA. CODE ANN. § 59.1-575 (2023) (defining personal data as "any information that is linked or reasonably linkable to an identified or identifiable natural person [not including de-identified or publicly available information]"); OHIO REV. CODE ANN. § 1349.19(A)(7)(a) (LexisNexis 2023) (defining personal information to include unencrypted first and last name in combination with a social security number, driver's license number, or account/credit card number if combined with a security code); 201 MASS. CODE REGS. 17.02 (LexisNexis 2023) (same as Ohio but making no mention of encryption and not requiring a security code along with credit card info).

103. The Virginia Consumer Data Protection Act (CDPA), for example, has a higher threshold number of Virginia residents whose personal information is processed by the entity than California (100,000 versus 50,000); Virginia also, alternatively, combines number of people processed with gross annual revenue, whereas California has a flat revenue provision. *Compare* VA. CODE ANN. § 59.1-576(A) (2023), *with* CAL. CIV. CODE § 1798.140(c). Ohio, on the other hand, has a much lower threshold for application, covering for-profit and non-profit businesses (unlike California and Virginia) that "access[ ], maintain[ ], communicate[ ], or process[ ] personal information or restricted information in or through one or more systems, networks, or services located in or outside this state." OHIO REV. CODE ANN. § 1354.01(A)–(B).

104. Ohio, for instance, provides a compliance safe harbor, where a business is granted immunity if it can demonstrate compliance with an "industry recognized framework" such as NIST special publication 800-171; special publication 800-53; FedRAMP; the "center for internet security critical security controls for effective cyber defense" (recall the California AG's data breach report); or ISO 27000 family standards. OHIO REV. CODE ANN. § 1354.03(A)(1). Virginia, on the other hand, has not indicated how to interpret its reasonableness standard found in Section 59.1-574(A)(3) of the Code of Virginia. Massachusetts, perhaps most rigorous of them all, requires "[e]very person that owns or licenses personal information about a resident" to have a written comprehensive information security program; the statute meticulously details several administrative and technical components that must be described in the program. 201 MASS. CODE REGS. 17.03–04.

105. Virginia only allows the AG to enforce the statute and impose penalties up to $7,500; it further provides a 30-day cure provision identical to the CCPA's. VA. CODE ANN. § 59.1-584. Ohio also does not provide a private right of action. OHIO REV. CODE ANN. § 1354.04. The Massachusetts data breach statute makes no mention of whether it affords or prohibits a private right of action, but courts have typically rejected private causes of action to enforce the statute. *See* Justin H. Dion & Nicholas M. Smith, *Consumer Protection—Exploring Private Causes of Action for*

want to arrange states on a spectrum based on maximum penalties for failing to abide by the duty, California would in some respects be leagues beyond the other data protection laws. On the other hand, its definition of personal information, its cure provision, and its scope threshold mean that some business models may be able to avoid liability under the CCPA but not under the Massachusetts, Ohio, or Virginia laws.

States like Georgia or Pennsylvania, where federal courts sitting in diversity have recognized a duty, lie along this spectrum.[106] For a defendant, the expected cost of a lawsuit is, in many ways, much higher in these states than in states where a duty to safeguard personally identifiable information is recognized by statute but enforceable only by the Attorney General. To add more uncertainty to the mix, the story of Georgia (and Pennsylvania, which is not much different) shows that we are not just looking at fifty potentially different state regimes; we are looking at fifty state court regimes *plus* the federal regimes that have generated case law interpreting the law of those states and reached different conclusions (or at least, created different bodies of settled and unsettled issues).

Furthermore, even within the category of states where the duty is defined only through the common law, a business must consider the myriad ways that the duty can be limited, cabined, and expanded. Is the duty premised on the existence of a special relationship between the parties? Does it embody the proposition in Section 319 of the Restatement (Second) of Torts which extends the special relationship to third parties under certain circumstances? Does the case law stress the defendant's awareness of the risk when it recognizes a duty? To what extent is the court willing to wade into breach analysis, and how might it differ? These qualifications popped up in the case studies but were glossed over in favor of a clearer and binary, albeit reductionist, narrative tracking the recognition of a duty or lack thereof. The same questions must be asked when engaging in the federal court analysis, along with the all-important issue of standing (which plagues courts on both levels

Victims of Data Breaches, 41 W. NEW ENG. L. REV. 253, 281 (noting that the "apparent lack of an individual cause of action leaves enforcement solely in the hands of the attorney general").

106. *See In re* Rutter's Data Sec. Breach Litig., 511 F. Supp. 3d 514, 529–30 (M.D. Pa. 2021) (upholding plaintiffs' negligence claim and finding that defendant's "affirmative act of retaining credit and debit card information created a risk of foreseeable harm from unscrupulous third parties" sufficient to recognize a common law duty under Pennsylvania law).

on this subject matter, particularly in terms of injury-in-fact and causation).

There is, of course, one end of the spectrum where states do group together uniformly: where there is explicitly no duty to safeguard personal information. Those are the states like Illinois, Missouri,[107] and Washington (although Washington has been trying to enact a CCPA-esque statute for the past three years).[108] There, a business can rest assured that it owes no duty, in federal or state court, at least until the legislature acts.

Indeed, the call for legislative action has been a trend among the state appellate court opinions as discussed above.[109] Georgia and Illinois courts, at least, have been unwilling to reconcile data breaches with common law negligence theory without the legislature's blessing, and some federal courts (depending on the circuit) refuse to "break new ground in state law."[110] For better or worse, state legislatures are beginning to oblige. But that, too, raises a host of problems, including interest group capture (recall the motivations behind California's Prop 24) and lack of conformity across legislative approaches.

All in all, this tattered patchwork surrounding a legal duty to safeguard personal information begs the question of federalization, which leads us to Part II and the central normative question of this Note.

II.
FEDERALISM, FEDERALIZATION, AND DATA BREACHES

Just because states deal with data breaches differently does not mean that the rules governing data breaches should be federalized. American democracy arguably thrives on inefficiency and fric-

107. *See* Cmty. Bank of Trenton v. Schnuck Mkts., Inc., 887 F.3d 803, 818 (7th Cir. 2018) (finding silence on the part of Missouri state courts on the topic of duty and reasoning that the state courts would likely find no common law duty).

108. *See, e.g.*, Buckley v. Santander Consumer USA, Inc., No. C17-5813, 2018 U.S. Dist. LEXIS 53411, at *15 (W.D. Wash. Mar. 29, 2018) (rejecting plaintiffs' allegations that "Santander's failure to maintain adequate security implicate a common law legal duty that could support a negligence claim").

109. *E.g.*, McConnell v. Dep't of Labor, 814 S.E.2d 790, 799 (Ga. Ct. App. 2018); Cooney v. Chi. Pub. Schs., 943 N.E.2d 23, 27 (Ill. App. Ct. 2010).

110. Dinerstein v. Google, LLC, 484 F. Supp. 3d 561, 595 (N.D. Ill. 2020) (quoting Sabrina Roppo v. Travelers Com. Ins. Co., 869 F.3d 568, 596 (7th Cir. 2017)).

tion.[111] It is therefore important to contextualize data breaches and the information derived from the case studies within the *federalism* versus *federalization* discourse to examine the grounds on which federalization can be justified and the extent to which federalism should be preserved.

A. The Federalism vs. Federalization Debate

Courts and legal scholars typically raise three arguments in favor of constraints on centralized federal power:

1. States can act as laboratories of democracy, testing novel legal or social experiments without risking national fallout if they go wrong.[112]
2. Allowing states the freedom to decide their substantive law enhances democratic participation and preserves political accountability.[113]
3. Diverse state stances allow people to organize their lives according to their preferences, which increases aggregate social welfare.[114]

These classic federalism arguments,[115] when leveraged by courts, are rooted in notions of history and attention to a structural balance of power evocative of Hamilton's "local administrations for local purposes" and his admonition of the "oppressive use of [federal] power" to decide traditionally local functions.[116]

Arguments for federalization, in contrast, typically appeal to principles of efficiency and coordination.[117] The central question

111. *See* Barry Friedman, *Valuing Federalism*, 82 MINN. L. REV. 317, 388 (1997) (arguing that "American democracy rests explicitly on the idea that there is a benefit to inefficiency"); *see also* Heather Gerken, *The Taft Lecture: Living Under Someone Else's Law*, 84 U. CIN. L. REV. 377 (2018) (arguing that spillovers—by producing friction and exposure to different viewpoints—are not only inevitable but a valuable part of democratic society).

112. *See* Samuel Issacharoff & Catherine M. Sharkey, *Backdoor Federalization*, 53 UCLA L. REV. 1353, 1355 (2006).

113. *See* Friedman, *supra* note 111, at 389–95.

114. Michael W. McConnell, *Federalism: Evaluating the Founders' Design*, 54 U. CHI. L. REV. 1484, 1493–94 (1987) ("So long as preferences for government policies are unevenly distributed among the various localities, more people can be satisfied by decentralized decision making than by a single national authority.").

115. *See* Betsy Grey, *The New Federalism Jurisprudence and National Tort Reform*, 59 WASH. & LEE L. REV. 475, 511 (2002) (noting that the Supreme Court traditionally cites these three values of federalism).

116. THE FEDERALIST NO. 32 (Alexander Hamilton).

117. *See* Friedman, *supra* note 111, at 405 (pointing out that the mass of federalization scholarship, typically populated by political economists, focuses on efficiency-based arguments).

of federalization literature examines the circumstances under which efficiency concerns outweigh the countervailing interests and benefits of state sovereignty. To answer this question, Samuel Issacharoff and Catherine Sharkey identify two animating principles behind federalization: (1) the desire for uniformity of regulation, and (2) the desire to prevent states from exporting the negative consequences of their experiments onto other states.[118] Within these two vertical (national market coordination) and horizontal (policing state conduct) categories, we can organize other federalization arguments to sharpen the contours around the types of goods or conduct that may warrant federalization.

On the vertical side, the desire for national market coordination is premised on the good or conduct being inherently interstate or national. Typical examples include interstate highways and the military.[119] But it may also extend more broadly to situations where the transaction costs of fifty regulatory regimes would destroy economies of scale and prevent the good from being produced at all (or at a welfare-maximizing price). It could also reach beyond commerce to the context of rights—where Congress or the Supreme Court recognizes a fundamental right beyond the states' power to curtail.[120]

A final way to recognize that conduct may be national is through a procedural lens—based on how the right develops and gets enforced. When the vast majority of cases of a certain type are brought in federal court (e.g., by CAFA), the substantive development of the common law consequently moves to federal court and federal standardization.[121] Such movement may indicate that state courts can no longer handle the litigation of that issue—be it mass tort cases like asbestos, electronic contracts cases, or products liability lawsuits with uniform nationally distributed goods—and so the substantive law should be federalized to prevent issues arising from unsettled law.[122]

On the horizontal side, there are many ways to conceptualize instances that require the prevention of spillover effects from intra-

118. Issacharoff & Sharkey, *supra* note 112, at 1369.

119. Friedman, *supra* note 111, at 406–07, 407 n.374.

120. *See id.* at 319 (justifying certain federalization arguments as recognizing the need to "provide a national floor on fundamental rights").

121. For an elaboration of this theory and effect in the context of electronic contract cases, see Issacharoff & Marotta-Wurgler, *supra* note 101, at 600–01.

122. *See id.* at 601 (arguing that federal courts deciding state substantive law issues creates a problem where no apex court can conclusively define the law of any jurisdiction because the interpretations of state law determined by federal courts sitting in diversity do not bind state courts).

state experiments. The classic example is the pollution problem—where "individual actors [(states)] face incentivizes to engage in harmful behavior because the benefits are localized to them . . . while the burdens are externalized to downstream communities."[123] Another related idea is the tragedy of the commons problem, where a state is disincentivized to provide the right because if it does, a parade of outsiders will flood the state and leech off of its benefits.[124] A similar but inverse horizontal federalization issue is what we might call a "first-mover penalty"—where states are disincentivized to provide a right/good because businesses and investment will flee to other states.[125]

Because arguments for federalism and federalization rest on wholly different premises, they often speak past each other in debate.[126] But it is also possible to think of these federalization arguments as diluting the benefits of state sovereignty and attacking the premises on which federalism arguments rely. States cannot effectively operate as laboratories of democracy when they are disincentivized to experiment due to free-rider or tragedy of the commons concerns. Nor can state citizens have better democratic accountability on a state level when they cannot outvote the out-of-state poli-

123. Issacharoff & Sharkey, *supra* note 112, at 1369.

124. An example here is healthcare. *See* Nat'l Fed'n of Indep. Bus. v. Sebelius, 567 U.S. 519, 594–95 (2012) (Ginsburg, J., dissenting) ("States cannot resolve the problem of the uninsured on their own. Like Social Security benefits, a universal health-care system, if adopted by an individual State, would be 'bait to the needy and dependent elsewhere, encouraging them to migrate and seek a haven of repose.'" (quoting Helvering v. Davis, 301 U.S. 619, 644 (1937))).

125. This phenomenon has a few corollaries. First, states will not experiment because public officials are risk-averse and fear trying something that becomes unpopular and causes them to lose office. *See* Susan Rose-Ackerman, *Risk Taking and Reelection: Does Federalism Promote Innovation?*, 9 J. LEGAL STUD. 593, 594 (1980). *But see* Friedman, *supra* note 111, at 398 (arguing that "[e]xperimentation is not an option, it is a way of life" to counter the premise that public officials are "sitting at a desk carefully calculating" the risk of a given proposal). Second, states will have a difficult time implementing morally desirable programs that have high economic detriments if other states do not follow suit. *Id.* at 408 (discussing this idea in the context of the struggle to eliminate child labor).

126. *See* Thomas W. Merrill, *Preemption in Environmental Law: Formalism, Federalism Theory, and Default Rules*, *in* FEDERAL PREEMPTION: STATES' POWERS, NATIONAL INTERESTS 166, 168 (Richard A. Epstein & Michael S. Greve eds., 2007) (commenting that "[o]ne person's healthy regional diversity is another's interstate externality"); *see also* Friedman, *supra* note 111, at 405 (pointing out that the mass of federalization scholarship "has been ignored by judges, constitutional lawyers, and constitutional theorists" and hypothesizing that it is because "the constitutional plan does not seem to require the question [of efficiency] be answered, or even to be asked at all").

ticians whose legislation caused their polluted water. Similarly, state courts cannot effectively build out substantive liability rules when all litigation on the topic is in federal court. Figure 3, below, arranges these countervailing arguments for federalism and federalization against each other.

Federalism	**Federalization**
Laboratories of democracy	Inherently national good/ standard First mover penalty Free rider problem Spillover effects Forum predominance
Democratic accountability	Spillover effects
Decentralized resources and enforcement	State cannot handle the litigation, national agenda
Individual choice	Desire to recognize a fundamental right
Insulation from (national) interest group capture	Insulation from (state) interest group capture

Figure 3: Values of Federalism vs. Countervailing Values of Federalization

B. Federalism vs. Federalization in the Context of Data Breaches

1. Laboratories of Democracy and Experimentation

Federalization of the substantive law determining liability for data breaches appears inevitable given the ever-increasing number of bills that have cropped up in Congress over the past few years.[127] The problem impeding congressional action seems to be the content, not the desire. Which types of businesses should it cover? Should there be a private right of action? What should damages/ penalties look like? How about preemption? In this context, the lab-

127. More than thirty bills have been filed since 2018. *See* Cameron F. Kerry & Caitlin Chin, *How the 2020 Elections Will Shape the Federal Privacy Debate*, BROOKINGS (Oct. 26, 2020), https://www.brookings.edu/blog/techtank/2020/10/26/how-the-2020-elections-will-shape-the-federal-privacy-debate [https://perma.cc/59FH-VMM3]. *But see* Solow-Niederman, *supra* note 4 (arguing that legislative inertia is likely to hamper a timely solution).

oratories of democracy approach envisions states as sandboxes for some of these contested variables, with the most promising model informing the federal framework.[128]

The immense heterogeneity in state approaches (as discussed in Part I) suggests that, at least in the enforcement context, laboratories of experimentation will be able to provide some helpful data. Not only do the states generate the same topical debates as the federal forum,[129] but there seems to be some diversity in state enforcement models. In Virginia, Massachusetts, and Ohio, only the Attorney General can enforce the data breach duty to safeguard, while California's CPRA has retained a private right of action and imposes significant statutory damages.[130] While this diversity creates a wide range in expected costs of litigation across states (and a big headache for businesses), it could provide useful data for a federal regime on optimal deterrence values. Indeed, over the next few years, the on-the-ground ramifications of the different state enforcement models should provide information that will help in designing a federal scheme.[131]

---

128. Some scholars argue that this idea of cooperative federalism is not necessarily anti-federalism despite its ultimate ends of eventually adopting a national "best" solution. *See* Abbe Gluck, *Nationalism as the New Federalism (and Federalism as the New Nationalism): A Complementary Account (and Some Challenges) to the Nationalist School*, 59 ST. LOUIS U. L.J. 1045, 1046 (2015) (attributing this proposition to Heather Gerken).

129. In essentially every case, concerns about overregulation through a flood of nuisance suits weigh against an overreliance on the limited powers of the state attorney general. *See, e.g.*, Seattle Times Ed. Bd., *Pass Washington Privacy Bill with Attorney General Enforcement*, SEATTLE TIMES (Mar. 4, 2020), https://www.seattletimes.com/opinion/editorials/pass-washington-privacy-bill-with-attorney-general-enforcement/ [https://perma.cc/752M-WU45] (warning that a private right of action would lead to "gotcha lawsuits" and "potentially creat[e] a flood of litigation"); H. COMM. INNOVATION, TECH. & ECON. DEV., SECOND SUBSTITUTE HOUSE BILL REPORT 2SSB 6281, at 8–9 (Wash. 2020) (describing public arguments in support of and opposed to adding a private right of action); Edelman, *supra* note 74 (describing the same debate leading up to the CCPA's passage); CAMERON F. KERRY ET AL., BRIDGING THE GAPS: A PATH FORWARD TO FEDERAL PRIVACY LEGISLATION 19–20 (Brookings 2020) (raising the same concerns on the federal level).

130. *See supra* Part I.E; *see also supra* note 105.

131. The same argument can be made for many of the differences in state approaches described in Part I.E. Should the federal legislation exempt nonprofits like in California, or has that created a loophole that the California legislature and other policy experts are now trying to close? What is the optimal threshold for exempting businesses that are too small to burden with the threat of costly litigation—should we combine a revenue provision with the amount of data processed (Virginia) or not (California)? Should our definition of personal information be narrow (California) or broad (Ohio)?

To bolster the federalism point further, many of the federalization camp's strongest concerns have less force in the data breach context. One example is spillover effects. More stringent state duties of care around data arguably produce only positive externalities. As then-California AG Kamala Harris mentioned in the 2016 Data Breach Report, "[by implementing a less-protective federal regime], residents of other states would lose the benefit they now enjoy from the highest-common-denominator approach many organizations take in multi-state breach responses, in effect affording California-level protections to residents of all states."[132] One could rebut that it imposes increased and unwanted operational costs on out-of-state businesses. But the covered entity provisions of state data breach legislation are typically such that the costs are felt only if the business engages in substantial amounts of commerce with residents of the state—and only residents of that state are able to sue, which cabins the amount of spillover.[133]

The pollution analogy, then, would supposedly operate in situations where states with lax data protection regimes (e.g., Illinois) gained a benefit by attracting businesses who then harmed out-of-state residents (e.g., Californians) through their lax standards that caused a data breach. But in theory, an Illinois business would not be able to impose harm on California residents through a data breach without facing the repercussions of a suit under the CPRA (assuming it meets the covered entity requirements). Notably, that would also diminish the value to the state of being a compliance haven. Say the affected out-of-state residents live in Missouri (no duty) rather than California. In that case, they will have no ability to sue the Illinois business, but since Missouri had no duty anyway, Illinois has not generated a negative externality relative to Missouri. And since their legal standards are aligned, Illinois has not gained any upstream benefits relative to Missouri.

Unlike the spillover effects argument, the free-rider theory may hold greater weight against the laboratories of experimentation idea. Under this argument, state legislatures would be disincentivized to recognize a duty for fear of losing business investment. Indeed, Silicon Valley businesses have purportedly begun migrating to Texas, although confounding variables abound.[134] And an obvi-

132. CAL. DATA BREACH REP., *supra* note 56, at 5.

133. *But see* Class Action Compl. at 3, Barnes v. Hanna Andersson, LLC, No. 20-cv-00812 (N.D. Cal. Feb. 3, 2020) (using the CCPA as a hook to gain settlement for out-of-state residents).

134. Lizette Chapman, *Silicon Valley Is Flooding into a Reluctant Austin*, BLOOMBERG (Apr. 8, 2021), https://www.bloomberg.com/news/articles/2021-04-

ous rebuttal to this argument is the evidence of a growing amount of state data protection legislation. However, the fact that California, Virginia, Massachusetts, and Ohio all have data protection statutes may disincentivize further statutory experimentation among other states if they feel like they can either free-ride off of those stringent laws *or* free-ride off of their legislative construction. Indeed, Kamala Harris anticipated (and invited) the former in her above comment; and as to the latter, other states' legislative proposals do appear to closely track the CCPA.[135] This could certainly limit the heterogeneity of models, although a sort of federalized uniformity would eventually develop all the same through the copycat legislation.

Another problem with laboratories of experimentation in the context of data breaches is the stagnation of state common law development despite the absence of state statutory schemes.[136] Not only do state courts not have the chance to hear many data breach cases, but federal courts also fail to move the ball forward due to their lack of binding effect, Article III standing issues, or general reticence in developing state common law. The result—as Professors Issacharoff and Marotta-Wurgler conclude while researching similar effects in the domain of electronic consumer contracts—is an unstable and inconclusive body of law.[137]

The issue is worse than mere instability; it is also the inflated importance of outdated cases with inaccurate analogies due to the fact that scarcity fails to breed nuance. Recall that both *Cooney* and *McConnell* dealt with in-state residents, erroneous disclosure by the government, and no reasonable expectation of a "breach." Despite their influence in defining Georgia and Illinois law, respectively,

---

08/austin-texas-ready-or-not-becomes-hot-spot-for-silicon-valley-transplants [https://perma.cc/5JP2-JF97]. Increased liability for data breaches is one example of the myriad regulations California imposes on businesses that jurisdictions like Texas do not.

135. Gretchen A. Ramos & Darren Abernethy, *Additional U.S. States Advance the Privacy Legislation Trend in 2020*, NAT'L L. REV. (Jan. 27, 2020), https://www.natlawreview.com/article/additional-us-states-advance-state-privacy-legislation-trend-2020 [https://perma.cc/G48J-UYX7] (noting that New Hampshire and Illinois have closely modeled their bills on the CCPA, "adopt[ing] the CCPA's text wholesale in some instances").

136. *See generally supra* Sections I.A–D.

137. Issacharoff & Marotta-Wurgler, *supra* note 101, at 627–28 (describing two "difficulties" arising from federalized common law: (1) "federal courts, unlike state courts, are disabled by *Erie* from creating new common law," and (2) "rulings of federal courts sitting in diversity jurisdiction are treated as a one-off development, without binding effect on state courts or other courts. As a result, the normal hierarchical ordering of the law does not occur").

they do not reflect the predominant fact pattern for data breach cases in their own states.[138] Yet, as we saw in *Community Bank of Trenton*, these cases may determine the rule for data breaches involving more foreseeable risks, for third-party disclosures due to criminal theft, and for far more large-scale activities.

Perhaps the best, or at least most straightforward, argument against the laboratories of experimentation idea is the vertical federalization idea that massive transaction costs are being imposed on an inherently interstate activity. Data breaches are the nearly inevitable byproduct of doing business on the internet, which rarely occurs within a single state's borders. As a result, data storage (and thus data breaches) will often involve residents of multiple states.[139] This is the case regardless of business size or revenue—a blog with a listserv can run into the same compliance hurdles as a multinational corporation. Against this backdrop, compliance becomes a huge problem given that the laws are not only heterogeneous but also because following the most stringent law does not necessarily ensure compliance with the rest.[140] And if we further assume that ex ante business decisions about investment in security are based on estimates of ex post breach costs, what exactly should that ex ante risk calculus look like in such a diverse ecosystem? At best, it will create substantial transactional costs of doing business across states; costs that would otherwise be spent innovating, providing services, or lowering prices.

2. Democratic Accountability and Insulation from Interest Group Capture

The democratic accountability argument is a double-edged one for federalism proponents, at least in the context of data

138. *See supra* Part I.A–B.

139. Surprisingly, there is no good data on this. Verizon's annual Data Breach Investigations Report, a document of talismanic significance in the field, does not offer a breakdown of data breaches by whether victims were from multiple states. *See* VERIZON 2020 DBIR, *supra* note 3.

140. Ohio provides a safe harbor where businesses can show compliance with a stricter (typically federal) regime, but Massachusetts, California, and Virginia do not. And Massachusetts's written information security program requirements do not necessarily match the Center for Information Security's twenty components (California's former and arguably current baseline) much less whatever the emergent CalPPA will decide is optimal. *See supra* Part I.E; *see also* Jerry Jones, *Let's Close the Gap and Finally Pass a Federal Data Privacy Law*, TECHCRUNCH (July 23, 2020, 1:15 PM), https://techcrunch.com/2020/07/23/lets-close-the-gap-and-finally-pass-a-federal-data-privacy-law/ [https://perma.cc/4GC3-VJ9A] ("[State and municipal] data privacy laws will be inconsistent, creating a patchwork of rules based on geography, leading to unnecessary friction and complexity.").

breaches. One cannot argue both that the current state-led system brings government closer to its constituents (and their preferences), and that positive spillover effects exist. If spillover effects exist, then there are state residents spilled upon with no ability to oust the lawmakers generating those effects. Federalization arguably would provide more democratic accountability, then, not less. But since the existence of positive externalities in this area is uncertain, the democratic accountability argument is worth fleshing out a bit further, especially because it touches on the other federalism issues of individual choice and interest group capture.

The California case study is illustrative as an argument both for and against the idea that states grant more democratic accountability.[141] On the one hand, the CCPA generated an immense amount of debate from California citizens, advocacy groups, and companies alike. When the California legislature passed the bill, its constituents knew exactly who had signed and opposed it. They could vote out those lawmakers (or reject the ballot measure) without worrying about other states' citizens.

On the other hand, the CCPA was a complete failure of interest group capture.[142] So much so, that the current iteration of the CCPA—the CPRA—overhauled the law *intentionally* via ballot proposition so it could skirt the procedural protections (and possibility of capture) afforded by the bicameral process.[143] And despite seeming like the apotheosis of local democratic majoritarianism, ballot measures face even greater issues of democratic accountability and interest group capture.[144] Prop 24, which passed through the

141. *See supra* Part I.C.3.

142. *See* Ross, *supra* note 78 (retracting her support of the CCPA despite being one of its primary drafters, because "unfortunately, the law itself—which is a compromise between legislators and many of the influential tech companies in California—is a significantly watered-down version of the original initiative").

143. *See* Edelman, *supra* note 74 (describing that California State Senate Majority Leader, Bob Hertzberg "urged Mactaggart to bypass the legislative process" upon passing the CCPA because "all the business people were [using the legislative process] to cut up our credibility").

144. *See* Caroline Hansen, *The Democratic Paradox of Ballot Measures: In Order to Form a More Perfect Uber?*, EQUAL DEMOCRACY PROJECT, HARV. L. SCH. (Nov. 1, 2020), https://orgs.law.harvard.edu/equaldemocracy/2020/11/01/the-democratic-paradox-of-ballot-measures-in-order-to-form-a-more-perfect-uber/ [https://perma.cc/CVV2-XNUY] (describing how ballot measures have ironically been usurped by corporate interests and used as a "fast and easy way to overturn competitively unfavorable laws passed through the traditional state legislative process").

singlehanded lobbying efforts of a wealthy resident disgruntled by the fruits of democratic compromise, appears to be no different.[145]

Would federalization afford greater democratic accountability, though? Or does it just face the same issues on a larger scale? James Madison argued that the numerosity and viewpoint diversity afforded by federalization make it harder for factionalism and interest group capture to occur than at the state level.[146] While Madison's theory has found some empirical support,[147] it is hard to say for sure.[148] It is also important to recognize that the California legislature, due to its influential status as a tech hub and its reputation as a de facto standard-setter for the country, may suffer from more interest group capture than other state legislatures due to the outsized value received from successful lobbying efforts. To draw a stronger conclusion, it would be worthwhile to examine the effects of interest group capture on the promulgation of other states' data breach laws, such as those in Virginia or Ohio, for example.

Despite the many conditions that make data breaches an intuitively appealing candidate for federalization, running those arguments through the theoretical rationales for and against federalization yields a more conflicted picture. Given the powerful arguments on both sides, pure federalism or pure federalization (i.e., complete substantive and procedural preemption) are not the optimal regulatory strategies for deciding the scope of the duty to

145. *See* Edelman, *supra* note 74 ("The initiative was the brainchild of Alastair Mactaggart, a wealthy San Francisco real estate developer, who had the idea in the shower in 2015 and funded the effort out of pocket."); *see also* Ben Adler, *California Passes Strict Internet Privacy Law with Implications for the Country*, NPR (June 29, 2018, 5:05 AM), https://www.npr.org/2018/06/29/624336039/california-passes-strict-internet-privacy-law-with-implications-for-the-country [https://perma.cc/WCG4-KXT3] (categorizing the CPRA's passage as possible "because a wealthy voter named Alastair Mactaggart leveraged the state's ballot initiative process to bring the American tech industry to its knees").

146. THE FEDERALIST NO. 10 (James Madison).

147. *See* Ryan T. Moore & Christopher T. Giovinazzo, *The Distortion Gap: Policymaking Under Federalism and Interest Group Capture*, 42 PUBLIUS 189, 189 (2012) (arguing that "[e]ven when interest groups capture state policymaking at the same rate as states' national representatives, a 'distortion gap' exists [such that] national policy-making provides more aggregate welfare when voters widely disagree with moderately prevalent strong interest groups").

148. *See* Richard A. Smith, *Interest Group Influence in the U.S. Congress*, 20 LEGIS. STUD. Q. 89, 89 (1995) (providing a meta-analysis of the interest group capture studies and finding that the research presents a more "mixed picture of interest group influence" in Congress).

safeguard PII, at least not while the laboratories of experimentation model continues to hold weight.[149]

We can conclude, too, that *some* federal regulatory scheme would be better than the current fifty-state patchwork. Moreover, congressional action appears imminent regardless of the theoretical merits outlined above.[150]

C. Courts or Regulation?

If there should be a federal statute, how should it divide power between decentralized and centralized litigation/regulation? This is a multidimensional issue, grappling with federalism versus federalization on the one hand and liability versus regulation on the other.[151] From the federalism dimension, preserving laboratories of experimentation requires allowing states to continue to promulgate their own laws and local enforcement models. But if Congress recognizes that some safety standards should exist, or at least that some level of uniformity would be useful (as this Part has argued), then a federal statute should provide a floor that states can surpass, rather than fully preempt state laws.[152]

But we still have the other dimension left to tackle—between litigation and regulation. We can assume that a statute will impose only broad-brush guidelines around safety standards, particularly in a field where the technology and industry standard are ever-chang-

149. This temporal aspect merits emphasis. As time produces more information for courts and agencies, the value of experimentation decreases relative to the value of national uniformity (assuming the underlying good has national market characteristics). As Gary Schwartz commented, surveying the field of products liability, "[a] time arrives for more mature and experienced decision making. After thirty years with products liability at the state level, that time has probably come." Catherine M. Sharkey, *Products Liability Preemption: An Institutional Approach*, 76 GEO. WASH. L. REV. 449, 483 (2008) (quoting Gary T. Schwartz, *Considering the Proper Federal Role in American Tort Law*, 38 ARIZ. L. REV. 917, 930 (1996)).

150. *See* KERRY ET AL., *supra* note 129, at 4 (describing the ever-increasing pressure and number of data privacy bills in Congress).

151. *See* Sharkey, *supra* note 149, at 480 (using a helpful table to plot this multidimensional issue).

152. From a policy perspective, this middle route is more practical, too, in the sense of getting a bill passed. *See, e.g.*, Cristiano Lima & John Hendel, *California Democrats to Congress: Don't Bulldoze Our Privacy Law*, POLITICO (Feb. 21, 2019), https://www.politico.com/story/2019/02/21/congress-data-privacy-california-1185943 [https://perma.cc/LMD3-XAPQ] (noting the California House delegation's animosity towards full substantive federal preemption). The Consumer Online Privacy Rights Act (COPRA) advocates for this federal floor model: Section 302 preempts "directly conflicting" state laws, but a law will not be considered "in direct conflict if it affords a greater level of protection" than COPRA. *See* KERRY ET AL., *supra* note 129, at 16.

ing. Which sphere, then, should control the development of those substantive requirements? Deciding on the optimal mix of ex post liability rules and ex ante regulation is a fraught process,[153] and the privacy/data breach space is no exception.[154] But scholars have laid out some guideposts to navigate these murky waters.

Economist and legal scholar Steven Shavell provides four factors to consider when deciding between ex post liability rules and ex ante regulation: (1) Who has a better understanding of the risk-risk tradeoffs inherent in the regulated entity's particular activities? (2) Are private parties able to pay for the harms they cause? (3) Are private parties able to escape suit for their harms? (4) What are the respective administrative costs of the tort system versus direct regulation?[155] Other scholars have added considerations based on perceived gaps in the Shavell framework, including (5) the likelihood of interest group capture, (6) the extent to which compensation should be prioritized over deterrence, (7) path dependence, from both a federalism and institutional perspective, and (8) the novelty of the relevant technology.[156]

Eight factors are a lot to work through, but some need less time than others in the context of data breaches and have already been discussed at least in part. The likelihood of interest group capture, for instance, is a known risk on the legislative front, and there is at least a moderate risk of agency capture, too, due to the wealth and power of the tech lobby, the asymmetry of repeat defendants versus one-shot plaintiffs,[157] and the possibility of regulatory arbi-

153. *See* Sharkey, *supra* note 149, at 452 ("The difficulty, then, is how to discern the appropriate sphere for federal regulation, a difficulty only exacerbated by the modern world of dual state common-law and federal regulatory systems addressing similar problems.").

154. *See* Cohen, *supra* note 6, at 3 (noting that there is "less unanimity" among federal privacy bills with regards to picking an enforcement mechanism between private rights of action and public enforcement litigation).

155. Steven Shavell, *Liability for Harm Versus Regulation of Safety*, 13 J. LEGAL STUD. 357, 358–64 (1984).

156. *See* Sharkey, *supra* note 149, at 482 (noting that the Shavell framework fails to consider interest group politics and regulatory capture); Catherine Sharkey, *Tort as Backstop to Regulation in the Face of Uncertainty*, JOTWELL (Nov. 26, 2013), https://torts.jotwell.com/tort-as-backstop-to-regulation-in-the-face-of-uncertainty/ [https://perma.cc/RN6C-BMRZ] (reviewing Thomas W. Merrill & David M. Schizer, *The Shale Oil and Gas Revolution, Hydraulic Fracturing, and Water Contamination: A Regulatory Strategy* (Colum. L. and Econ., Working Paper No. 440, 2013)) (adding these last four factors).

157. That said, the class action plaintiffs' bar may end up being a repeat player, too, if these cases end up aggregated in class actions or multi-district litigation, as is likely given their characteristics and the current trend. *See* Elizabeth Chamblee Burch & Margaret S. Williams, *Repeat Players in Multidistrict Litigation:*

trage given the jurisdictional overlap of many tech companies' activities.[158]

The ability of private parties to pay (the second factor) and compensatory versus deterrent interests (the sixth factor) are conditional and clear-cut, respectively. Actual damages are typically minimal or speculative for these underlying privacy violations (hence the myriad standing issues), but the introduction of statutory damages could—as discussed in Part I.C—lead to bet-the-company lawsuits depending on their valuation and structure. This means that the second factor will not help us choose between regulation and liability. But the sixth factor leans heavily towards deterrence (and thus ex ante regulation) given the current mismatch between desired behavior (better data security) and nominal actual damages of privacy violations.[159]

Escape (the third factor) is a tough question. Every state imposes data breach notification requirements, but it is hard to say (for obvious reasons) the extent to which data breaches go unreported. Once they are reported, however, the privacy class action plaintiffs' bar appears rather active. Article III standing issues are perhaps the most straightforward way that companies are able to "escape" consumer suits following data breaches. But then again, the imposition of a federal statutory right of action could cure the standing problem and close this avenue of escape, thus favoring litigation and liability rules.[160] From another angle, "escape" from consumer suits arguably poses a diminished concern when the individual harm suffered is so small.

1. Differential Knowledge

Differential knowledge refers to who has better expertise or access to information. Generally, this first factor favors liability rules, under the reasonable assumption that private parties understand their own costs and benefits of engaging in a risky activity better

The Social Network, 102 CORNELL L. REV. 1445, 1445–46 (2017) (employing social network analysis to find that "a key group of attorneys maintained their elite position within the network," on both defendant and plaintiff sides).

158. *See generally* Elizabeth Pollman, *Tech, Regulatory Arbitrage, and Limits* (Eur. Corp. Governance Inst., Working Paper No. 455, 2019) (discussing the presence and limitations of regulatory arbitrage in the tech industry).

159. *See* Cohen, *supra* note 6, at 19 (noting that the consumer benefits of monetary awards would amount to "a few dollars to each affected consumer").

160. *See* Uzuegbunam v. Preczewski, 141 S. Ct. 792, 802 (2021) (holding that "a request for nominal damages satisfies the redressability element [necessary for Article III] standing where a plaintiff's claim is based on a completed violation of a legal right").

than regulators do.[161] This assumption is also bolstered in the data breach space where—at least for an omnibus baseline safety standard—a regulator would have to understand the risk-risk tradeoffs of a wide swath of covered entities from small to large businesses, since businesses of all sizes and industries store personal data online. Given this premise, it is also reasonable to assume that each covered entity will have a very different profile of available resources, quantity and quality of sensitive data stored, and risk of breach. Thus, the inquiry of what exactly is "reasonable" data security will be highly case—and fact—specific, and businesses will be much better positioned to evaluate those tradeoffs than a regulator. Relatedly, standards will be favored over rules, and courts will be better positioned to deal with fact-dependent reasonableness inquiries around those standards than ex ante regulation.[162] Indeed, this logic may explain the FTC's historic approach to enforcing data breaches according to a notoriously vague reasonableness standard and refusal to promulgate more specific guidance.[163]

On the other hand, there is reason to doubt the premise that businesses are actually better positioned to understand the risk-risk tradeoffs of failing to implement a given cybersecurity protocol. Small and medium-sized businesses often lack the resources and expertise to understand their cybersecurity risks, including the expected valuation of a breach, and fail to engage in basic cyber hygiene.[164] Even among Fortune 500 businesses, only 62% have a

161. *See* Sharkey, *supra* note 149, at 481.

162. *See* Richard Posner, *Regulation (Agencies) versus Litigation (Courts): An Analytical Framework*, *in* REGULATION VS. LITIGATION: PERSPECTIVES FROM ECONOMICS AND LAW 11, 14 (Daniel P. Kessler ed., 2010) (describing how ex ante regulation "buys precision at the cost of excluding case-specific information that the promulgators of the regulation either did not anticipate or excluded in order to keep the regulation simple . . . . Standards . . . versus rules . . . allow much more information to be considered in particular cases"). Posner also notes that ex post regulation provides "more information, including up-to-date and case-specific information, and it is screened and weighed more carefully because it is presented in a contested proceeding." *Id.* at 15.

163. *See* Randy Milch & Sam Bieler, *A New Decade and New Cybersecurity Orders at the FTC*, LAWFARE (Jan. 29, 2020, 8:00 AM), https://www.lawfareblog.com/new-decade-and-new-cybersecurity-orders-ftc [https://perma.cc/CDQ2-QVSL] (describing the history of the FTC's "reasonableness" regime and how its vague standard recently got the FTC in trouble in the *LABMD* case, discussed *infra* Part II.D.1).

164. *See, e.g.*, *Strengthen Your Cybersecurity*, U.S. SMALL BUS. ADMIN., https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats [https://perma.cc/T4E3-4LD4] ("[A] majority of small business owners feel their businesses are vulnerable to a cyberattack. Yet many small businesses cannot afford professional IT solutions, have limited time to devote to cybersecurity, and don't

dedicated Chief Information Security Officer (CISO) responsible for evaluating their company's cybersecurity risks.[165]

At the same time, cyberattacks (the primary cause of data breaches)[166] are rarely bespoke pieces of malware targeted at specific businesses. Instead, the most common attacks are shotgun blasts across the internet, targeting basic vulnerabilities in software, operating systems, and human behavior.[167] This combination—the lack of knowledge/expertise of most individual actors, and the commonality of generic attack vectors—suggests that an agency may be better positioned to understand most businesses' risk-risk tradeoffs *and* that fact-specificity may not be as critical in evaluating cybersecurity reasonableness as one might intuit. All of this, combined with a growing consensus around certain data security practices (e.g., the Critical Security Controls (CSC) guidelines),[168] points towards the utility of agency regulation through concrete rules.[169]

---

know where to begin."); Josue, *The New Realities of a Remote Workforce Increase Cybersecurity Concerns for Half of All Small Business Owners, But Policies, Training Still Lag, Cyber Readiness Institute Survey Finds*, CYBER READINESS INST. (Apr. 5, 2020), https://cyberreadinessinstitute.org/news-and-events/the-new-realities-of-a-remote-workforce-increase-cybersecurity-concerns-for-half-of-all-small-business-owners-but-policies-training-still-lag-cyber-readiness-institute-survey-finds/ [https://perma.cc/6QVX-VUVG] (describing the findings of a Cyber Readiness Institute survey of 412 small businesses and reporting that only 33% of small businesses provide cybersecurity training).

165. *The Cloudfathers: An Analysis of Cybersecurity in the Fortune 500*, BITGLASS, https://pages.bitglass.com/rs/418-ZAL-815/images/Bitglass_TheCloudfathers_Fortune500.pdf [https://perma.cc/L2ZP-D4XV]. OF course, it would not be entirely accurate or fair to say that businesses without CISOs do not evaluate cybersecurity risk.

166. *See* VERIZON 2020 DBIR, *supra* note 3, at 7.

167. According to the 2020 Verizon Data Breach Investigations Report, phishing and credential stuffing are the two most common attack vectors that lead to data breaches. *Id.* at 13; *see also id.* at 19 (noting that 80% of breaches caused by "hacking" stem from brute force, i.e., en masse, methods). Credential stuffing consists of brute force plugging in exposed personal information into a slew of websites until they eventually work (i.e., allow the attacker to log in). *See, e.g.*, Neal Mueller, *Credential Stuffing*, OWASP, https://owasp.org/www-community/attacks/Credential_stuffing [https://perma.cc/8JJW-UQ3Y] (describing the attack and its popularity).

168. For example, the Verizon 2020 DBIR and the California AG's 2016 Data Breach Report both recommend that all businesses abide by the Center for Internet Security (CIS) CSC guidelines. VERIZON 2020 DBIR, *supra* note 3, at 101; CAL. DATA BREACH REP., *supra* note 56, at 30.

169. *See also* Cohen, *supra* note 6, at 12–13 (arguing that a privacy regulation that lacks specific data protection safety requirements "invites death by a thousand cuts").

2. Path Dependence, Novelty, and Regulation in the Face of Uncertainty

Path dependence looks at which actors have traditionally regulated the field, from both a federalism and institutional perspective. Path dependence relies on the assumption that the traditional regulator probably has more expertise and infrastructure already built than other alternative agencies.[170] But data breaches are a relative *terra nullius*. Granted, many plaintiffs and scholars attempt to tie the harm to common law tort ideas of trespass, breach of implied contract, and defamation, all traditionally left to the states. But, as discussed in Part I, state and federal courts have repeatedly pushed back on grounding such "novel technology" in traditional tort law.[171]

This bears on the institutional path dependence question, too. Since courts have repeatedly punted on paving new ground in tort law, and often explicitly call on the legislature to act, we can cross off the courts as the appropriate first mover. Instead, a statutorily enshrined duty to safeguard would prime the pump, so to speak, and reinvigorate courts' efforts to work within their comfort zone by fleshing out the parameters of what "reasonable" cybersecurity means.

That is not to say that agencies have no role to play. Agencies may be the best positioned to understand the risk-risk tradeoffs and aggregate information across states and industries to design best practice cybersecurity standards.[172] And in the face of uncertainty around the federalism-federalization timeline (see Part II.B), agencies may be the optimal institutional actor to decide whether and when a uniform federal regulatory policy should exist.[173]

---

170. *See* Thomas W. Merrill & David M. Schizer, *The Shale Oil and Gas Revolution, Hydraulic Fracturing, and Water Contamination: A Regulatory Strategy*, 98 MINN. L. REV. 145, 251 (2013) (arguing that "[i]nstitutions that have regulated issues in the past will have a presumptive claim to do so in the future, based on their expertise, their relationships with important interest groups, and their natural inclination to protect their turf," unless that status quo is "severely dysfunctional").

171. *See, e.g.*, Collins v. Athens Orthopedic Clinic, 837 S.E.2d 310 (Ga. 2019); McConnell v. Dep't of Labor, 787 S.E.2d 794 (Ga. 2016).

172. Better, too, than the legislature, because in areas that require dynamic and constantly updating regulatory responses (e.g., due to novel or ever-changing technology), agency rulemaking and policy statements are far more flexible than the bicameralism and presentment process.

173. Professor Sharkey describes what she calls an "agency reference model for judicial decisionmaking" around whether/when a uniform federal structure should exist:

But a regulatory void may emerge as the agency gathers information about when that time should be and what that regulatory policy should look like (e.g., through observing state models, consulting experts, and engaging with the public through notice-and-comment rulemaking). On this issue, Professors Merrill and Schizer argue that "[t]ort law emerges as a backstop to best practices regulation: tort liability rules provide 'a form of protection for those injured by technological innovations, while information gradually accumulates that may eventually lead to more protective ex ante regulation.'"[174] Thus, optimal regulation requires an interplay between federal agencies and courts, spurred first by legislative action that recognizes the duty and authorizes rulemaking without preempting states or private parties from experimenting and enforcing the statute.

D. Delegation to Whom?

1. Public Regulation: The FTC?

Tying this theoretical musing back to data breaches presents a practical question: Which agency should enforce a duty of care in safeguarding personal information? Institutional path dependence—in other words, giving power to the domain's "traditional" regulator—would point the organic statute toward vesting enforcement authority in the FTC.[175] The FTC is responsible for enforcing a number of statutes containing privacy and data security provisions,[176] and it has promulgated the Safeguards Rule, perhaps the closest to a general baseline data protection rule in the Code of Federal Regulations.[177] Also, the FTC has been enforcing a mushy

> Agencies can serve as a reference in determining the optimal regulatory strategy; specifically, agencies conduct context-specific cost-benefit (or risk-risk) analyses in deciding whether or not to pass regulations. This information base, moreover, can provide an empirical basis for the Court's assessment as to whether a uniform federal regulatory policy should exist in a particular area.

Sharkey, *supra* note 149, at 477–79.

174. Sharkey, *supra* note 156 (quoting Thomas W. Merrill & David M. Schizer, *The Shale Oil and Gas Revolution, Hydraulic Fracturing, and Water Contamination: A Regulatory Strategy* (Colum. L. and Econ., Working Paper No. 440, 2013)).

175. Which is exactly what some bills in the 116th Congress have done. *See, e.g.*, Do Not Track Act, S. 1578, 116th Cong. (2019); Mind Your Own Business Act of 2019, S. 2637, 116th Cong. (2019).

176. *See* FTC, FTC'S USE OF ITS AUTHORITIES TO PROTECT CONSUMER PRIVACY AND SECURITY 5 (2020) (listing, among others, COPPA, CAN-SPAM, TSR, and FCRA).

177. Promulgated under the Gramm-Leach-Bliley Act, the FTC Safeguards Rule requires covered financial institutions to establish a written information se-

safety standard around data breaches for many years under the "unfairness" prong of Section 5 of the Federal Trade Commission Act.[178] While Section 5 has no private right of action, in some cases it has provided an avenue for consumer suits in states that lack a data breach law on point.[179] The FTC therefore seems like the straightforward choice since it would continue to operate under a mandate that it has already de facto been enforcing.

With great power comes great baggage, however. Each agency carries with it preexisting jurisdictional and political limitations. Vesting power in the FTC would potentially exacerbate issues of regulatory arbitrage (e.g., with the Federal Communications Commission or Federal Election Commission). It could also hamstring the critical tool of notice-and-comment rulemaking, as the FTC is hampered by the more burdensome Magnuson-Moss rulemaking process.[180] The FTC also arguably lacks both the exper-

---

curity program around five broad requirements: (1) a designated employee to coordinate the program; (2) the identification of reasonably foreseeable external risks to the confidentiality, security, and integrity of customer information; (3) design and implement safeguards to control these risks, and regularly test and monitor the effectiveness of the controls; (4) service provider oversight, including taking reasonable steps to retain service providers capable of maintaining the safeguards and contractual provisions requiring such safeguards; (5) evaluate and adjust the program in light of testing and monitoring. FTC Standards for Safeguarding Customer Information, 16 C.F.R. § 314.4 (2023).

178. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 259 (3d Cir. 2015) (holding that a company can violate Section 5(a) by failing to maintain adequate data security protocols). *But see* LABMD, Inc. v. FTC, 894 F.3d 1221, 1237 (11th Cir. 2018) (finding the FTC's cease and desist order unenforceable due to lack of specificity with which the FTC attempted to enforce its data security standard under Section 5(a) of the Federal Trade Commission Act).

179. In a typical scenario, consumer suits will point to violations of Section 5 of the Federal Trade Commission Act to bolster negligence per se claims based on their own state UDAP laws (which *do* often have private rights of action), since those laws typically mirror the Federal Trade Commission Act. Indeed, they are often dubbed "Little FTC Acts." Not all courts recognize such claims, however. *See In re* Capital One Consumer Data Sec. Breach Litig., 488 F. Supp. 3d 374, 408 (E.D. Va. 2020) (holding that a negligence per se claim under New York law could be premised on the Federal Trade Commission Act, but not under Virginia law, which requires the statute or regulation to be expressly aimed at protecting public safety); *In re* Rutter's Inc. Data Sec. Breach Litig., 511 F. Supp. 3d 514, 532 n.9 (M.D. Pa. 2021) (commenting that "it is quite an open question whether a Pennsylvania state court would allow a plaintiff to use Section 5 of the FTCA as the basis of a negligence per se theory," but declining to resolve the question because plaintiffs already made out a claim under a negligence theory).

180. The Magnuson-Moss Warranty Act, 15 U.S.C. § 2301, imposes additional rulemaking steps on the FTC beyond those typical of informal rulemaking described in the Administrative Procedure Act. Such steps include more advanced notice of proposed rulemaking, submission of the proposed rule to congressional

tise and the resources to devote to such a major undertaking.[181] Casting an antitrust shadow over business surveillance abuses might further lead to bloated and misaligned regulation.[182]

Perhaps, alternatively, it would be wise to take a page out of California's book and create a new data protection agency unconstrained by these burdens.[183] But this too raises a host of questions. Would a new agency just create more room for regulatory arbitrage? To prevent this, would the agency take over the enforcement of other data security laws and regulations scattered across a slew of administrative agencies?[184] How should we chart this new agency's political, regulatory, and adjudicatory contours?

Ultimately, concerns around centralizing control in the FTC can be alleviated, either by Congress or by the FTC itself. Congress, for one, could directly remedy the issues of regulatory arbitrage

---

oversight committees, and a hearing requirement if any interested party requests one. While it is unclear whether Magnuson-Moss requirements apply to data protection rulemaking, the specter of Magnuson-Moss rulemaking has generated much debate in the cybersecurity enforcement space. *See* Milch & Bieler, *supra* note 163 (advising against vesting power in the FTC, given that "piecemeal adjudication under the venerable 'unfair practices' prohibition [is] effectively the FTC's only cybersecurity tool given the limitations of Magnuson-Moss rulemaking"); Ian M. Davis, *Resurrecting Magnuson-Moss Rulemaking: The FTC at a Data Security Crossroads*, 69 EMORY L.J. 781, 812 (2020) (arguing that the FTC should nevertheless reinvigorate Magnuson-Moss rulemaking to provide data security guidance); Rohit Chopra & Lina M. Khan, *The Case for "Unfair Methods of Competition" Rulemaking*, 87 U. CHI. L. REV. 357, 366–69 (2020) (arguing that the FTC has authority to engage in APA—not Magnuson-Moss—rulemaking to interpret "unfair methods of competition" under Section 5 of the Federal Trade Commission Act).

181. Cohen, *supra* note 6, at 9. *But see* Sam Bieler & Randy Milch, *Cybersecurity in One Voice: Leveraging CISA Programming to Improve FTC Cybersecurity Enforcement*, LAWFARE (Dec. 5, 2019, 8:00 AM), https://www.lawfareblog.com/cybersecurity-one-voice-leveraging-cisa-programming-improve-ftc-cybersecurity-enforcement [https://perma.cc/97Y2-HTU3] (proposing that the FTC leverage the expertise of other administrative agencies, particularly the Cybersecurity and Infrastructure Security Agency (CISA), by integrating their programming into FTC orders and potentially creating a compliance safe harbor).

182. Cohen, *supra* note 6, at 11 (arguing that "antitrust interventions designed to extend data flows outside the licensing ecosystems of dominant entities will only make privacy problems worse if they are not paired with other, privacy-focused interventions" (emphasis omitted)).

183. Some bills have proposed this. *See, e.g.*, Online Privacy Act of 2019, H.R. 4978, 116th Cong. §§ 301–14 (2019); Data Protection Act of 2020, S. 3300, 116th Cong. § 4 (2020).

184. Senator Gillibrand's Data Protection Act would transfer some enforcement power from the FTC to the new Data Protection Agency. *See* Zack Whittaker, *A New Senate Bill Would Create a US Data Protection Agency*, TECHCRUNCH (Feb. 13, 2020, 5:00 AM), https://techcrunch.com/2020/02/13/gilliband-law-data-agency/ [https://perma.cc/H4KV-Q9BW].

and so-called "mossified" rulemaking through a clear, direct explanation of intent, as it did for the Gramm-Leach-Bliley Act. Regardless, the FTC has begun to act anyway. In October 2021, the FTC updated the Safeguards Rule to expand its scope and strength, requiring non-bank financial institutions to implement additional administrative, physical, and technical security controls to protect personal data.[185] Should the FTC continue this tack of promulgating rules targeted at comprehensive data security safeguards under its broad jurisdictional authority, it may solidify its role as the de facto federal data protection agency.

2. Private Regulation: Cyber Insurance?

Insurance may pose an alternative or complementary standards-setter. From a theoretical perspective, insurance is an attractive solution for many reasons. First, if we assume that both duty-holders (businesses) and administrative agencies as they currently stand are ill-positioned to evaluate risks and promulgate a workable standard of reasonable care, insurers naturally provide those functions through the underwriting process. Insurance companies are incentivized (indeed, it is their business model) to aggregate information about the probability of each type of cyber event occurring for different types of businesses and activities.[186] Using this knowledge, insurers then incentivize businesses to incorporate safety standards through the insurance policy terms. Specifically, insured companies lose coverage for certain negligent acts and pay higher premiums for activities that the insurer designates as risky.[187] Some insurance policies even go so far as to create data breach preparation and response protocols within the insureds' organizational de-

185. Press Release, FTC, FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches (Oct. 27, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial-information-following-widespread-data [https://perma.cc/8SCW-GMPF].

186. For sources describing insurance companies' information aggregation function, see Jay P. Kesan & Carol M. Hayes, *Strengthening Cybersecurity with Cyberinsurance Markets and Better Risk Assessment*, 102 MINN. L. REV. 191, 222–23 (2017), detailing how insurance companies pool and share loss data to correctly price premiums, and Randal Milch, Statement at Meeting of the Comm'n Enhancing Nat'l Cybersecurity 12 (2016) [hereinafter Milch Statement], describing how the underwriting process aggregates information and disseminates it to insured businesses.

187. *See* Kesan & Hayes, *supra* note 186, at 224 (noting that some insurance policies incorporate exclusions for negligent events, e.g., those resulting from failure to update software).

partments,[188] and often require periodical "cyber health checks" to assess business compliance.[189]

Second, insurance provides a risk-spreading function that "enabl[es] those who might have been hobbled by risks to take actions to benefit both themselves and society."[190] This attribute will be particularly relevant if Congress does end up moving towards a statutory damages model for data breaches, since many businesses will be deterred from providing critical socially desired functions of data storage and processing.[191] Indeed, as courts and legislatures begin to allow monetary relief, as appears to be the trend, this risk-spreading function is not only critical but impossible for an administrative agency to provide.

These two benefits carry prerequisites that do not necessarily hold up in the field of cyber insurance. First, cyber insurance faces severe informational hurdles that underpin the industry's ability to evaluate risk and generate profits. There is currently a lack of actuarial data on key metrics such as the frequency, magnitude, and claim costs of actual and potential data breach incidents.[192] The propensity for error generated by low information is exacerbated by the ever-changing threat landscape, which limits the value of historical loss data for forecasting current risk.[193] On top of it all, legal ambiguity surrounding the tort system's treatment of data breaches adds another layer of uncertainty, which compounds the underly-

188. Shauhin A. Talesh, *Data Breach, Privacy, and Cyber Insurance*, 43 L. & SOC. INQUIRY 417, 420 (2018).

189. *Id.* at 429.

190. Kesan & Hayes, *supra* note 186, at 221–22; *see also* Milch Statement, *supra* note 186, at 12 (emphasizing the loss spreading function of insurance to manage and reduce the economic impacts of cyber risk).

191. *See* Bradbury, *supra* note 66 (commenting that the CCPA's per-violation statutory damages model could cause bet-the-company litigation).

192. Kesan & Hayes, *supra* note 186, at 232, 235; *see also* Milch Statement, *supra* note 186, at 13 (adding that forensic post-breach reports are often covered by attorney work-product privilege, which limits the availability of information regarding the types of defenses that were deployed and failed); Randy Milch, *What's Good for Litigation Isn't Necessarily Good for Cybersecurity*, LAWFARE (Mar. 5, 2021, 11:07 AM), https://www.lawfareblog.com/whats-good-litigation-isnt-necessarily-good-cybersecurity [https://perma.cc/2TER-GCJS].

193. *See* Tom Johansmeyer, *Cybersecurity Insurance Has a Big Problem*, HARV. BUS. REV. (Jan. 11, 2021), https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem [https://perma.cc/KKG8-CKS3]; *see also* Milch Statement, *supra* note 186, at 13 ("[N]ew cyber attacks . . . can dramatically change the set of inquiries an insurer might have.").

ing probabilistic or factual uncertainty that the insurer must account for when determining premiums.[194]

A dearth of information creates several cascading problems on the insurance market. Insurers typically attempt to offset the high error in calculating risk by increasing premiums. And indeed, the "ratio of premiums to the coverage limit for cyberinsurance is triple the ratio of other liability policies and six times higher than the ratio for property insurance."[195] High premiums can lead to moral hazard[196] and create adverse selection issues, where those with high cyber risk purchase insurance while low-risk businesses exit the market in favor of self-insurance.[197] This creates a homogeneous pool of high-risk insureds, which further increases risk for insurers (not unlike the market for health insurance) and causes market exit on the supply side.[198] This exacerbates the inefficacy of the insurance industry's ability to spread risks (among insurers and insureds), as well as the industry's information problem, whose solution relies on a thick market of suppliers and purchasers to aggregate and pool information to capture the effects of the law of large numbers.[199]

Certain intrinsic characteristics of cyberattacks add to the concern that insurance may not be the best solution. The main problem boils down to correlated risk, or the likelihood that a harmful

194. Mark A. Geistfeld, *Legal Ambiguity, Liability Insurance, and Tort Reform*, 60 DEPAUL L. REV. 539, 541 (2011).

195. Kesan & Hayes, *supra* note 186, at 234.

196. Rather than invest directly in cybersecurity, a business would spend most of its cybersecurity budget on buying insurance. From a public policy perspective, this outcome is inefficient and could be remedied in part by administrative agency actions such as standards-setting (to decrease uncertainty) and statutory compliance defenses. *Id.* at 243 (describing how the National Flood Insurance Act helped offset some insurance risk by requiring communities to demonstrate compliance with FEMA standards in order to purchase flood insurance). It could also be mitigated by insurance policy terms that set requirements for security audits or that condition coverage on compliance with a set of security standards.

197. *Id.* at 218–19. This market for lemons would only occur where the policyholder could do enough ex ante risk analysis on their own—a premise not necessarily substantiated by the bulk of relevant businesses. High premiums can also lead to a moral hazard issue.

198. The market for cyber insurance appears to be in this negative feedback loop state. Tom Johansmeyer comments that despite the $5 billion global market for cyber insurance, "[t]here just isn't enough money in cyber insurance. And it's hard to tell right now if there ever will be." Johansmeyer, *supra* note 193. He further explains that not only are the demand and supply pools heavily concentrated such that a single large loss "would likely take decades for insurers to earn back," but the reinsurance industry is also highly concentrated, with four reinsurers accounting for more than 60 percent of the market. *Id.*

199. Geistfeld, *supra* note 194, at 540.

event leads to multiple simultaneous claims by insureds.[200] If an event has high correlated risks, the insurer will be unable to spread risk and, as a result, will exclude that event from coverage.[201] While insurers are currently uncertain whether to treat cyberattacks as correlated risks,[202] many (if not most) common attack vectors appear correlated given hackers' propensity to target companies indiscriminately using common software or hardware vulnerabilities rather than specific payloads designed for the company itself.[203] Even targeted attacks, which would seem unlikely to be correlated, can still produce correlated losses depending on the splash effects of the attack and type of company in question. For example, a virus initially targeting a large software provider could spread to the provider's clients through a software update, as was the case in the SolarWinds hack.[204]

Data breaches caused by nation state actors present another common attack vector and potential form of correlated risk. Nation state cyber activity accounts for a significant and increasing number of cyber incidents,[205] including high-profile hacks on Sony,[206]

200. *See* James Ming Chen, *Correlation, Coverage, and Catastrophe: The Contours of Financial Preparedness for Disaster*, 26 FORDHAM ENV'T L. REV. 56, 66 (2014) ("Highly correlated catastrophic risks inflict 'numerous losses . . . simultaneously from a single event.'" (quoting Michael J. Trebilcock & Ronald J. Daniels, *Rationales and Instruments for Government Intervention in Natural Disasters*, *in* ON RISK AND DISASTER: LESSONS FROM HURRICANE KATRINA 89, 93 (Ronald J. Daniels et al. eds., 2006))).

201. *See id.* at 66–67. For this reason, damages arising from floods, hurricanes, earthquakes, and the like are not covered by standard commercial general liability policies.

202. Kesan & Hayes, *supra* note 186, at 223–24.

203. *See supra* note 167.

204. *See* Dina Temple-Raston, *A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack*, NPR (Apr. 16, 2021), https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack [https://perma.cc/M8XU-9AD6].

205. *See* Alex Scroxton, *Nation-State Cyber Attacks Double in Three Years*, COMPUT. WKLY. (Apr. 8, 2021, 2:14 PM), https://www.computerweekly.com/news/252499042/Nation-state-cyber-attacks-double-in-three-years [https://perma.cc/GE3L-Y2U6] (reporting on a study by HP and the University of Surrey analyzing cyber incident data between 2017 and 2019); COUNCIL OF ECON. ADVISORS, EXEC. OFF. OF THE PRESIDENT, THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY 4 (2018) (finding that state-affiliated groups accounted for 18 percent of threat actors, albeit relying on 2017 data). *But see* VERIZON 2020 DBIR, *supra* note 3, at 11 (finding that state-affiliated attacks accounted for less than 10 percent of breaches).

206. Issie Lapowsky, *What We Know About the New U.S. Sanctions Against North Korea in Response to Sony Hack*, WIRED (Jan. 2, 2015), https://www.wired.com/2015/01/us-sanctions-north-korea-for-sony-hack/ [https://perma.cc/3KWM-TGYS]; *but*

Marriott,[207] Yahoo,[208] Equifax,[209] and SolarWinds.[210] Yet many cyber insurance policies, which are typically distinct from traditional commercial general liability policies,[211] incorporate exclusions to protect insurers from losses caused by a sovereign power.[212]

Yet none of these issues are insurmountable, and if businesses will be subject to increasing liability and damages for failure to secure personal data (as this Note recommends), then insurance will be necessary to offset some of those risks. In fact, a federal statutory duty might go a long way in solving the informational and risk spreading problems. Imposing a duty would cause the demand for insurance to rise (generating more information and allowing for better risk spreading) and simultaneously diminish legal uncertainty (reducing forecasting error and thus premiums).

---

see Kim Zetter, *The Sony Hackers Were Causing Mayhem Years Before They Hit the Company*, WIRED (Feb. 24, 2016), https://www.wired.com/2016/02/sony-hackers-causing-mayhem-years-hit-company/ [https://perma.cc/HJ2C-T8CZ] (noting that there are no definitive ties between the culprits—the Lazarus Group—and North Korea).

207. David E. Sanger et al., *Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing*, N.Y. TIMES (Dec. 11, 2018), https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html [https://perma.cc/6KAZ-9PBC].

208. Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSO (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html [https://perma.cc/Y93D-F74V].

209. Brian Krebs, *U.S. Charges 4 Chinese Military Officers in 2017 Equifax Hack*, KREBS ON SECURITY (Feb. 10, 2020), https://krebsonsecurity.com/2020/02/u-s-charges-4-chinese-military-officers-in-2017-equifax-hack/ [https://perma.cc/T452-JVZ3].

210. *See* Temple-Raston, *supra* note 204.

211. Talesh, *supra* note 188, at 426 ("Modern [Commercial General Liability (CGL)] policies specifically exclude electronic data from the definition of property damage, which means that the only form of coverage that CGL policies can provide is associated with liability from physical damage to hardware, which is unusual in most cyber incidents.").

212. *See* Adam Satariano & Nicole Perlroth, *Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong.*, N.Y. TIMES (Apr. 15, 2019), https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html [https://perma.cc/7ENQ-HGDL] (describing the legal battle between Zurich Insurance and Mondelez in the wake of the NotPetya cyberattack in 2017, noting that "Mondelez was deemed collateral damage in a cyberwar" that is covered under a "war exclusion"); Michael Menapace, *Property Insurance, Cyber Insurance, Coverage and War: Losses from Malware May Not Be Covered Due to Your Policy's Hostile Acts Exclusion*, NAT'L L. REV. (Mar. 10, 2019), https://www.natlawreview.com/article/property-insurance-cyber-insurance-coverage-and-war-losses-malware-may-not-be-0 [https://perma.cc/AAC2-8ENT] (commenting that common cyber insurance policy provision language excludes coverage from, among other things, losses caused by a "government or sovereign power (de jure or de facto)").

If this proves ineffective, the government has tools to lower premiums and reduce insurer risk (i.e., to increase the supply of insurance). For instance, it could mandate cyber insurance in certain high-risk industries (e.g., among software providers) to solve the adverse selection problem (as with car insurance or workers' compensation). Alternatively, it could take on some insurer risk by underwriting cyber insurance policies. Jay Kesan and Carol Hayes note that this latter method proved to be effective in the somewhat analogous area of flood insurance, where correlated risk was high and insurers fled the market.[213] To solve the problem, Congress passed the National Flood Insurance Act, in which the National Flood Insurance Program (NFIP) would underwrite insurance policies and allow private insurers to sell them for a commission.[214] While the NFIP method has its own issues,[215] public-private risk sharing could kickstart information accrual and turn the negative feedback loop into a positive one. As the market thickens, the need for government subsidies would decrease since risk would be adequately spread across insurers, reinsurance, and a large pool of insureds.

An insurance solution would also align with a hybrid federalization model, which this Note recommended in Part II.B. The McCarran-Ferguson Act places insurance regulation in the hands of the states and outside the scope of other federal laws.[216] At the same time, the National Association of Insurance Commissioners (NAIC) functions as a self-regulatory body whose model acts provide (harmonized) guidance for state regulators.[217] In the absence of a specialized administrative agency on point, these private bodies fill the void to create standards, provide guidance, and aggregate information for private businesses, insurers, and regulators alike.[218]

CONCLUSION

In many respects, this Note has raised more questions than it has answered. What *is* the optimal balance between regulation and

213. Kesan & Hayes, *supra* note 186, at 243–46.

214. *Id.* at 243.

215. Kesan and Hayes warn that the NFIP method "give[s] insurers a windfall as they collect premiums without actually bearing the risk, and should not be adopted for cyberinsurance without significant changes." *Id.* at 246.

216. 15 U.S.C. §§ 1011–15.

217. *See* Kesan & Hayes, *supra* note 186, at 227.

218. Aside from NAIC, the Insurance Services Office (ISO) also functions as a centralized information clearinghouse, collecting data from insurers regarding loss experiences and providing estimates to the industry. *See* Geistfeld, *supra* note 194, at 550.

tort, federalism and federalization, when factors point in different directions? And, if we should defer to an agency to decide this question, in which agency should we vest this power?

At the same time, this Note has emphasized that the current state of affairs is at best suboptimal and at worst untenable. Partial federalization and legislative inaction have created a fifty-[plus]-state minefield, causing courts to either avoid the issue or generate a rocky federal common law that is unbinding and easily overturned. In terms of a path forward, the persistence of conflicting factors indicates that there is value to be captured from decentralization and centralization, and from a dialectical relationship between agencies and courts. A federal statutory model that embodies this guidance would adopt a hybrid approach—one that does not fully preempt states' abilities to experiment or prohibit private parties' abilities to bring suit under the federal right of action. A federal duty could also invigorate the cyber insurance industry, which could provide a complementary, if not alternative, regulatory role to an administrative agency.