NOTE

Before the Breach: The Role of Cyber Insurance in Incentivizing Data Security

*Brendan Heath**

ABSTRACT

Data breaches continue to increase in size, scope, and consequence as companies face the prospect of millions of personal records of their customers or clients being disclosed to internet hackers. In the face of this growing risk, insurance policies explicitly written to cover cyber incidents offer benefits to society in the form of increased security incentives. There is, however, continuing uncertainty about the development of this form of insurance.

This Note explores theories of torts and insurance in driving efficient management of risk and addresses the possibilities and limitations of both fields in developing effective deterrence of risk. After examining the role of the federal and state governments in insurance schemes generally, this Note argues that although the risks associated with data breaches offer novel difficulties, they are fundamentally more insurable than those of natural disasters and terrorism, which the government takes a more direct hand in insuring. This Note describes the development of the private cyber-insurance model and its split from traditional commercial general liability ("CGL") policies, concluding that ambiguities should be resolved in ways that promote independent-standing cyber policies. Finally, the Note examines the trend in the data-storage industry of demanding limitations on liability and indemnification in contracts

* J.D., 2018, The George Washington University Law School; B.A., Politics, 2012, Princeton University. I would like to thank Professors Paul Rosenzweig, Daniel Solove, and Marc Mayerson for their insight and support regarding this topic, and the dedicated and diligent staff at the *George Washington Law Review*. They put an incredible amount of care into each and every publication, and I am immensely honored by the opportunity to contribute.

with the companies whose data is stored. It concludes that such provisions ought to be held contrary to public policy, enabling subrogation suits and preserving the deterrent effects of tort law.

Table of Contents

Introduction

On December 14, 2016, Yahoo! Inc. set a new record.[1] After uncovering a 2014 hack of 500 million user accounts that past September,[2] Yahoo revealed that it had also been the victim of another, unrelated hack of more than *one billion* user accounts, in which hackers accessed names, email addresses, telephone numbers, dates of birth, and passwords.[3] The press quickly noted that these two inci-

---

1 *See* Vindu Goel & Nicole Perlroth, *Yahoo Says 1 Billion User Accounts Were Hacked*, N.Y. Times (Dec. 14, 2016), http://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?_r=0 [https://perma.cc/XS54-VEWE].

2 Dustin Volz, *Hackers Steal Data from 500 Million Yahoo Accounts*, Reuters (Sept. 22, 2016, 5:11 PM), http://www.reuters.com/article/yahoo-cyber-idUSL2N1BY0SZ [https://perma.cc/M5KP-VNXT].

3 Press Release, Yahoo! Inc., Important Security Information for Yahoo Users, Bus.

dents were "the largest known security breaches of one company's computer network."[4] Perhaps the most galling factor for Yahoo was how foreseeable these attacks were, given the company's history.[5] Yahoo had also been the victim of a 450,000-account hack in 2012, for a total of three massive breaches over the course of three years.[6] Unfortunately for Yahoo, the news broke while the company was in the midst of an acquisition by Verizon.[7] Following revelations of this latest breach, Verizon began to reexamine the deal,[8] and the acquisition price was eventually reduced by $350 million.[9] Additionally, it was reported that New York Attorney General Eric Schneiderman was investigating whether Yahoo had violated New York law by failing to inform its customers about the hack.[10] The Securities and Exchange Commission ("SEC") also commenced an investigation regarding Yahoo's failure to notify investors about the breach.[11] In recognition of the potential negative financial impact of such investigations, the revised Verizon-Yahoo merger agreement placed all liability for any shareholder suit or SEC investigation, as well as fifty percent of liability from any other government investigation or other third-party litigation, on Yahoo.[12] Yahoo also suffered on the stock market: the day after announcing the billion-user-account hack, Yahoo's stock dropped 4.4%, erasing $1.7 billion from its value.[13] As for personal

---

WIRE (Dec. 14, 2016, 4:51 PM), https://yahoo.tumblr.com/post/154479236569/important-security-information-for-yahoo-users [https://perma.cc/7WMP-D4Y9].

4 *E.g.*, Goel & Perlroth, *supra* note 1.

5 *See id.*

6 *Id.*

7 *See* Scott Mortiz & Brian Womack, *Verizon Explores Lower Price or Even Exit from Yahoo Deal*, BLOOMBERG TECH. (Dec. 15, 2016, 3:17 PM), https://www.bloomberg.com/news/articles/2016-12-15/verizon-said-to-explore-lower-price-or-even-exit-from-yahoo-deal [https://perma.cc/S3VU-BQQR].

8 *See id.*

9 Akin Oyedele, *Verizon Has Cut Yahoo's Price by $350 Million*, BUS. INSIDER (Feb. 21, 2017, 7:32 AM), http://www.businessinsider.com/yahoo-verizon-revised-deal-2017-2 [https://perma.cc/UYW8-V5SF].

10 *See* Press Release, New York State Office of the Attorney General, A.G. Schneiderman Issues Consumer Alert After Second Yahoo Data Breach, Examines Circumstances of Breach and Disclosure to Law Enforcement (Dec. 15, 2016), http://www.ag.ny.gov/press-release/ag-schneiderman-issues-consumer-alert-after-second-yahoo-data-breach-examines [https://perma.cc/M4PY-JJQ3].

11 *See* Suzanne Barlyn, *U.S. SEC Probing Yahoo Over Previously Disclosed Cyber Breach-Filing*, REUTERS (Jan. 23, 2017, 7:47 AM), http://www.reuters.com/article/yahoo-sec-probe-idUSL1N1FD0TJ [https://perma.cc/3E8D-G6AC].

12 *See* Press Release, Verizon, Verizon and Yahoo Amend Terms of Definitive Agreement (Feb. 21, 2017), http://www.verizon.com/about/news/verizon-and-yahoo-amend-terms-definitive-agreement [https://perma.cc/L8P8-BZLV].

13 Shira Ovide, Opinion, *The $1 Billion Price for Yahoo's Incompetence*, BLOOMBERG:

repercussions, Yahoo's general counsel resigned, and CEO Marissa Meyer lost both her annual bonus and equity grant, a combined value of up to $14 million.[14] Finally, although not explicitly linked to revelations of the breach, in March 2017, Yahoo announced that Meyer would no longer serve as CEO following the acquisition of the company by Verizon.[15]

The sheer magnitude of these Yahoo breaches, coupled with the dramatic financial and personal consequences for Yahoo and its officers, should serve as a warning to other companies that hold consumers' personal data. The average cost of a data breach to a U.S. company reached $221 per exposed record in 2016, and although most companies will not face anywhere near the scope of the largest Yahoo hack, costs can still be prohibitively large.[16]

Companies are heeding these portents. In a 2016 survey of risk experts worldwide by insurance company Allianz, cyber incidents (including crime and data breaches as well as general IT failures) generally ranked as the third-highest concern, above worries about natural catastrophes, legislative and regulatory changes, and macroeconomic developments.[17] Cyber incidents were also identified as one of the fastest-growing risks; as recently as 2013, cyber incidents ranked only fifteenth, but they are currently rated the top long-term risk.[18]

CYBERDUNCE, (Dec. 15, 2016, 1:16 PM), https://www.bloomberg.com/gadfly/articles/2016-12-15/yahoo-s-cyberfail-could-cut-1-billion-from-verizon-deal [https://perma.cc/AJ89-D426]. Yahoo's stock value eventually returned to pre-breach disclosure levels after about a month. *See Altaba Inc.*, YAHOO! FIN., https://finance.yahoo.com [https://perma.cc/H4XN-HYUM] (search for "YHOO"; then follow "Historical Data" hyperlink; then select "5Y" under "Time Period").

14 *See* Steve Kovach, *Yahoo's Top Lawyer Is Out After Investigation Finds Yahoo Execs Didn't 'Properly Comprehend or Investigate' Massive Hacks*, BUS. INSIDER (Mar. 1, 2017, 5:52 PM), http://www.businessinsider.com/yahoo-general-counsel-ronald-s-bell-resigns-2017-3 [https://perma.cc/5WA9-UVBT]; Steve Kovach, *Yahoo's Board Is Not Paying Marissa Mayer Her 2016 Bonus Because of the Hacking Incidents*, BUS. INSIDER (Mar. 1, 2017, 5:08 PM), http://www.businessinsider.com/marissa-mayer-gives-up-bonus-and-equity-grants-following-yahoo-hacks-2017-3 [https://perma.cc/D3WZ-CYJX]; Marissa Mayer, *Update on Yahoo's Security Incident*, TUMBLR (Mar. 1, 2017), http://marissamayr.tumblr.com/post/157876672644/update-on-yahoos-security-incident [https://perma.cc/6SM9-AVXM].

15 *See* Yahoo! Inc., Current Report (Form 8-K), Item 5.02 (Mar. 10, 2017); Steve Kovach, *Marissa Mayer Won't Be the CEO of Yahoo's Remaining Business, Altaba, After the Verizon Deal Closes*, BUS. INSIDER (Mar. 13, 2017, 10:14 AM), http://www.businessinsider.com/marissa-mayer-to-step-down-yahoo-ceo-after-verizon-deal-closes-2017-3 [https://perma.cc/Q9X7-5VD5].

16 *See* PONEMON INST., 2016 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS 2 (June 2016). The average organizational cost, including both direct and indirect costs such as loss of business, was $7.01 million in the U.S. *Id.* Cost does vary enormously by the amount of data lost. For breaches of fewer than 10,000 records, the average total cost was $2.1 million. *Id.* at 3, 15.

17 ALLIANZ SE & ALLIANZ GLOBAL CORP. & SPECIALTY SE, ALLIANZ RISK BAROMETER: TOP BUSINESS RISKS 2016 1 (2016).

18 *Id.* at 10, 13.

Troublingly, however, worries about cybersecurity have yet to inspire effective investment in adequate prevention. Studies report that between fifty-three and eighty percent of data breaches are discovered by entities other than the breached organization,[19] and there can be a substantial gap between the time of intrusion and the moment the attack is detected. Ponemon's 2016 Cost of Data Breach Report estimated that affected companies took an astonishing 229 days on average to detect a case of criminal or malicious data breach.[20] In contrast, some methods of intrusion by hackers require mere minutes to compromise the target system.[21] Finally, Alison Cerra of Intel Security Group reports that "71% of those aged 18–34 believe their data is more secure today than it was a year ago,"[22] showing that the general public underestimates the threat of data breaches.

Industries exposed to cyber risk thus face two interrelated problems: the underincentivization of data security and the risk of sudden financial loss in the event of a data breach. Fortunately, there is a way to address both simultaneously—cyber insurance. Although insurance has been recognized as a means of mitigating risks to individuals and companies for centuries,[23] it also can serve as a way of incentivizing the avoidance of those risks. Incentivization works by pricing premiums, at least partially, upon certain risk-reducing standards that policyholders are encouraged to meet.[24] The burgeoning field of cyber insurance, however, faces numerous obstacles limiting its efficient development.[25]

---

19 McAfee, Inc., McAfee Labs Threats Report: September 2016 (2016), http://www.mcafee.com/us/resources/misc/infographic-threats-report-sep-2016.pdf [https://perma.cc/CL3V-ZX9G]; Verizon, 2016 Data Breach Investigations Report 7 (2016).

20 Ponemon Inst., *supra* note 16, at 3.

21 Verizon, *supra* note 19, at 10. This figure is greatly influenced by the nature of phishing attacks—the only time it takes to compromise a system is the time it takes to type the acquired username and password. *Id.*

22 Allison Cerra, *Risky Business: Miscalculating Cyber Threats*, McAfee: Securing Tomorrow (Oct. 31, 2016), https://securingtomorrow.mcafee.com/executive-perspectives/risky-business-miscalculating-cyber-threats [https://perma.cc/GLE6-D32X].

23 *See* Andrew Beattie, *The History of Insurance*, Investopedia, http://www.investopedia.com/articles/08/history-of-insurance.asp [https://perma.cc/Q3YE-EK2X] (explaining that there are prototypical insurance schemes listed in the Code of Hammurabi).

24 Kenneth S. Abraham, The Liability Century 228 (2008).

25 Although the portion of businesses purchasing cyber insurance has grown by eighty-five percent over the past six years, between 2015 and 2016, growth slowed to seven percent, down from an eighteen-percent increase the previous year. Amy O'Connor & Andrea Wells, *Steamin' Hot Markets of 2017: Cyber—The Belle of the Market Ball*, MyNewMarkets (Mar. 29, 2017), http://www.mynewmarkets.com/articles/182961/steamin-hot-markets-2017-cyber-belle-market-ball [https://perma.cc/B4SX-ZGL9].

This Note argues that although the cyber industry continues to grow under the private sector, the government can and should play a supporting role by developing baseline standards and collecting historical data. This approach diverges from other relatively novel insurance schemes such as terrorism insurance, in which government plays a more direct role.[26] Additionally, this Note argues that courts can assist in the development of cyber insurance by clearly distinguishing cyber insurance from commercial general liability ("CGL") coverage. Finally, when companies that collect personal information from their customers provide that information to a third party for storage, many third parties expressly disclaim liability resulting from a data breach. In this scenario, this Note proposes that courts and state legislatures expressly nullify such limitations of liability as contrary to public policy. This would open such storage vendors to liability to their customers or, in the case of a subrogation action, to the data-collecting company's insurer. Subrogation actions, in particular, provide the dual benefits of risk mitigation for the company that collects consumer data and incentives for better data security on the part of the vendor that stores the data.

Part I provides background on the role of the insurance industry in managing society's risks, generally, and the tort law background of data-breach cases, specifically. The first Section details the evolution of views from intense skepticism of liability insurance to the acknowledgement that such insurance can instead promote risk avoidance by policyholders. The second Section describes the emergence of liability for data breaches and the challenges that still face such actions, including suits from consumers whose data was exposed and enforcement actions by governmental regulatory agencies.

Part II compares models for government intervention on the insurance side of data breaches, specifically arguing that the threat of hacks leading to data breaches is fundamentally different enough from the types of fields in which other governmental insurance programs are available that the field is currently best left to private industry. Part III discusses the relationship between coverage for data breaches and the more traditional CGL policy, which covers a wider range of claims, and argues that greater efficiency is achieved through a more rigorous distinction between the two.

Finally, Part IV examines situations in which companies acquiring personal data from their customers do not store it themselves but,

---

26 *See infra* notes 120–123 and accompanying text.

rather, hire a third-party storage provider to do so. This Part argues that attempts by such storage providers to limit their liability in the event of a data breach should be nullified on grounds of public policy. Such a provision would enable the data-acquiring company's insurer to file a subrogation suit against the negligent storage provider, incentivizing better data security while still providing the benefit of insurance to the data-acquiring company.

I. The Twin Functions of Insurance and Tort

A. The Role of Insurance in Promoting Risk Avoidance

The primary function of insurance has traditionally been understood to be spreading loss: loss is transferred from an individual to an insurance company through claims and simultaneously from an insurance company to all of its policyholders through the collection of premiums.[27] This model serves both individual and societal goals; the individual benefits from peace of mind, knowing that potential catastrophe has been guarded against, and society as a whole benefits from spreading risk among a large group, making financial losses to that group more predictable.[28] Going without insurance harms an individual, if that individual chooses to disregard risk, and harms society as a whole, if individuals decide to meet risks by inefficiently holding cash reserves.[29] On the other hand, one of the traditional worries about insurance, particularly liability insurance, has been "moral hazard"—that policyholders would be less incentivized to exercise care in avoiding or preventing the losses for which they became insured, which would result in an increase in the overall amount of societal injuries.[30] This concern was so great that under nineteenth-century tort law, liability insurance was disallowed because it was considered harmful to the public.[31]

In the overall economic context of the time, however, liability insurance was also less financially necessary simply because strict legal doctrines in tort law limited potential judgments.[32] For example, workplace injury suits in the twentieth century had to overcome the doc-

---

27 *See* Emmett J. Vaughan & Therese M. Vaughan, Essentials of Insurance 16–17, 23 (1995).

28 *See id.* at 17, 23.

29 *See id.* at 16, 23.

30 Abraham, *supra* note 24, at 16. Moral hazard is considered less problematic in first-party insurance such as life or property insurance because the insured has an independent interest in what he or she has insured. *Id.*

31 *See id.* at 17.

32 *See id.* at 19.

trines of contributory negligence, assumption of the risk, and the "fellow-servant" rule before liability could be established.[33] As industrialization increased the rate of accidental injury, many such incidents were left uncompensated.[34] Over time, organized labor exerted pressure on legislatures to begin adding more statutory exceptions to these conservative tort doctrines, expanding liability and financial risk to employers along with it.[35] In response, insurers attempted to offer coverage for this newly expanding risk,[36] and courts acquiesced, discarding the moral-hazard, public-policy objection to liability insurance.[37] The key language came from a case that did not directly involve liability insurance, but its language offered an opportunity to refocus the entire concept of insurance: "By obtaining insurance, [the insured] does not diminish his own responsibility to the owners of the goods, but rather increases his means of meeting that responsibility."[38] Thus, the social good of ensuring the adequate compensation of victims arose as a counterweight to the social harm of moral hazard in considering the value of liability insurance.[39] Additionally, even in these early decisions, courts argued that the presence of insurance might not create as much moral hazard as had been presumed:

> The [insured] will, from motives of self-interest, if from none other, endeavor to reduce . . . the amount of the annual premium payable therefor, while the aggregate of insurance which he may be able to procure, as well as the rate charged him for it, will always depend in a large measure, if not entirely, upon the prudence, care, and skill with which his affairs are managed and conducted.[40]

From these beginnings, the notion that insurance could reduce rather than increase overall risks of occurrences began to gain acceptance and, by the mid-twentieth century, was used to justify other expansions of tort liability. For example, Justice Roger Traynor of the Supreme Court of California argued that manufacturers should face strict liability for product defects because they were in a better posi-

---

33 *See id.* at 42 (establishing, respectively, that a victim could not sue his employer for injuries if the victim was negligent in the injury, if he had accepted the risk of injury in his employment, or if the injury was committed through the negligence of another employee).

34 *See id.* at 26–27.

35 *See id.* at 27–28.

36 *See id.* at 28.

37 *See id.* at 29–30.

38 Phoenix Ins. Co. v. Erie & W. Transp. Co., 117 U.S. 312, 324 (1886).

39 ABRAHAM, *supra* note 24, at 26.

40 Boston & A.R. Co. v. Mercantile Tr. & Deposit Co. of Balt., 34 A. 778, 787 (Md. 1896).

tion than the public to take steps to prevent defects and to insure against such injuries.[41]

Importantly, the ability of insurance to incentivize the reduction of risk does have serious limitations. First, when insurers have difficulty assessing the historical risk of various policyholders, it follows that they will be unable to appropriately reward the relatively cautious.[42] Additionally, some risks are fundamentally impossible to guard against completely, no matter how attractive a potential premium discount.[43] In the cyber field, for example, the two most effective ways to reduce the risk of a data breach would be to disconnect from the internet altogether and to stop collecting customer data. For many companies, however, a reversion to paper records would be completely incompatible with their business model.[44] Likewise, companies would find it difficult to do many transactions with customers if their data were not collected at some point. Indeed, for many businesses the financial balance depends on collecting more data, not less.[45] Finally, although risk prevention can be an important part of insurance, it directly competes with the other key function of insurance—loss-spreading.[46] Deterring risk requires an insurance company to price its premiums differently depending on policyholder risk, which increases the fiscal burden on relatively risky policyholders and reduces it on the prudent.[47] As such, a society's insurance and liability public policies are forced to strike a balance between these interests.[48]

---

41 *See* Greenman v. Yuba Power Prods., Inc., 377 P.2d 897, 901 (Cal. 1963); Escola v. Coca Cola Bottling Co. of Fresno, 150 P.2d 436, 440–41 (Cal. 1944) (Traynor, J., concurring); *see also* Kenneth S. Abraham, *Liability Insurance and Accident Prevention: The Evolution of an Idea*, 64 MD. L. REV. 573, 601 (2005).

42 *See* ABRAHAM, *supra* note 24, at 231.

43 *See id.* at 231–32.

44 *See* Alejandro Crawford & Lisa Chau, *Why Google's Business Model Works*, U.S. NEWS & WORLD REPORT (June 25, 2013, 10:35 AM), https://www.usnews.com/opinion/blogs/economic-intelligence/2013/06/25/why-googles-business-model-works [https://perma.cc/P8XQ-ZQDL] (referring to Google's use of customer data obtained by offering free services like Gmail to make money through selling such data to advertisers). "It is this monetization of [user data] that enables a business to sustain itself, compete for market share, and grow. Without this kind of monetization, a business seldom generates enough cash flow to justify successive investments in innovation, not to mention build customer relationships and the like." *Id.*

45 *See* James R. Kalyvas & David R. Albertson, *A Big Data Primer for Executives*, *in* JAMES R. KALYVAS & MICHAEL R. OVERLY, BIG DATA 1, 4–5 (2015); Natalie Barbour, *3 Ways to Use Customer Data to Increase Conversions Right Now*, BIGCOMMERCE, https://www.bigcommerce.com/blog/customer-data-important-ecommerce [https://perma.cc/FQC4-6H3Z].

46 ABRAHAM, *supra* note 24, at 239.

47 *See id.*

48 *Id.*

Because the original function of insurance was loss-spreading, the function of risk prevention merits little more than passing skepticism in some insurance scholars' estimations.[49] Still, targeted efforts can keep these two functions in balance while some other interest is advanced. For example, promoting more accurate government data sharing and standards establishment with the insurance industry can increase industry-wide efficiency in pricing and administration costs.[50]

B. The Role of Tort Law in Promoting Risk Avoidance

Of course, there would be no need for insurance if there were no risk to insure against. For a company holding customer data, that risk manifests in lawsuits and adverse judgments following a data breach. But as a relatively new phenomenon, the ability to recover against a company for a third party's access to and use of personal data took time to develop.

The fundamental asymmetry of data-breach cases is that neither the consumer nor the company holding their data may be very successful in recovering from the ultimate wrongdoer—the external hacker.[51] Hackers that operate from abroad[52] make enforcing any kind of judgment more difficult, as does their immediate shifting or spending of any ill-gotten funds.[53] Therefore, plaintiffs' lawyers will typically look to recover against whatever institution was tasked with holding the information that was stolen.[54]

---

49 *E.g.*, VAUGHAN, *supra* note 27, at 23 n.5 ("[T]hese loss-prevention activities are not essentially a part of the operation of the insurance principle. Insurance could exist without them, and they could and do exist without insurance. Insurance in and of itself does not favorably alter the probability of loss."). *See generally* ABRAHAM, *supra* note 24, at 602–07.

50 *See infra* Section II.C.

51 This Note focuses on data breaches caused by an external actor, rather than by a company insider, sheer mistake, or other types of damage caused by hacking. For perspective, in 2016, forty-eight percent of data breaches were caused by malicious or criminal action rather than by company negligence or technical error alone. Breaches by the former cause were about twenty-five percent more expensive to the company than the latter. *See* PONEMON, *supra* note 16, at 11.

52 For example, indictments were brought in March 2017 against two Russian spies and two hackers hired by the Russian government, in connection with the 2014 breach of 500 million Yahoo user accounts. Ellen Nakashima, *Justice Department Charges Russian Spies and Criminal Hackers in Yahoo Intrusion*, WASH. POST (Mar. 15, 2017), https://www.washingtonpost.com/world/national-security/justice-department-charging-russian-spies-and-criminal-hackers-for-yahoo-intrusion/2017/03/15/64b98e32-0911-11e7-93dc-00f9bdd74ed1_story.html?utm_term=.F9d0e3142b43 [https://perma.cc/XC7B-V66N].

53 112 AM. JUR. TRIALS 1 § 20 (2017).

54 *See id.*

One potential theory is negligence, but simply alleging that a company was negligent in protecting a customer's personal information may be barred by the economic loss doctrine.[55] This doctrine was originally formulated to distinguish contract and tort claims in product liability cases, allowing claims in tort only when defects in the product produced damage to other property or persons, not solely to the product itself.[56] However, it also serves more broadly to block any claims in tort when the underlying damage alleged is solely economic in nature, and courts have not hesitated to apply the doctrine when all that is alleged in a data-breach case is that information has been stolen.[57]

Contract claims can be equally difficult for the simple reason that companies holding customers' information may simply avoid promising to protect the customer's data for the underlying transaction.[58] Similarly, unjust enrichment claims are not possible because the benefit the company receives by obtaining the customer's private information (along with their money) is compensated in turn by the provision of whatever good or service the customer has ordered.[59]

Finally, invasion-of-privacy claims face challenges with facts unique to the modern phenomenon of hacking. Many states' elements of an invasion-of-privacy claim require that the private information be publicly disseminated,[60] and it can be difficult for customers to show that the hacked data was disclosed any further than to the hackers themselves.

More recently, the doctrine of Article III standing has developed into an even more formidable obstacle. In 2013, the Supreme Court, in *Clapper v. Amnesty International USA*,[61] held that future injury

---

55 *See In re* Zappos.com, Inc. Consumer Data Sec. Breach Litig., No. 3:12-cv-00325-RCJ-VPC, 2013 WL 4830497, at *3 (D. Nev. Sept. 9, 2013); Evan M. Wooten, *The State of Data-Breach Litigation and Enforcement: Before the 2013 Mega Breaches and Beyond*, 24 J. Antitrust & Unfair Competition L. Sec. St. B. Cal. 229, 232 (2015).

56 Matthiesen, Wickert, & Lehrer, S.C., Economic Loss Doctrine in All 50 States 2–3, https://www.mwl-law.com/wp-content/uploads/2013/03/economic-loss-doctrine-in-all-50-states.pdf [https://perma.cc/FL9U-SVZS].

57 *See In re* TJX Cos. Retail Sec. Breach Litig., 564 F.3d 489, 498–99 (1st Cir. 2009), *as amended on reh'g in part* (May 5, 2009); Sovereign Bank v. BJ's Wholesale Club, Inc., 533 F.3d 162, 175–78 (3d Cir. 2008); Enslin v. Coca-Cola Co., 136 F. Supp. 3d 654, 672–73 (E.D. Pa. 2015); *In re Zappos.com, Inc.*, 2013 WL 4830497, at *3.

58 *See In re Zappos.com, Inc.*, 2013 WL 4830497, at *3.

59 *Id.* at *5.

60 *See, e.g.*, DelleCurti v. Walgreen Co., 70 N.E.3d 111, 116 (Ohio Ct. App. 2016); *see also* Galaria v. Nationwide Mut. Ins. Co, 998 F. Supp. 2d 646, 661–63 (S.D. Ohio 2014), *rev'd on other grounds*, 663 F. App'x 384 (6th Cir. 2016) (discussing the requirement of public dissemination under Kansas, Minnesota, and Ohio law in data-breach cases).

61 133 S. Ct. 1138 (2013).

must be imminent rather than speculative to establish standing and that expenses incurred by the plaintiffs to avoid potential harm are self-incurred harms rather than injury directly attributable to the defendant.[62] Nevertheless, *Clapper* has not proven to be an absolute bar to data-breach cases. *Clapper* itself did not concern a data breach, and although some courts interpret *Clapper* as blocking claims in those situations because the threat of an identity thief actually using the stolen information is hypothetical,[63] other courts have found factual distinctions, generally reasoning that the increased risk of harm due to identify theft is sufficiently imminent.[64] The pithiest argument for this position came in *In re Adobe Systems, Inc. Privacy Litigation*:[65] "[A]fter all, why would hackers target and steal personal customer data if not to misuse it?"[66]

As to specific causes of action, some state laws permit invasion-of-privacy claims without the necessity of showing that the private information has been published or publicly disseminated.[67] Additionally, one way to bypass old theories in tort or contract is to create entirely new causes of action by statute. The leading example is California's Security Breach Information Act.[68] Not only does the statute expressly require businesses that own information about California residents to "implement and maintain reasonable security procedures and practices . . . to protect the personal information from unauthorized access, destruction, use, modification, or disclosure";[69] it also creates a private right of action and prohibits contractual waiver of

---

62 *Id.* at 1143.

63 *See* Cahen v. Toyota Motor Corp., 147 F. Supp. 3d 955, 969–71 (N.D. Cal. 2015); *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 25 (D.D.C. 2014); *see also* Antman v. Uber Techs., Inc., No. 3:15-cv-01175-LB, 2015 WL 6123054, at *11 (N.D. Cal. Oct. 19, 2015) (finding lack of standing because only names and drivers' license information were stolen rather than more lucrative information such as passwords, social security numbers, or credit card numbers); Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847, 857 (S.D. Tex. 2015) (denying standing because the only unauthorized use of the credit card information was flagged as fraudulent and declined).

64 *See* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388–89 (6th Cir. 2016); Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 WL 3511500, at *5–6 (N.D. Ill. July 14, 2014); *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 962–63 (S.D. Cal. 2014).

65 66 F. Supp. 3d 1197 (N.D. Cal. 2014).

66 *Id.* at 1216. This reasoning was reinforced by the allegation that stolen data had already been used. *Id.*

67 *E.g.*, Phillips v. Smalley Maint. Servs., Inc., 435 So. 2d 705, 709 (Ala. 1983).

68 CAL. CIV. CODE § 1798.82 (West 2016).

69 *Id.* § 1798.81.5(b).

such right by public policy.[70] Other approaches include unfair-competition laws[71] and certain fact-specific reliance theories.[72]

The increased potential for private defendants to move forward with data-breach litigation and for public entities to bring enforcement actions translates to increased cost to companies, both in defending such actions and in the payment of damages should those suits succeed. For example, the vast majority of states require companies facing data breaches to inform their customers individually of the breach.[73] Penalties may vary wildly when assessed based on number of records disclosed or delay in the company's response to the breach.[74] Thus, the expansion of cyber risk requires a counterbalancing availability of cyber insurance.[75]

II. Fits and Starts in Government Promotion of Cyber Risk Avoidance

The federal government, apart from enabling consumer suits, may choose from a spectrum of options in directly promoting risk avoidance. Perhaps the most direct approach is the imposition of regulatory requirements upon affected entities. This approach brings unique difficulties. First, imposing broad requirements in order to maintain maximum flexibility for enforcement risks creates uncertainty in the regulated market.[76] Additionally, the United States has a "sectoral" approach to consumer data protection, featuring scattered statutes focusing on various industries individually, unlike the "omnibus" approach favored in Europe.[77] Such fragmentation creates fur-

---

70 *Id.* § 1798. 84(a)–(c).

71 *See In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1223 (N.D. Cal. 2014).

72 Order Granting in Part and Denying in Part Def.'s Mot. to Dismiss at 6, *In re* LinkedIn User Privacy Litig., No. 5:12-cv-03088-EJD, 2014 WL 1323713 (N.D. Cal. Mar. 28, 2014) (allowing a reliance claim to proceed on the theory that the plaintiff bought "premium" service from the defendant based on the representation that her data would be secure).

73 *See, e.g.*, Tex. Bus. & Com. Code Ann. §§ 521.052(a), 521.053 (West 2015) (covering both post-breach notification and data security in general); N.Y. Gen. Bus. Law § 899-aa (McKinney 2017) (covering post-breach notification alone). *See generally* 152 Am. Jur. Proof of Facts 3d 409 §§ 13–14 (2016) (listing and referencing each state's notice of data-breach statutes).

74 There are typically caps, however; Texas limits notification penalties for a single breach to $250,000 and New York to $150,000. *See* Tex. Bus. & Com. Code Ann. § 521.151(a-1); N.Y. Gen. Bus. Law § 899-aa(6)(a).

75 *See* Abraham, *supra* note 24, at 2 (noting that, in the past, "new forms of insurance developed along with the expansion of tort liability, sometimes before and sometimes after a new form of tort liability was created").

76 *See infra* Section II.A.

77 Daniel J. Solove & Paul M. Schwartz, Information Privacy Law 790 (5th ed.

ther uncertainty, as jurisdictions may overlap and requirements may diverge.[78] Even piecemeal regulations may still have outside effects on covered entities, as some companies choose to comply with the most rigorous regulations among the jurisdictions in which they do business.[79] Finally, as the availability of cyber insurance increases, concerns about the cost of regulation diminishes, easing the concerns of regulators.[80]

Federal and state governments themselves may also participate in the insurance market. Such government programs range from marketing policies to customers to sharing the costs of paying out claims or subsidizing the reinsurance market.[81] Among the risks these government programs address, including flood, earthquake, hurricane, and terrorist attack, the common thread is that commercial insurers have found each particularly difficult to assess properly, leading to unstable markets.[82] Although cyberattacks and data breaches do share some of the features of such risks, they are fundamentally more insurable, especially in their regularity.[83]

Finally, government can play an essential coordinating role in public-private dialogues, helping to craft industry standards and disseminating information to make the insurance market more efficient.[84]

A. Developments in State and Federal Data-Security Regulations

The most direct way for the government to incentivize data security is to issue laws and regulations simply mandating the desired standards. For example, New York State regulations effective March 1, 2017, require entities operating under the purview of New York Banking Law, Insurance Law, or Financial Services Law to maintain a comprehensive cybersecurity program that includes maintaining a written policy, chief information security officer, and data-breach response plan.[85] Having such specific requirements can potentially affect corporate governance as a whole, requiring directors and officers of covered

---

2015). *See generally* Council Regulation 2016/679, 2016 O.J. (L 119) 1 (establishing comprehensive standards for processing and movement of personal data in the European Union).

78 *See infra* Section II.A.

79 *See id.*

80 *See id.*

81 *See infra* Section II.B.

82 *See id.*

83 *See id.*

84 *See infra* Section II.C.

85 *See* N.Y. COMP. CODES R. & REGS. tit. 23, §§ 500.01–500.04, 500.16, 500.21 (2017).

companies to take a direct interest in implementing the cybersecurity standards.[86] For enforcement, however, the regulation is far less specific, merely alluding to the preexisting regulatory authority of the New York superintendent of financial services.[87]

One of the downsides of direct regulation in this manner is the uncertainty inherent in its implementation. The New York regulation is the first of its kind in the country,[88] and the precise burden on regulated entities remains to be seen.[89] Additionally, certain key provisions, such as encryption requirements for data in transit and at rest, are flexible—the covered entity's chief information security officer may approve "effective alternate compensating controls" if he or she determines that encryption is infeasible.[90] This ambiguity creates uncertainty for covered entities regarding how strictly regulators will choose to oversee such decisions.[91]

Similar concerns have hindered attempts to impose data-security regulations at the federal level. In late 2016, the Federal Communications Commission ("FCC") issued an order imposing various privacy and security requirements upon broadband internet service providers.[92] Among provisions concerning more transparent privacy policies,[93] disclosure of collected data to other parties,[94] and data-breach notification procedures,[95] these rules included a requirement of "rea-

---

86 *See* Elizabeth Blosfield, *D&O Liability Insurance Could Feel Effects of New York's Cyber Regulation*, INS. J. (Apr. 6, 2017), http://www.insurancejournal.com/news/east/2017/04/06/447137.htm [https://perma.cc/TBP8-MXA6] (suggesting that as these new standards pique interest in cyber-liability insurance for companies, their directors and officers may be interested in personal insurance as well, to cover potential personal liability for failing to implement the regulations).

87 N.Y. COMP. CODES R. & REGS. tit. 23, § 500.20. *See generally* N.Y. FIN. SERV. LAW §§ 301–303, 309 (McKinney 2011) (outlining the superintendent's authority).

88 Jim Finkle & Karen Freifeld, *New York State Finalizes First-in-Nation Cyber Security Regulation*, INS. J. (Feb. 17, 2017), http://www.insurancejournal.com/news/east/2017/02/17/442262.htm [https://perma.cc/KQP6-S3PX].

89 One estimate of annual costs, focusing on mid-sized firms, ran between $65,000 and $85,000. Elizabeth Blosfield, *New York Cyber Regs Take Effect, Mid-Sized Firms Could See Biggest Impact*, INS. J. (Mar. 1, 2017), http://www.insurancejournal.com/news/east/2017/03/01/443228.htm [https://perma.cc/M6YN-LT3T]. Of course, exact costs will vary "[d]epending upon a covered entity's size and reach." JillAllison Opell & Ron Lebow, *New York's Cybersecurity Rules: What Insurance Professionals Should Know*, INS. J. (Mar. 6, 2017), http://www.insurancejournal.com/news/east/2017/03/06/443547.htm [https://perma.cc/595B-KS4F].

90 N.Y. COMP. CODES R. & REGS. tit. 23, § 500.15(a).

91 *See* Opell & Lebow, *supra* note 89.

92 *See* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 87,274 (Dec. 2, 2016) (to be codified at 47 C.F.R. pt. 64).

93 *Id.* at 87,290.

94 *Id.* at 87,296.

95 *Id.* at 87,311.

sonable data security" for customers of telecommunications carriers.[96] The FCC noted that the requirement was phrased broadly enough to offer latitude in enforcement but reassured smaller providers that they would not face a strict liability standard.[97] Indeed, the regulations take into account a set of factors when determining appropriate levels of security.[98] Such latitude in enforcement, however, increases uncertainty; nine cable and broadband associations filed a petition for a stay, arguing that "the scope of information that would be held to the . . . standard of what would be considered 'reasonable' is impermissibly broad."[99] Ultimately, after a change in presidential administrations and the appointment of a new chairman,[100] the FCC agreed and the rule on reasonable data-security measures was stayed.[101]

An additional source of ambiguity at the federal level comes from overlap between federal agencies: rather than expressly defining reasonable data-security practices, the original FCC order referenced existing laws and guides.[102] Without any specific reference regarding how these other approaches or models would be interpreted, the FCC stay found there to be a risk that FCC standards would diverge from those of the Federal Trade Commission ("FTC"), under which other internet and technology companies are regulated.[103] In a press release, the FCC explained that its primary motivation for reversal was the importance of uniform internet privacy standards.[104] This reasoning

---

96 *Id.* at 87,307.

97 *See id.* at 87,307–08.

98 *Id.* at 87,340. These factors are (1) the nature and scope of the carrier's activities, (2) the sensitivity of collected data, (3) the size of the carrier, and (4) the technical feasibility. *Id.*

99 Joint Petition for Stay of Am. Cable Ass'n et al. at 22, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 32 FCC Rcd. 1,793 (2017) (WC Docket No. 16-106), https://ecfsapi.fcc.gov/file/101270254521574/012717%20Petition%20for%20Stay.pdf [https://perma.cc/4B66-DWZN].

100 *See* Alex Byers & Tony Romm, *Trump Said to Elevate Ajit Pai to FCC Chairman*, POLITICO: FORTY FIVE (Jan. 20, 2017, 12:37 PM), http://www.politico.com/blogs/donald-trump-administration/2017/01/ajit-pai-fcc-chairman-233905 [https://perma.cc/W59K-YDM9].

101 *See* Protecting the Privacy of Customers of Broadband & Other Telecomms. Servs., 32 FCC Rcd. 1793 (Mar. 1, 2017) (granting stay in part).

102 *See* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. at 87,307–10.

103 *See* Protecting the Privacy of Customers of Broadband & Other Telecomms. Servs., 32 FCC Rcd. at 1796–97, 1799. *See generally* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 24–26 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/SL5P-MNZT] (asserting authority to enforce "reasonable security for consumer data" under section 5 of the FTC Act and referencing dozens of enforcement actions).

104 *See* Press Release, Fed. Commc'ns Comm'n, FCC Takes Step Towards Ensuring Con-

reveals a broader debate surrounding issues of flexibility and ambiguity in regulation, as the sheer size and complexity of the Internet raises fundamental questions about the proper jurisdiction for privacy issues and the desirability of uniformity.[105] As noted in a joint FCC-FTC press release, "Americans care about the overall privacy of their information when they use the Internet, and they shouldn't have to be lawyers or engineers to figure out if their information is protected differently depending on which part of the Internet holds it."[106] With such essential issues at stake, members of Congress and interest groups quickly lined up on both sides of the issue, presaging political conflict.[107]

These jurisdictional and interpretive conflicts need not slow the growth of the cyber-insurance market. Although progress in the federal arena may be stalled, regulations at the state level, such as the aforementioned New York financial organization regulations, provide strong incentives for companies to adopt stricter data security measures, even for customers outside of New York.[108] This trend allows for the expansion of incentives across the country despite the sectoral nature of U.S. federal privacy laws.[109] Just as the hypothetical consumer in the FCC press release does not distinguish between the various possessors of his or her personal information on the internet, so long as that information is protected, companies possessing such information are incentivized to mitigate risks stemming from holding that information, whether they come from the possibility of a consumer

---

sumers Have Uniform Online Privacy Protections (Mar. 1, 2017), https://apps.fcc.gov/edocs_public/attachmatch/DOC-343703A1.pdf [https://perma.cc/J7RV-AQX4].

105 *See* Press Release, Fed. Commc'ns Comm'n & Fed. Trade Comm'n, Joint Statement of FCC Chairman Ajit Pai and Acting FTC Chairman Maureen K. Ohlhausen on Protecting Americans' Online Privacy (Mar. 1, 2017), https://www.ftc.gov/news-events/press-releases/2017/03/joint-statement-acting-ftc-chairman-maureen-k-ohlhausen-fcc [https://perma.cc/6T6U-K4FX].

106 *Id.*

107 *See* Jon Brodkin, *Broadband Lobbyists Celebrate as FCC Halts Data Security Requirements*, Ars Technica (Mar. 2, 2017, 1:53 PM), https://arstechnica.com/tech-policy/2017/03/isps-cheer-pause-of-rule-that-guards-private-data-from-security-breaches [https://perma.cc/KGG7-HUPP]; Jeff Flake, Editorial, *Settling a Bureaucratic Turf War in Online Privacy Rules*, Wall St. J. (Mar. 2, 2017, 7:06 PM), https://www.wsj.com/articles/settling-a-bureaucratic-turf-war-in-online-privacy-rules-1488413165 [https://perma.cc/3HGN-CBB2]; Harper Neidig, *House Dems Push FCC to Adopt Stronger Cybersecurity Measures*, Hill (Mar. 2, 2017, 11:53 AM), http://thehill.com/policy/technology/322009-house-dems-push-fcc-to-adopt-stronger-cybersecurity-measures [https://perma.cc/QU2Z-GH7W].

108 *See* Solove & Schwartz, *supra* note 77, at 793 (noting that some companies follow California privacy laws for all their customer data because those laws are typically the strictest, and it would be too onerous to carve out separate procedures for customers from other states).

109 *See id.* at 790, 793.

lawsuit or a regulatory enforcement action.[110] Eventually, the most prominent regulation may come to be used as a model across states or industries.[111] In tort law, expansions of legal theories of liability and a corresponding commercial market for liability insurance tend to grow together; each one capable of spurring growth in the other.[112] A widespread and efficient method of insuring cyber risks thus can mitigate concerns about the cost of imposing further potential liabilities upon companies.[113]

B. Government-Supported Insurance and the Insurability of Risks

Besides providing the statutory or regulatory incentives for risk mitigation, the federal and state governments have taken an active role in providing compensation for occurrences of particular risks, such as natural disasters and terrorist attacks. Fundamentally, an insurable risk has four required elements: a large number of predictable losses, losses that are definite and measurable, losses that are fortuitous in nature, and losses that are not systemic.[114] Catastrophic risks such as earthquakes, floods, and terrorist attacks present several problems to traditional insurers because of these factors. Most crucially, catastrophes are often geographically concentrated in their effects, causing insurers great concern over taking on too many policies tied to the same locality, and that wariness may either limit coverage or raise premiums to account for the elevated risk.[115]

Additionally, the amount of loss can be highly variable; for example, the median loss from earthquake in the United States between 1950 and 2000 was $2.7 billion, but the maximum loss was $51.3 bil-

---

110 *Cf.* ABRAHAM, *supra* note 24, at 55 (noting that after the transition to the workers' compensation model from the civil suit model in the early twentieth century, all but the largest employers purchased insurance to mitigate the costs of that program). Other mitigation methods included passing costs to their customers through higher prices and to employees through depressed wages. *See id.* at 54, 57–58.

111 *See* Suzanne Barlyn, *New York Regulator Wants Other States to Model Cyber Laws After Its Rules*, REUTERS (Apr. 9, 2017, 7:52 PM), http://www.reuters.com/article/us-new-york-cyber-idUSKBN17B13K [https://perma.cc/28MK-7XQ7] (noting that the National Association of Insurance Commissioners has been unable to come to a consensus on a model cybersecurity law).

112 *See* ABRAHAM, *supra* note 24, at 4.

113 *Cf. id.* at 173 ("In these situations . . . the unavailability of insurance had prevented legal change that might well otherwise have occurred earlier. . . . [T]he availability of insurance was a necessary condition for the expansion of liability.").

114 VAUGHAN & VAUGHAN, *supra* note 27, at 24.

115 *See* Patricia Grossi & Howard Kunreuther, *Introduction: Needs, Stakeholders, and Government Initiatives*, *in* CATASTROPHE MODELING 3, 9 (Patricia Grossi et al. eds., 2005).

lion.[116] Flooding featured a similar spread, with a median loss of $1.6 billion and a maximum loss of $25 billion.[117] For terrorist attacks, the 1993 bombing of the World Trade Center resulted in a loss of $725 million, while the September 11, 2001, terrorist attacks that destroyed the Twin Towers caused $80 billion in losses.[118] Such large variances make approximating future losses extremely difficult. The relative infrequency of natural disasters and terrorist attacks also makes future loss difficult to predict; there were only six earthquakes and eighteen floods causing more than $1 billion in loss or more than fifty deaths in the United States between 1950 and 2000.[119] Finally, the risk of a terrorist attack is uniquely dynamic; because they are catastrophes caused by human agency, the willingness, capacity, and target selection of a potential terrorist attacker changes in relation to the circumstances, as does the ability of target countries to take countermeasure proactively.[120]

To cope with these difficulties, in each of these areas the federal government has stepped in to reinforce the private insurance industry. For flooding, the National Flood Insurance Program features both private and public aspects—private insurers market policies to consumers and businesses, with premiums and claims paid through a federal fund, while the federal government administers programs to gauge flood risk and promote flood mitigation in various communities.[121] For terrorism, the Terrorism Risk Insurance Act of 2002[122] was passed in response to a near collapse of the terrorism-insurance market after the September 11, 2001, attack.[123] Renewed in 2015,[124] the statute requires property and casualty insurers to offer terrorism insurance, but reimburses claims above certain thresholds,[125] essentially offering reinsurance. States, too, have stepped into catastrophe insurance. The California Earthquake Authority administers privately sold policies

116 Patricia Grossi et al., *An Introduction to Catastrophe Models and Insurance*, *in* CATASTROPHE MODELING, *supra* note 115, at 37 fig.2.8.

117 *Id.*

118 Howard Kunreuther et al., *Extending Catastrophe Modeling to Terrorism*, *in* CATASTROPHE MODELING, *supra* note 115, at 210.

119 Grossi et al., *supra* note 116, at 36, 37 fig.2.8.

120 Kunreuther et al., *supra* note 118, at 215–16.

121 Grossi & Kunreuther, *supra* note 115, at 16–17.

122 Terrorism Risk Insurance Act of 2002, Pub. L. No. 107-297, 116 Stat. 2322 (2002) (codified as amended in scattered sections of 12 U.S.C., 15 U.S.C., & 28 U.S.C.).

123 Kunreuther et al., *supra* note 118, at 210, 216.

124 Terrorism Risk Insurance Program Reauthorization Act of 2015, Pub. L. No. 114-1, 129 Stat. 3 (2015).

125 Terrorism Risk Insurance Act § 103(c), (e).

from a publicly managed fund.[126] Taking a slightly different tack, the Florida Hurricane Catastrophe Fund establishes a public trust fund that pays out a percentage of claims following major hurricanes, while stipulating limits on the ability of insurers to cancel their property policies.[127] Each of these programs was set up after the private insurance industry indicated an inability to participate fully in the market, following particularly devastating natural disasters.[128]

Data security and the threat of external hacks share some, but not all, of the features that indicate a greater need for government participation in the insurance market. Unlike catastrophic events, hacking attempts, spread across the entire spectrum of online targets, are far more common.[129] Additionally, although there can be a sizable spread among the losses caused by breaches of various sizes, a company's risk is far more quantifiable than in a catastrophic-loss scenario.

Compiling a total count of customer records possessed is a relatively simple task, as many of the penalties specified in breach notification statutes are specifically tied to the number of records exposed.[130] Furthermore, at least one of the primary losses borne by affected customers, the necessity for credit-monitoring services, is also directly linked to the number of affected customers. Companies holding customer data and their insurers can thus begin to make more reasonably accurate predictions about the upper bounds of risk than is possible regarding catastrophic coverage. As for the third factor, data breaches caused by outside malicious hackers are, by definition, outside the direct control of the affected company.[131] Additionally, despite certain patterns in the incidences of cyberattacks, no company or industry type, regardless of its size, remains immune from attack.[132]

Finally, data breaches present a variable level of systemic risk, depending in large part on the method of access. For example, a so-

126 *About CEA*, CAL. EARTHQUAKE AUTHORITY, https://www.earthquakeauthority.com/About-CEA [https://perma.cc/C84J-2Z56].

127 Grossi & Kunreuther, *supra* note 115, at 18.

128 *Id.* at 15–19.

129 *Cf.* VERIZON, *supra* note 19, at 1. Verizon's *2016 Data Breach Investigations Report* examined over 64,000 incidents and 2,200 confirmed breaches in 2015. *Id.*

130 *See, e.g.*, N.Y. GEN. BUS. LAW § 899-aa(6)(a) (McKinney 2017) (providing for the greater of $5,000 or $10 "per instance of failed notification," up to a limit of $150,000, in cases of knowing or reckless violation).

131 PONEMON INST., *supra* note 16, at 11. The other two causes of data breaches mentioned in the Ponemon report, system error and employee negligence, are also beyond the volition of the affected company. *See id.*

132 *See* VERIZON, *supra* note 19, at 4 tbl.1.

cial-engineering hack first targets personnel with messages tailored to trick workers into giving up network credentials.[133] The success of such an attack depends upon the level of training or intuition a company's employees (or contractors) possess and is therefore not systemic.[134] On the other hand, a virus, which can duplicate and spread itself across computers,[135] presents greater systemic risks. A single, particularly prolific variant, or one that targets a core software application or program used across many networks, rather than by a single computer or network, presents particularly widespread risk.[136] Stephen Catlin, the head of the largest Lloyd's of London insurer, stressed this point in calling for government intervention into the cyber-insurance market, noting that "[i]t's possible that you can have the same loss happening around the globe."[137] Although certainly true, companies and individuals can affect their own level of risk by keeping antivirus programs and other cyber defenses up to date.[138] Additionally, the interconnectedness of the Internet works both ways: although hackers have a broad reach of potential targets, security information can also be swiftly and widely spread.[139]

Besides independent cyber-specific governmental insurance programs, another potential approach is extending the existing terrorism insurance programs to cyber risks. Among other advocates of government involvement in cyber insurance, the National Rural Electric Cooperative Association has suggested in comments to the U.S. Department of Commerce that the Terrorism Risk Insurance Program be extended to cover cyberattacks.[140] Currently, activation of the pro-

---

133 *See* THOMAS J. SHAW, INFORMATION SECURITY AND PRIVACY 165–66 (2011).

134 *See* Joseph Steinberg, *Cybersecurity Predictions for 2017: The Experts Speak*, INC (Jan. 9, 2017), https://www.inc.com/joseph-steinberg/cybersecurity-predictions-for-2017-the-experts-speak.html [https://perma.cc/WBR5-7NCX].

135 SHAW, *supra* note 133, at 164–65.

136 *See, e.g.*, Emanuel Kopp et al., *Cyber Risk, Market Failures, and Financial Stability* 21 (Int'l Monetary Fund, Working Paper No. WP/17/185, 2017), https://www.imf.org/~/media/Files/Publications/WP/2017/wp17185.ashx [https://perma.cc/D5F4-XXHE].

137 Matthew Heller, *Lloyd's Insurer Says Cyber Risks Too Big to Cover*, CFO (Feb. 6, 2015), http://ww2.cfo.com/risk-management/2015/02/lloyds-insurer-says-cyber-risks-big-cover [https://perma.cc/6NJ5-TL4L].

138 *See* STROZ FRIEDBERG, 2017 CYBERSECURITY PREDICTIONS 21 (2017).

139 *See Using Rapid Release Virus Definitions to Update Symantec AntiVirus 10.x or Symantec Client Security 3.x Clients and Servers*, SYMANTEC: SUPPORT (Jan. 15, 2010), https://support.symantec.com/en_US/article.TECH101229.html [https://perma.cc/JK5J-SW5F]. Of course, there will always remain the threat from exploits first discovered by hackers, which cannot be defended against until they are first used. SHAW, *supra* note 133, at 170.

140 Nat'l Rural Elec. Coop. Ass'n, Comment Letter in Response to March 28, 2013, Notice of Inquiry of the U.S. Dep't of Commerce, Nat'l Telecomms. & Info. Admin. (Apr. 29, 2013),

gram rests with the Secretary of Commerce, Secretary of State, and Attorney General.[141]

Regarding this potential overlap of terrorism and cyber risks, although a sophisticated enough adversary certainly could launch cyberattacks motivated by terrorism on the United States,[142] great care would have to be taken in distinguishing ideologically motivated attacks from those driven by other motives. The indictments of four defendants in connection with the 2014 breach of 500 million Yahoo user accounts demonstrate that motivations for a hack can bleed into one another.[143] In that case, the defendants, including two Russian Federal Service officers, were accused of exploiting the hack for both state-sponsored espionage and personal financial gain.[144] As governments increase their offensive cyber capabilities, a global arms race of sorts could develop in which the ability to disrupt major infrastructure would be attainable by more and more parities, while criminal groups expand into attacks on lesser-protected commercial targets.[145]

Ultimately, however, there has not yet been a major terrorist cyberattack,[146] which might demonstrate the inadequacy of commercial cyber insurance. Additionally, although the government has stepped in to play a role for each of the catastrophic risks detailed above, that role has been a supporting one, suggesting that cyber insurance might well coexist with government-supported terrorist attack insurance support. Fundamentally, though there are novel risks associated with cyberattacks, data-breach situations currently present a relatively smaller profile of noninsurability.

---

https://www.ntia.doc.gov/files/ntia/nreca_comments_april_29_2013.pdf [https://perma.cc/7MYA-CEZT].

141 Terrorism Risk Insurance Act of 2002, Pub. L. No. 107-297, 116 Stat. 2322 (2002) (codified as amended in scattered sections of 12, U.S.C., 15 U.S.C., & 28 U.S.C.).

142 *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-876T, INFORMATION SECURITY: CYBER THREATS FACILITATE ABILITY TO COMMIT ECONOMIC ESPIONAGE 4 (2012).

143 *See* Press Release, Dep't of Justice, U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts (Mar. 15, 2017), https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions [https://perma.cc/5CYU-FAGN]; *see also* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-876T, INFORMATION SECURITY: CYBER THREATS FACILITATE ABILITY TO COMMIT ECONOMIC ESPIONAGE 4 (2012) (indicating that terrorists may resort to hacking to raise funds).

144 *See* Press Release, *supra* note 143.

145 STROZ FRIEDBERG, *supra* note 138, at 10–11.

146 *See* Joseph Marks, *ISIL Aims to Launch Cyberattacks on U.S.*, POLITICO, (Dec. 29, 2015, 5:28 AM), http://www.politico.com/story/2015/12/isil-terrorism-cyber-attacks-217179 [https://perma.cc/986L-J575].

C. *Standard Setting and Information Dissemination*

An alternative governmental contribution to the cyber-insurance industry is in cooperative standard setting and collection of benchmarking information. One promising effort is the Cybersecurity Framework ("Framework") from the National Institute of Standards and Technology ("NIST"). Established by executive order in February 2013,[147] the Framework is an effort to standardize the very concept of cybersecurity across industries.[148] It offers tiers of priorities that companies can use as a model in structuring a cybersecurity program, descending from the overarching "functions" that a cybersecurity policy should address to individual "subcategories" that provide precise technical references.[149]

The same executive order also required that the departments of Commerce and Treasury analyze the benefits and effectiveness of the program through various incentives.[150] The responses from both agencies illustrate the benefits of federal involvement in the insurance industry. The Department of Commerce report directly encouraged collaboration with providers, envisioning a bilateral dialogue in which private industry would provide experience and expertise in cybersecurity best practices and the government would contribute to standardized underwriting practices.[151] Both reports noted the potential use of the Framework in determining tort liability and suggested that providing some shelter from liability might offer a strong incentive for companies to focus on increased cybersecurity.[152] The Department of Treasury report explicitly considered the potential for direct government involvement in cyber insurance but rejected that in favor of allowing the standardization aspects of the Framework to assist in the development of the private cyber-insurance sector.[153]

---

147 *See* Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013).

148 *See* NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 3 (2014).

149 *See id.* at 7–8.

150 Exec. Order No. 13,636 § 8.d, 78 Fed. Reg. 11,739, 11,742 (Feb. 12, 2013).

151 *See* NAT'L TELECOMMS. & INFO. ADMIN., DEP'T OF COMMERCE, DISCUSSION AND RECOMMENDATIONS TO THE PRESIDENT ON INCENTIVES FOR CRITICAL INFRASTRUCTURE OWNERS AND OPERATORS TO JOIN A VOLUNTARY CYBERSECURITY PROGRAM 1–2 (2013), https://www.ntia.doc.gov/report/2013/discussion-and-recommendations-president-incentives-critical-infrastructure-owners-and-o [https://perma.cc/949T-FEZ4].

152 *See id*. at 2; DEP'T OF TREASURY, REPORT TO THE PRESIDENT ON CYBERSECURITY INCENTIVES PURSUANT TO EXECUTIVE ORDER 13,636, at 10 (2013).

153 DEP'T OF TREASURY, *supra* note 152, at 5. Arguments for direct government intervention in the insurance market for cybersecurity have been offered by both private and public organizations. *See* L.A. Dep't of Water & Power, Comment Letter on Incentives to Adopt Im-

These policies and procedures offer useful guidance to the insurance industry in developing more robust cyber insurance. According to the Insurance Information Institute, the top barriers to cyber insurance include a lack of data and too little certainty.[154] Without rigorous historical records regarding cyberattack incidents, insurers have difficulty accurately pricing risk.[155] Ideally, insurers would be able to reduce the risk of cyber incidents to a single numeric score.[156] The NIST Framework offers a compelling analogue: framework implementation tiers, which describe how organized, proactive, and comprehensive an organization is in managing its cybersecurity risks.[157] By classifying the company's progress on various elements of the Framework functions according to the implementation tiers, an overall profile can be created summarizing the degree of preparedness a company has adopted in the face of cyber incidents.[158] Combining this information with increased reporting and sharing of data involving incidents would allow insurers to move towards more confident assessment of risk.

Among direct governmental contributions to the mitigation of risk of data breaches, therefore, piecemeal statutory and regulatory schemes still incentivize data security at the level of the most rigorous standard.[159] Additionally, the risk of a data breach is better suited to private insurance companies than are other categories of catastrophic risk.[160] Finally, government efforts towards sharing information on data breaches and setting technical standards in data security provide essential background information for the growth of the commercial cyber-insurance industry.[161]

---

proved Cybersecurity Practices (Apr. 29, 2013), https://www.ntia.doc.gov/files/ntia/042913_ladwp_comments.pdf [https://perma.cc/2LKG-HY5K]; Nat'l Rural Elec. Coop. Ass'n, Comment Letter in Response to March 28, 2013, Notice of Inquiry of the U.S. Dep't of Commerce, Nat'l Telecomms. & Info. Admin. (Apr. 29, 2013), https://www.ntia.doc.gov/files/ntia/nreca_comments_april_29_2013.pdf [https://perma.cc/JR8X-WAF2].

154 *See* ROBERT P. HARTWIG, INS. INFO. INST., CYBERRISK: THREAT AND OPPORTUNITY 26, 28–29 (2016).

155 *See id.* at 28.

156 *See* STEPHEN BUSATERI, VERIZON, INSURANCE INDUSTRY PERSPECTIVE ON THE VERIZON 2015 STATE OF THE IOT REPORT 2 (2015), http://www.verizonenterprise.com/resources/reports/rp_verizon-2015-state-of-the-iot-report-insurance-industry-perspective_en_xg.pdf [https://perma.cc/SE8W-T3AQ].

157 *See* NAT'L INST. OF STANDARDS & TECH, *supra* note 148, at 9–11.

158 *See id.*

159 *See supra* Section II.A.

160 *See supra* Section II.B.

161 *See supra* Section II.C.

III. Separation of Cyber Policies from Commercial General Liability Policies

Within the realm of cyber insurance currently provided by the private sector, there are key questions about characterization, one of which is to what degree data-breach cases fall within a traditional commercial general liability ("CGL") policy, rather than a cyber-specific policy. Although CGL policies did not contemplate the computer context when they were first written, certain cases were able to succeed on a theory of property damage.[162] For example, one court found that lost data may be considered property if it has "permanent value" and is "integrated completely" with physical property.[163] Another court found that a data breach can cause personal injuries, reasoning that accessing confidential emails and then disseminating or otherwise making known their contents may give rise to an invasion-of-privacy claim.[164]

However successful some of these actions have been, the inherent ambiguities surrounding digital property and privacy make attempting insurance coverage through generic provisions increasingly difficult. In another case involving lost data, a Connecticut appellate court found no coverage under a CGL policy because there was no proof the information had been published.[165] Yet another court held that a hack and data breach were, in fact, publication but that the insurance policy at issue still did not apply because it was not the insured that published the information but a third party.[166]

Conflicting and overlapping standards, although expected in a relatively novel and abstract area of law, make running a business difficult. The insurer who is wary of such disputes can simply craft exclusions into the CGL terms to prevent these disputes from emerging in

---

162 Jim Vorhis & Joan Cotkin, *How Courts Have Decided Coverage Issues in Cyber Insurance Cases*, L.A. Law., Sept. 2015, at 37.

163 *See* Retail Sys., Inc. v. CNA Ins. Cos., 469 N.W.2d 735, 737 (Minn. Ct. App. 1991). In this case, a tape containing valuable data was physically lost by the insured, but the principle might also apply if the physical "housing" of the data were instead destroyed, damaged, or otherwise made unusable. *See id.*

164 Tamm v. Hartford Fire Ins. Co., No. 020541BLS2, 2003 WL 21960374, at *1 (Mass. Super. Ct. July 10, 2003).

165 *See* Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co., 83 A.3d 664, 672–73 (Conn. App. Ct. 2014), *aff'd*, 115 A.3d 458 (Conn. 2015). This distinction could also be applied as a barrier to consumer suits, depending on the specific facts of the case. *See supra* notes 64–66 and accompanying text.

166 *See* Zurich Am. Ins. v. Sony Corp. of Am., No. 651982/2011, 2014 WL 3253541, at *1 (N.Y. Sup. Ct. Feb. 24, 2014); Judy Selby, Cyber Insurance: Insuring for Data Breach Risk, Practical Law Practice Note 2-588-8785 (2017).

the first place, a trend that has already begun, including through amendments to existing policies.[167] Separating cyber insurance from CGL provisions is also beneficial due to fundamental differences in the types of claims. One essential quality is the relative "length of the tail" on the claims in a given field of insurance—that is, the gap in time between a company's liability-creating behavior and the filing of a claim based on that liability.[168] Standardized CGL policies were amended in 1966 to provide coverage against "occurrences" generally.[169] This stands in contrast to a previous regime in which insurance was provided against "accidents."[170] Insurers argued that "accidents" refer only to events that were short in duration and, therefore, relatively immediate.[171] On the other hand, "occurrences" includes injuries that are caused some time in the past, even to the point that the actual lawsuit is decades removed from the expiration of the specific policy or the insurance company's relationship with the policyholder.[172]

This distinction between "accidents" and "occurrences" developed in the mid-twentieth century as plaintiffs became more and more capable of bringing these temporally distant suits.[173] For example, for some claims, the statute of limitations did not begin to run until the potential plaintiff learned of his or her injury and that injury's link to the potential defendant.[174] Particularly in cases involving pollution or exposure to other environmental hazards, a recognizable medical symptom of injury and the cause of that injury may not be apparent for many years.[175] The prospect of a policyholder's risks not fully manifesting for years into the future makes it difficult for an insurance company to gauge accurately the overall risk it incurs in the insurance contract and, therefore, complicates pricing. Additionally, a longer tail between the occurrence and the claim compounds external effects on the insurance industry, including changes in the insurance industry specifically, the tort and legal system generally, and the economy as a

167 *ISO Comments on CGL Endorsements for Data Breach Liability Exclusions*, INS. J. (July 18, 2014), http://www.insurancejournal.com/news/east/2014/07/18/332655.htm [https://perma.cc/9FRX-8L5H].

168 ABRAHAM, *supra* note 24, at 139, 155.

169 *Id.* at 157.

170 *Id.*

171 *See id.* at 156–57.

172 *See id.* at 155.

173 *Id.*

174 *Id.* at 156.

175 *Id.*

whole.[176] This risk to the insurance industry led to sizable volatility in the market for policyholders in the mid-1970s and 80s; premiums experienced particularly dramatic increases, even to the extent that "[f]or some policyholders for a limited time, CGL coverage was not available at any price."[177]

Fortunately, the data-security field does not present similar problems. Separation from the CGL policy model has allowed cyber insurance to revert to the "claims-made" model, in which a policyholder is only covered while a policy is active.[178] This standard implies that businesses must maintain their policies for as long as they estimate claims might remain against them.[179] In the cyber context, the lag time between the occurrence of a hack and its detection is, on average, less than a year,[180] presenting a far shorter window than the potentially decades-long lag in pollution-related cases.[181] This relatively shorter tail mitigates the burden on policyholders to maintain such claims-made policies, along with the burden on insurers regarding factors that would ordinarily make data-breach insurance more volatile and difficult to price. For instance, companies can more quickly update their security policies in response to breaches, and insurers have more immediate feedback regarding which companies present the worst track records when it comes to data security. Additionally, because the regulatory and legal framework surrounding data security, privacy, and insurance is newly developing and prone to change,[182] a shorter tail ameliorates the insurance industry's challenges in adjusting to such changes. This does not mean that the market, and premiums, will necessarily be steady. A major adjustment to liability standards or an unforeseen, catastrophic hack would undoubtedly shock the cyber-insurance system,[183] but knowing that these would

176 *See id.* at 158–62. Nevertheless, extending long-tail CGL coverage benefits the insurer. The insurer will not actually expect to pay out the claims for a long time after it has collected the premiums. In the meantime, while it is holding the cash, it can invest it, for instance, in bonds. *See, e.g.*, Letter from Warren E. Buffet, Chairman of the Bd., to Shareholders of Berkshire Hathaway Inc. 8–9 (Feb. 25, 2017), http://www.berkshirehathaway.com/letters/2016ltr.pdf [https://perma.cc/7TM3-GZ48]. In 2016, Berkshire Hathaway held about $91 billion in "float," as the sums are called, while paying out only $27 billion in claims. *See id.* As such, even minor adjustments in the interest rate may have a massive effect on insurance companies' bottom lines.

177 ABRAHAM, *supra* note 24, at 162–64.

178 Ethan D. Lenz & Morgan J. Tilleman, *The Impact of Big Data on Insureds, Insurance Coverage, and Insurers*, *in* BIG DATA, *supra* note 45, at 137, 139, 145 (2015).

179 *Id.*

180 *See supra* note 20 and accompanying text.

181 ABRAHAM, *supra* note 24, at 139.

182 *See supra* Sections I.B & II.A.

183 *See supra* note 142 and accompanying text.

likely only affect policies sold in the last few years reduces the great destabilizing effects upon the insurance industry that are prominent in long-tail systems.[184] As such, the claims-made model is relatively more advantageous for cyber insurance as a rapidly developing field.

Just as insurers need firm standards from the technology industry and government to be able to evaluate the pricing of their policies, insured companies need to be able accurately to predict the amount of coverage they will receive, given the specific risk profile of their business. Trying to integrate cyber liability into the existing CGL framework has thus far only resulted in confusion and differing standards.[185] Although insurance companies are taking matters into their own hands by writing data-breach exclusions into their standing CGL contracts,[186] courts can help promote a clearer standard by, on the one hand, more strictly interpreting standard CGL contracts and cyber exclusions and, on the other, more leniently interpreting specific cyber coverage in data-breach cases.

If traditional liability insurance is inappropriate for cyber coverage, then, perhaps a more appropriate analogy is flood insurance.[187] As in cyber, flood insurance is typically provided separately from CGL policies because of narrowly defined exclusions that are extremely tricky to apply in real-world scenarios.[188] Additionally, the insured's incentives are similarly limited to mitigation, as neither the hack victim nor the flood victim can expect to recover against the underlying cause of their injury.

Of course, cyber insurance may cover many other sources of internet-related risk besides that stemming from data breaches, including risks similar to those covered by CGL policies, such as loss or destruction of customer-unrelated data of the company, business interruption costs related to downtime caused by external hacking, or copyright or trademark infringement defense.[189] In many of these situations, the ultimate risk stems from the same fundamental roots as information security.[190] In particular, hackers using the same point of entry or method of attack may look to accomplish differing goals. For

184 *See* ABRAHAM, *supra* note 24, at 126.

185 *See supra* notes 163–66 and accompanying text.

186 *See supra* note 167 and accompanying text.

187 Jeffrey T. LaRosa & John P. Campbell, *Cyber Insurance Risks for Insurance Brokers and Lessons Learned from Flood Exposures*, N.J. LAW., June 2016, at 59.

188 *Id.* at 59–60. In the flooding context, the distinction is between damage from wind and damage caused by water. *Id.* at 62.

189 *See* HARTWIG, *supra* note 154, at 20.

190 *See* VERIZON, *supra* note 19, at 17–21, 52–55, 60–63.

example, a social engineering (phishing) attack will aim to trick the employees of target companies into revealing their credentials,[191] but once those credentials are acquired, one hacker may turn to credit cards, bank accounts, or other financial information[192] while another may turn to cyber espionage,[193] and a third may simply use the compromised computer as part of a "distributed denial of service attack" on a third party.[194] Therefore, increased security against the initial social engineering attack may lead to reduced risks from each of the further risks that attack would have enabled. Beyond security, specifically crafted cyber-insurance policies can provide coverage for other unique internet privacy risks, such as liability for wrongful data collection.[195] This adaptability, coupled with a tight link to the specific security practices that can mitigate wide categories of internet-related risks, will become especially important as ever more novel forms of cyber criminality emerge.[196]

IV. An Outside Obstacle: Third-Party Storage Providers and Subrogation

One striking scenario that impedes the distribution of risk, regardless of the type of policy, occurs with the introduction of a third party. This Part examines scenarios in which a company collecting data from their customers elects to use a third-party data-storage provider to host its data, and it is through that storage provider's negligence that the data is lost or released.

A. Indemnity Provisions in Typical Third-Party Data-Storage-Provider Contracts

Just as companies that store data face accusations of negligence from their customers, companies that contract out data storage to

191 *See* Shaw, *supra* note 133, at 165–66.

192 *See* Verizon, *supra* note 19, at 21, 68.

193 *See id.* at 53–55.

194 *See* Shaw, *supra* note 133, at 167. A distributed denial-of-service ("DDoS") attack involves coordinating many computers simultaneously to bombard a target website with traffic, forcing it to shut down. *See id.*

195 Elizabeth Blosfield, *Firms Should Look Closely at Data Practices, New York Conference Panelists Say*, Ins. J. (Sept. 28, 2016), http://www.insurancejournal.com/news/east/2016/09/28/427692.htm [https://perma.cc/J7D9-CRP4].

196 Stroz Friedberg specifically predicted a rise in the threat of data manipulation, including of commercial, financial, communication, and human relations data, as an outgrowth of increased criminal-breach capabilities. Stroz Friedberg, *supra* note 138, at 12–13; *see also* Stroz Friedberg, 2018 Cybersecurity Predictions: A Shift to Managing Cyber as an Enterprise Risk 2, 4 (2018) (asserting the accuracy of its 2017 predictions).

third-party vendors may accuse those vendors of negligence if their actions contributed to the breach. One of the same defenses offered by the former may, however, be attempted by the latter: contractual disclaimer of liability. For example, Amazon Web Services advertises security in its storage and database services.[197] In its "Customer Agreement," Amazon agrees to "implement reasonable and appropriate measures designed to help you secure Your Content against accidental or unlawful loss, access or disclosure."[198] Yet these agreements are still subject to both indemnification and limitation-of-liability clauses, with the latter specifically including any unauthorized access to any customer content or data.[199] IBM's "Client Relationship Agreement," covering its cloud services, and the "Google Cloud Platform Terms of Service" are similar in specifically targeting data-breach situations.[200] These terms are not limited to big tech companies, which provide storage to a wide range of commercial customers. Niche companies that cater to specific businesses or industries may also involve the storage or transmission of those customers' consumer data.[201] Furthermore, additional provisions—presumably accounting for situations in which complete indemnification is held unenforceable—work to cap recovery, typically to the price paid by the company for the data-storage service or for the subscription amount for up to a year prior to the hack.[202]

The ubiquity of these kinds of provisions indicates an industry standard in data storage that companies holding consumer information have apparently been either unaware of or simply unable to overcome.[203] This state of affairs exists despite repeated calls and advice

197 *AWS Cloud Security*, AMAZON WEB SERVICES, https://aws.amazon.com/security [https://perma.cc/6EFL-5FXK].

198 *AWS Customer Agreement* § 3.1, AMAZON WEB SERVICES, https://aws.amazon.com/agreement [https://perma.cc/Z9LQ-QL5G].

199 *See id.* §§ 9.1, 11.

200 *Compare Client Relationship Agreement* § 5(e), IBM, http://www-05.ibm.com/support/operations/files/pdf/cra_us.pdf [https://perma.cc/3B3E-59MT], *with Google Cloud Platform Terms of Service* § 12, GOOGLE, https://cloud.google.com/terms [https://perma.cc/ACD7-LM98].

201 *See, e.g.*, *Twilio Terms of Service* §§ 5, 12, 13, 14, TWILIO, https://www.twilio.com/legal/tos [https://perma.cc/AT7J-373G]. Twilio provides application programming interfaces ("APIs") for app makers of voice, video, and messaging services. *See The Company*, TWILIO, https://www.twilio.com/company [https://perma.cc/A4W9-YQRW].

202 *See, e.g.*, *supra* notes 197–201.

203 Richard Bortnick, *Insurers: Assert Your Subrogation Rights*, CYBERINQUIRER (Apr. 24, 2016, 5:12 PM), http://web.archive.org/web/20161027100914/http://cyberinquirer.com/2016/04/24/insurers-assert-your-subrogation-rights. Third-party storage vendors, particularly those based in the cloud, offer powerful incentives compared with an in-house storage system; these include convenience in setup and expansion, lower personnel costs, and flexible pricing models. Brian J.

from industry professionals that companies (and governments) looking to contract with a data-storage vendor specifically negotiate better terms on indemnifications and waivers of warranty.[204] Given the potentially astronomical costs of a data breach,[205] these clauses severely limit the ability of a customer to recover anywhere near the cost of the breach. The cyber insurers of data-collecting companies are thus in a potentially awkward spot as they contemplate paying claims to their policyholders that arise from an entirely different company's negligence.[206] Additionally, insurers face difficulties in pricing, as they may not be able accurately to gauge the risk posed by a third party;[207] only a handful of data-storage contracts offer specific security guarantees or audits to their customers, let alone to their customer's insurance company.[208]

B. Unleashing Subrogation

Indemnification provisions stifle the risk-distribution and risk-deterrent features of insurance. Without such barriers, there is a direct way to fulfill both functions: subrogation. In this type of action, the insurer essentially inherits any legal claim the insured had relating to

---

Pass, *Personal Cloud Computing*, *in* CLOUD COMPUTING LEGAL DESKBOOK 143, 148 (Jonathan S. Aronie ed., 2014).

204 Michael R. Overly, *Information Security in Vendor and Business Partner Relationships*, *in* BIG DATA, *supra* note 45, at 21, 29; DANA B. ROSENFELD & ALYSA ZELTZER HUTNIK, DATA SECURITY CONTRACT CLAUSES FOR SERVICE PROVIDER ARRANGEMENTS (PRO-CUSTOMER) §§ 4(c), 9, PRACTICAL LAW STANDARD CLAUSES 2-505-9027; Michael R. Overly, *Drafting and Negotiating Effective Cloud Computing Agreements*, LEXIS PRAC. ADVISOR J. (Nov. 30, 2015), https://www.lexisnexis.com/lexis-practice-advisor/the-journal/b/lpa/archive/2015/11/30/drafting-and-negotiating-effective-cloud-computing-agreements.aspx#sthash.ksUI2geK.dpuf [https://perma.cc/ACJ2-XUWX]; Jessica Hughes, *Data Breaches in the Cloud: Who's Responsible?*, GOV'T TECH. (Aug. 26, 2014), http://www.govtech.com/security/Data-Breaches-in-the-Cloud-Whos-Responsible.html [https://perma.cc/B9P6-UVJF]; Kaiser Wahab, *Cloud Service Contracts: Breaking Down the All Important Service Level Agreement (SLA)*, SECURITY ADVOC. (Mar. 20, 2013), http://www.thesecurityadvocate.com/2013/03/20/cloud-service-contracts-breaking-down-the-all-important-service-level-agreement-sla [https://perma.cc/5UDT-85HP].

205 PONEMON INST., *supra* note 16, at 2 (finding that the average total organizational cost from a data breach in the United States was $7.01 million). Costs do vary enormously, however, by the amount of data lost—for breaches of fewer than 10,000 records, the average total cost is $2.1 million. *Id.* at 15.

206 *See* Bortnick, *supra* note 203.

207 *Id.*

208 *See, e.g.*, *Google Cloud Platform Terms: Data Processing and Security Terms* § 7.1, 7.5, GOOGLE, https://cloud.google.com/terms/data-processing-terms [https://perma.cc/ZPD4-SAP6]. This is, unsurprisingly, another area where customer-oriented experts recommend pushing for better terms. *See, e.g.*, ROSENFELD & HUTNIK, *supra* note 204, at 13 (recommending contractual obligation for service provider to notify customers in the event of a data breach).

the wrong or loss by paying out its policy to the insured.[209] Subrogation is fundamentally a doctrine of equity, applying beyond the insurance context.[210] It can also be provided for in contractual form.[211] Ideally, subrogation is a way of smoothing out the rough edges of risk by allowing the victim of loss to be insured while, at the same time, providing incentives for the long-term reduction of that risk by suit against the wrongdoer.[212] These complementary incentives are carefully balanced—if any of the three involved parties (the insurance company, the data-collecting company, and the data-storage provider) can disclaim their responsibility, the entire scheme is upset. "[P]arties contract to benefit themselves, and the consequences a contract may have on third parties is of minimal importance . . . unless, of course, such consequences impose liability on the contractors."[213]

Cyber-insurance policies may already have terms establishing the subrogation right of the insurer against a wide range of parties, including data-storage providers.[214] Recognizing that subrogation is meaningless if there is no claim to take up, subrogation provisions typically impose a duty on the insured to refrain from interfering with the insurer's enforcement rights, including both an affirmative duty to cooperate with the insurer by producing evidence and witness testimony[215] and a negative covenant to refrain from unilateral settlement of the claim.[216] As the insurer is taking the place of the insured, the insurer cannot assert any claim greater than what the insured had.[217]

---

209 Gregory R. Veal, *Subrogation: The Duties and Obligations of the Insured and Rights of the Insurer Revisited*, 28 TORT & INS. L.J. 69, 69–70 (1992).

210 Am. Sur. Co. of N.Y. v. Bethlehem Nat'l Bank, 314 U.S. 314, 317 (1941) ("[O]ne who has been compelled to pay a debt which ought to have been paid by another is entitled to exercise all the remedies which the creditor possessed against that other.") (quoting HENRY N. SHELDON, THE LAW OF SUBROGATION 15 (1893).

211 Veal, *supra* note 209, at 70.

212 *See* Brendan S. Maher & Radha A. Pathak, *Understanding and Problematizing Contractual Tort Subrogation*, 40 LOY. U. CHI. L.J. 49, 63 (2008). The authors also describe a parallel practice of "reimbursement," in which insurers recover against the insured for money received from the wrongdoer above the insurance payout, to prevent double recovery. *Id.* Because data-storage customers already face problems recovering at all against providers, this approach is less promising.

213 *Id.* at 83.

214 Micah E. Skidmore, *Negotiating Coverage & Pursuing Claims Under Cyber-Security & Privacy Insurance*, J. TEX. INS. L., Spring 2015, at 27, 33.

215 *See* Patrick J. Collins & Mark J. Struthers, *Protecting the Insurer's Subrogation and Recovery Rights Throughout the Claim Investigation*, 20 FIDELITY L.J. 231, 250 (2014).

216 Veal, *supra* note 209, at 80.

217 *Id.* at 70.

Of course, there are natural business pressures that may reduce the problems of indemnification over time, as insurers and companies begin to realize the extent to which their claims are weakened. Companies may directly bargain for more favorable terms with their storage providers as the cost-benefit analysis for mitigating data-breach costs adjusts with the news of each new massive hack. Or, insurance companies may exert the same pressure indirectly, by demanding ever-increasing premiums, writing exclusions, or simply refusing service if the insured has such an imbalanced contract with a data-storage provider. As a compromise, both the company and the insurer may bargain for increased security guarantees and compliance, or an increased cap on damages from the data-storage provider. There is, however, a more direct route. In the nineteenth century, railroads and other common carriers also attempted to use various forms of indemnification to undercut the regime of heightened liability to which they were subject. Courts, however, struck down these devices as being against public policy.[218]

The crux of the public policy argument is that the ultimate victim is not the data-storage provider, its commercial partner, or the insurance company. It is the consumer, who becomes exposed to identity theft. When the ultimate negative effects of a data breach fall upon a consumer, weak security becomes no more than an externality in the financial negotiations between data-acquiring and data-hosting companies.[219] Although the consumer's monetary damages may be addressed and credit-monitoring services obtained, there are still great personal headaches associated with the fundamental uncertainty of identity theft.[220] Credit cards may suddenly have massive fraudulent charges or debit accounts may be drained of funds, causing immediate personal inconvenience even if the charges are later reversed.[221] A particularly brazen identity thief may supply stolen identification in-

218 *See* R.R. Co. v. Lockwood, 84 U.S. (17 Wall.) 357, 384 (1873); ABRAHAM, *supra* note 24, at 22–24. This doctrine has been modified but survives today, including in the Carmack Amendment, which governs liability in shipping. *See* 49 U.S.C. § 14706 (2018). Although today carriers are permitted to limit their liability, there are four required steps, including offering the shipper the ability to choose among clearly delineated levels of liability. *See* OneBeacon Ins. Co. v. Haas Indus., Inc., 634 F.3d 1092, 1099 (9th Cir. 2011).

219 *Cf.* ABRAHAM, *supra* note 24, at 59 (noting that when workers' compensation schemes were first enacted, nonunionized industries had little decrease in workplace accidents, and reasoning that employers avoided financial incentives to reduce accidents in such industries by passing on the costs of the new program to their employees through lower relative wages).

220 *See* 112 AM. JUR. TRIALS § 13 (2009) (listing various fraudulent uses of stolen personal identification information).

221 *See id.*

formation to the police if he or she is ever arrested as a way of escaping a later warrant, which may lead to an unexpected arrest and detention of the victim.[222]

As to the mechanism of such a policy, there are two primary approaches. The Restatement (Second) of Contracts ("Restatement") describes as unenforceable on public policy grounds certain terms that exempt parties from tort liability,[223] but the existing categories are too narrow to apply in this context. This is because although torts caused intentionally or recklessly are subject to total unenforceability, if caused negligently, unenforceability only applies to those terms that "exempt[] one charged with a duty of public service from liability to one to whom that duty is owed for compensation for breach of that duty."[224] At common law, public policy nullification includes a set of factors for courts to consider, including the nature of the specific transaction and, occasionally, the specific language used.[225] California, in particular, weighs whether the business is already subject to regulation, performs an important public service, provides such service openly to the public, holds a relative position of power in bargaining, offers a standardized contract without the option of extra protection, and ultimately takes control of the other's person or property.[226] In a data-breach context, although data-hosting services are often presented in a contract-of-adhesion context, the other factors may not necessarily be present. For example, between a data-collecting and a data-hosting company, there may be little to no disparity in bargaining position, with both sides employing qualified financial and legal analysts. Likewise, although certain data-hosting companies may make their services available to the public, others may be more narrowly specialized.[227] Finally, in this context, the owner of the property that the data-hosting company ultimately comes to possess is not the company's bargaining partner but the consumer.

Despite this facial difficulty, there are also, depending on the jurisdiction, powerful weapons on the side of nullification. For example, in the Tenth Circuit, clauses providing indemnity for one's own negli-

---

222 *See id.*

223 *See* RESTATEMENT (SECOND) OF CONTRACTS § 195 (AM. LAW INST. 1981).

224 *Id.* § 195(2)(b).

225 *See* 5 RICHARD A. LORD, WILLISTON ON CONTRACTS § 12:2 (4th ed. 2009).

226 *See* Tunkl v. Regents of Univ. of Cal., 383 P.2d 441, 444–46 (Cal. 1963).

227 *See, e.g.*, COUNCIL OF MED. SPECIALTY SOC'YS, CMSS PRIMER FOR THE DEVELOPMENT AND MATURATION OF SPECIALTY SOCIETY CLINICAL DATA REGISTRIES (2016), https://cmss.org/wp-content/uploads/2016/02/CMSS_Registry_Primer_1.2.pdf [https://perma.cc/AQR7-F3X4].

gence are "looked upon with disfavor" and require "clear and unequivocal language."[228]

As for the California requirement that the business be the subject of regulation, the existence of data-protection statutes in a number of states may apply equally to the data-storage provider, despite its not actually "owning" the data.[229] Furthermore, both state law and the FTC have an interest in forbidding deceptive practices, which may include misleading representations of security to the customer.[230] These indicate a fundamental interest on the part of the state in protecting personal information. Essentially, a storage provider's avoidance of liability as against the commercial customer implicates the ultimate ability of the state to promote increased data security.[231]

California's Security Breach Information Act offers an even more direct approach. The Act's purpose is to promote the security of personal data of California residents, and it explicitly provides consumers with a private right of action to enforce their rights.[232] Vitally, the Act also stipulates that waiver of any of its parts is void as contrary to public policy.[233] It stands to reason, then, that if customer suits against businesses with lax security promote public policy and cannot be prevented by waiver, so should company or subrogation suits against data-storage providers. This expansion need not be dramatic: the cur-

---

228 Kan. City Power & Light Co. v. United Tel. Co. of Kan., 458 F.2d 177, 179 (10th Cir. 1972); *see also* James F. O'Neil Co. v. U.S. Fid. & Guar. Co., 381 F.2d 783, 786 (5th Cir. 1967) ("[F]or while such a contract of indemnification is not strictly against public policy, it so nearly borders on the line, that a strict construction against the one to be indemnified for his own negligence is necessary." (quoting Zurich Gen. Accident & Liab. Ins. Co. v. Liberman, 71 N.E.2d 281, 285 (Ohio Ct. Com. Pl. 1947))). Interestingly, there may be a difference in the interpretation of limitation of liability clauses and complete indemnification clauses. *See* Valhal Corp. v. Sullivan Assocs., Inc., 44 F.3d 195, 202 (3d Cir. 1995).

229 *See, e.g.*, FLA. STAT. ANN. § 501.171(1)(b) (West 2016) ("'Covered entity' means a sole proprietorship, partnership, [or] corporation . . . that acquires, maintains, stores, or uses personal information."); TEX. BUS. & COM. CODE ANN. § 521.052(a) (West 2015) ("A business shall implement and maintain reasonable procedures . . . to protect from unlawful use or disclosure any sensitive personal information collected or maintained.").

230 *See, e.g.*, D.C. CODE § 28-3904(f-1) (2016) (listing specific violations, including to "[u]se innuendo or ambiguity as to a material fact, which has a tendency to mislead"); N.J. STAT. ANN. § 56:8-2 (West 2016) (forbidding deception, false pretense, concealment, etc., in general); *see also* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015); Kathryn F. Russo, *Regulation of Companies' Data Security Practices Under the FTC Act and California Unfair Competition Law*, 23 COMPETITION: J. ANTITRUST & UNFAIR COMPETITION L. SEC. ST. B. CAL., Spring 2014, at 201.

231 *See* KENNETH T. LEVINE & JEFFREY ZIELINSKI, NAT'L ASS'N SUBROGATION PROF'LS, CYBER SUBRO: DATA BREACH RISKS AND SUBROGATION, http://www.subrogation.org/download/article/CyberSubro4134.pdf [https://perma.cc/MM7R-35ER].

232 CAL. CIV. CODE §§ 1798.81.5(b), 1798.84(b) (West 2016).

233 *Id.* § 1798.84(a).

rent definition of a "customer"[234] who may sue for violations of the statute, and who may not waive the included requirement of reasonable security measures, should be expanded to legal as well as natural persons. This provision demonstrates the simplest way towards opening up liability—a statutory provision. Unlike the approach embodied in section 195 of the Restatement, which may give rise to varied balancing tests and interpretative schemes across states, a legislative provision clearly indicating that such disclaimers of liability involving the personal information of third parties are against public policy would have a more direct effect, and the Restatement distinctly contemplates turning to relevant legislation for guidance.[235]

Thus, the assertion of a firm public interest in data security can reach into private data-storage-provider contracts, lifting the constraints on liability that prevent effective subrogation. In fact, subrogation in the cyber context is already being considered by courts: in 2015, Travelers Casualty and Surety Company of America ("Travelers") filed on behalf of one of its clients against a web design company, alleging that hackers breached the client's website and released personal information, causing the client to incur notification costs and Travelers to pay out the policy, upon which they took up the client's claims of negligence and breach of contract.[236]

CONCLUSION

External hacks of consumers' personal information present a unique challenge to the traditional legal and insurance system. Although it is often difficult or nearly impossible to punish or deter the ultimate wrongdoer, creating proper incentives for mitigation requires careful balancing between the consumer, company, insurer, and third-party vendor. The government can greatly assist the development of this regime by collaboratively developing useful standards for private industries alongside regulations. Private rights of action and government civil fines help to reimburse the consumer for damage from identity theft, while carefully crafted cyber-insurance policies mitigate costs to the insured company. Finally, barring indemnification of third-party vendors would allow the insurer to recover some amount

234 *Id.* § 1798.80(c)–(d).

235 *See* RESTATEMENT (SECOND) OF CONTRACTS § 179(a) (AM. LAW INST. 1981).

236 Complaint, Travelers Cas. & Sur. Co. of Am. v. Ignition Studio, Inc., No. 15-0608 (N.D. Ill. Jan. 21, 2015), 2015 WL 672169. Reportedly, the case settled for an undisclosed amount. *See* Richard Bortnick, *Cyber Subrogation, Finally*, ADVISEN (Apr. 29, 2015), http://www.advisenltd.com/2015/04/29/cyber-subrogation-finally [https://perma.cc/4C3L-FCPJ].

from the vendor, depending on the vendor's liability in the data breach, and properly exert pressure on the party with physical control of the data to protect it. The constant development of networking technology means the threat from external hacks may never be definitively overcome, but interested stakeholders, working together, can go a long way towards making sure that, whatever victories the hackers are able to accomplish, the system remains resilient.