# Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System

*Jeff Kosseff**

## INTRODUCTION

"Tell me about U.S. cybersecurity law," a British colleague requested at a recent conference. It seemed like an easy question, but it wasn't. I paused for far too long to think about it.

That's because there isn't a single U.S. law that comprehensively addresses cybersecurity. The Federal Trade Commission Act prohibits "unfair or deceptive acts or practices in or affecting commerce,"[1] and the Federal Trade Commission ("FTC") uses that law to penalize companies with inadequate data security protections.[2] Every state has a similar law, and most states also have passed laws that require companies to notify customers and regulators after data breaches. But those are narrow, punitive rules that deal with data breaches after the fact and don't really focus on cybersecurity as a whole.

We have a number of statutes that focus on consumer information, including: the Children's Online Privacy Protection Act,[3] which regulates the collection of information from minors under thirteen; the Video Privacy Protection Act,[4] which restricts the sharing of consumers' video viewing information; and the Gramm-Leach-Bliley Act,[5] which governs the disclosure of financial account data. But these statutes regulate *privacy,* not cybersecurity.

The military has released a cyber strategy which is compromised of quite a few cyber-defense missions,[6] but those

---

* Assistant Professor of Cybersecurity Law, U.S. Naval Academy, Annapolis, Maryland. The views expressed in this Article are only those of the author, and not of the Naval Academy or Department of Navy.

1 15 U.S.C. § 45(a)(1) (2012).

2 *See* FED. TRADE COMM'N, 2014 PRIVACY AND DATA SECURITY UPDATE (2014), www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf [http://perma.cc/U73Q-PF9Q].

3 15 U.S.C. §§ 6501–6506.

4 18 U.S.C. § 2710 (2012).

5 15 U.S.C. §§ 6801–6809.

6 *See, e.g.*, *The Department of Defense Cyber Strategy*, U.S. DEP'T DEF., http://

apply only to military operations. The Department of Homeland Security ("DHS") also has a strategy comprised of a number of goals and objectives,[7] but those primarily involve government infrastructure. The National Institute of Standards and Technologies has released helpful guidelines,[8] but those are, of course, only guidelines and do not have the binding force of law.

After pausing for far too long, I said, "We don't really have any cybersecurity laws." What we have, instead, is a patchwork of related laws, including breach notification and privacy statutes, that focus on penalizing companies for inadequate data security. But our legal system lacks a coordinated network of laws that are designed to promote cybersecurity and prevent data breaches from occurring in the first place.

This Article seeks to address this shortfall by articulating a consistent system of laws that would promote cybersecurity. Part I of the Article defines cybersecurity from a legal standpoint, and distinguishes it from concepts such as privacy and data security. Many laws that purport to encourage cybersecurity are, in fact, designed with a focus on protecting privacy or encouraging data security. Unlike privacy and data security, cybersecurity is focused not only on the information, but the entire system and network. For this reason, laws that focus only on privacy and data security may not consider all factors necessary to promote cybersecurity. By clearly defining the term, I hope to provide policymakers with clarity as they develop laws aimed at promoting cybersecurity.

Part II examines the patchwork of state and federal privacy and data security laws that are most commonly associated with cybersecurity, including data breach notification laws and data security requirements. These requirements have been the bedrock of U.S. cybersecurity law, yet they are ineffective at preventing cybersecurity incidents. For instance, companies that have experienced a data breach must devote significant resources to determining whether—and how—to satisfy the various notification requirements. This Article evaluates the efficacy of such a system, based on available data about cybersecurity incidents, and concludes that the current legal system contains a number of gaps that do not adequately address cybersecurity threats.

---

www.defense.gov/News/Special-Reports/0415_Cyber-Strategy [http://perma.cc/S7AT-GT47].

7 *See, e.g.*, DEP'T OF HOMELAND SEC., BLUEPRINT FOR A CYBER FUTURE: THE CYBER SECURITY STRATEGY FOR THE HOMELAND SECURITY ENTERPRISE (2011), www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf [http://perma.cc/GH9Y-V76Z].

8 *See Cybersecurity Framework*, NAT'L INST. STANDARDS & TECH., http://www.nist.gov/cyberframework/ [http://perma.cc/7K8W-J6CF] (last updated Dec. 11, 2015).

Part III of the Article draws from other areas of law to suggest a unitary framework that could provide strong, clear, and adaptable cybersecurity laws and policies. Frist, policymakers should consider centralizing cybersecurity responsibilities within a single federal agency, rather than scattering them among the FTC, fifty state attorneys general offices, and other agencies. Such a structure would allow specialized employees and leaders to shape the nation's cybersecurity defense system. Second, policymakers should reconsider the current system's focus on punitive measures, such as fining companies for failing to adequately notify customers of data breaches. While penalties always will be a necessary component of a cybersecurity law, our laws also should include incentives for companies to invest in costly cybersecurity protections. Among the policies that lawmakers might consider are tax credits for cybersecurity investments, a national cybersecurity insurance program, and a safe harbor from data security lawsuits for companies that adhere to a rigorous set of government-mandated security standards. This Article considers the theories that support including incentives, rather than only penalties, in a policy framework. It will also examine how the government has used such incentives in other areas, and how these incentives might advance cybersecurity goals.

I refer to this concept as "positive cybersecurity law"—policies designed to encourage cybersecurity before a malicious attack occurs. This requires a shift in thinking from our nation's longstanding mindset in which nearly all cybersecurity laws are punitive. While such regulations always play a role in cybersecurity, our system should be a mix of punitive *and* positive law. The unique design of cyberspace—interconnected networks of public and private infrastructure—demands a collaborative, rather than adversarial, relationship between the government and industry. A combination of "carrots" and "sticks" would most effectively encourage investments in cybersecurity.

## I. WHAT IS CYBERSECURITY?

A logical starting point for our discussion is a definition of cybersecurity. Although the term is commonly used by the press and policymakers, its precise scope often varies.

In the private sector, cybersecurity often is associated with data breaches. Indeed, a large portion of the cybersecurity industry is dedicated to helping companies prevent data breaches

and remediate the harm after a breach has occurred. Worldwide, the cybersecurity industry was estimated to generate $75.4 billion in 2015.[9] Companies are understandably concerned about the exposure of their customers' and employees' personal information, both because of potential legal liability and damage to their brand. Moreover, data breaches may expose a company's trade secrets or other confidential business information that could lead to significant financial harm to the company. Accordingly, data security is an integral part of the cybersecurity ecosystem.

However, data theft is only one aspect of cybersecurity. Cybersecurity professionals also help companies prevent the destruction or inaccessibility of data. Moreover, cybersecurity involves the *protection* of networks and systems from damage. In other words, cybersecurity aims to safeguard the confidentiality, integrity, *and* accessibility of data (commonly known as the "CIA" triad).[10]

Cybersecurity involves the protection of both private *and* public networks. Too often, policymakers and companies talk about "private-sector cybersecurity" and "public-sector cybersecurity." The open architecture of the Internet makes it futile to focus *only* on private-sector concerns, such as trade secret theft, or *only* on public-sector concerns, such as cyberattacks by other nation-states. For instance, North Korea's hack of Sony in 2014 implicated not only Sony's business interests and assets, but U.S. national security and international relations, leading President Obama to impose sanctions.[11] Similarly, if a cyberattack were to target U.S. government infrastructure, private companies likely would be affected. Accordingly, policymakers must look at cybersecurity in both the private *and* public sectors at the same time.

These goals are best reflected in the National Initiative for Cybersecurity Careers and Studies' ("NICCS")[12] definition of cybersecurity as "[t]he activity or process, ability or capability, or state whereby information and communications systems and the

---

9 Tara Seals, *Cybersecurity Spending to Hit $170Bn by 2020*, INFOSECURITY MAG. (July 13, 2015), http://www.infosecurity-magazine.com/news/cybersecurity-spending-to-hit/ [http://perma.cc/WJQ4-FZ59].

10 *See* Chad Perrin, *The CIA Triad*, TECHREPUBLIC (June 30, 2008, 8:13 AM), www.techrepublic.com/blog/it-security/the-cia-triad/ [http://perma.cc/8923-QKKT].

11 *See* Dan Roberts, *Obama Imposes New Sanctions Against North Korea in Response to Sony Hack*, GUARDIAN (Jan. 2, 2015, 4:08 PM), http://www.theguardian.com/us-news/2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-the-interview [http://perma.cc/6WXC-PRGX].

12 NICCS is a resources of cybersecurity information managed by DHS.

information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation."[13] Under this definition, cybersecurity involves the protection of both data and systems. The definition also does not apply separate standards for public and private systems. The NICCS definition serves as a useful starting point as we determine how to meet the goals of cybersecurity.

Importantly, cybersecurity and privacy are *not* one in the same. The modern legal concept of privacy emerged in Samuel D. Warren and Louis D. Brandeis' 1890 *Harvard Law Review* article, *The Right to Privacy*.[14] They defined privacy as "the right 'to be let alone,'"[15] reasoning that common law right to property "has grown to comprise every form of possession—intangible, as well as tangible."[16] Privacy, therefore, involves individuals' ability to control their personal data. Strong, proactive cybersecurity measures help to promote privacy by reducing the likelihood of unauthorized disclosure. However, there are a number of other avenues in which privacy can be protected, such as by providing individuals with choice about the collection and sharing of their data. Unfortunately, cybersecurity and privacy often are used interchangeably, leading some to the mistaken belief that privacy-focused laws also will promote cybersecurity.

Why does the definition matter? If our goal is to promote cybersecurity, we should have a clear idea of what exactly cybersecurity is. As I will describe in Part II, many of our laws that purport to promote cybersecurity do very little to accomplish that goal. Some areas of cybersecurity could benefit from new laws, but often those areas are entirely unaddressed in the current political debate at the federal and state levels. To assess whether our current laws advance the goals of cybersecurity, using the NICCS definition, we must examine whether they protect systems, networks, and data from damage, unauthorized use or modification, or exploitation.

---

13 *Explore Terms: A Glossary of Common Cybersecurity Terminology*, NAT'L INITIATIVE CYBERSECURITY CAREERS & STUD., www.niccs.us-cert.gov/glossary [http://perma.cc/Z2CL-33K3].

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

15 *Id.* at 195 (quoting THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT (2d ed. 1888)).

16 *Id.* at 193.

## II. THE CURRENT STATE OF CYBERSECURITY LAW

As discussed above, the United States does not have a cohesive cybersecurity legal framework. Instead, it had a patchwork of laws that address some aspects of data security. These laws fail to work together harmoniously, occasionally conflict, and do little to ensure the future security of data, networks, and systems. The current legal system largely is backward-looking, and provides companies and the public sector little guidance as to how to prevent future cybersecurity incidents.

### A. Breach Notification Laws

Forty-seven states and the District of Columbia have enacted data breach notification laws since 2002.[17] These laws require companies and government agencies to notify individuals that their personal information has been compromised. The laws vary significantly in scope. For instance, most laws are triggered if the individual's name is compromised, along with a financial account number, Social Security number, or driver's license number. However, some notification laws cover additional categories of information, such as medical data[18] and birth dates.[19] Some states only require notification if the company determines that the disclosure poses a reasonable risk of harm to the individuals,[20] while other states require notification regardless of the actual risk.[21] The required content and form of breach notices also vary by state. Breach notification laws apply to the state's residents, and most companies have customers in all fifty states. Accordingly, if a company experiences a data breach, it must devote significant time and staff to determining the states in which it must notify residents and regulators, as well as the timing, form, and substance of the notification. That time and money could be better spent on measures to mitigate the harm of the breach and to prevent future incidents from occurring.

Furthermore, it is unclear whether the data breach notice fulfills its intended purpose. Individuals are informed of data breaches weeks or months after the initial exposure. By the time that they receive the notice, identity theft and other damage

---

17 *See Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Oct. 22, 2015), www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [http://perma.cc/U4RK-4DDE].

18 CAL. CIV. CODE §§ 1798.29(g)(1)(D), 1798.82(h)(1)(D) (West 2016).

19 N.D. CENT. CODE § 51-30-01(4)(a)(5) (West 2016).

20 *See, e.g.*, COLO. REV. STAT. § 6-1-716 (West 2016).

21 CIV. § 1798.82.

likely already has occurred. The notices typically direct the individuals to obtain free credit reports, and some companies offer additional identity theft protection services. However, few customers actually use these services when offered.[22] Moreover, the rationale for data breach notification laws is outdated. States began passing data breach notification laws in 2002, when large-scale data breaches were relatively uncommon. The size, number, and scope of data breaches have increased exponentially in recent years. In a 2014 survey of executives, the Ponemon Institute found that 43% experienced a data breach in the past year, up from 33% in a 2013 survey.[23] Individuals should operate under the assumption that their data has been breached; therefore, they would be wise to take precautions such as changing passwords, checking their free annual credit reports, and routinely updating their computer anti-virus software and operating systems. Although data breaches may have been rare a decade ago when the breach notice laws were first enacted, breaches now are commonplace.

Although there is some value in notifying individuals of data breaches, this should not be the primary focus of cybersecurity law. Once a data breach has occurred, much of the harm is inevitable, regardless of whether customers have been notified. It would be far more productive if companies were able to devote all of their time and expertise to forensics: figuring out how the breach occurred, and how to prevent it from occurring again.

Unfortunately, our cybersecurity legal framework focuses heavily on breach notification laws. This is an outdated and increasingly futile exercise that adds unnecessary expense and slows companies' ability to respond to data breaches.

### B. FTC Data Security Enforcement and State Data Security Laws

Many people are surprised to learn that the United States does not have a national law that sets specific data security standards. Instead, the FTC uses its general consumer protection regulatory authority to bring enforcement actions against companies that it believes have failed to adequately safeguard personal information. The FTC asserts this authority under section 5 of the Federal Trade Commission Act, which allows the

---

22 *See* Jeff Kosseff, *Notified About a Data Breach? Too Late*, WALL ST. J. (Oct. 9, 2015, 7:04 PM), http://www.wsj.com/articles/notified-about-a-data-breach-too-late-1444345445.

23 Elizabeth Weise, *43% of Companies Had a Data Breach in the Past Year*, USA TODAY (Sept. 24, 2014, 3:33 PM), http://www.usatoday.com/story/tech/2014/09/24/data-breach-companies-60/16106197/ [http://perma.cc/U7AN-A2TL].

FTC to prevent companies from using "unfair or deceptive acts or practices in or affecting commerce."[24] Often, the FTC alleges that a company's lax data security practices constitute "unfair" trade practices.

For decades, there has been confusion as to what makes a trade practice "unfair." In 1964, the FTC issued guidance in which it stated that the following factors determine whether a trade practice was unfair:

> (1) whether the practice, without necessarily having been previously considered unlawful, offends public policy as it has been established by statutes, the common law, or otherwise—whether, in other words, it is within at least the penumbra of some common-law, statutory, or other established concept of unfairness; (2) whether it is immoral, unethical, oppressive, or unscrupulous; [and] (3) whether it causes substantial injury to consumers (or competitors or other businessmen).[25]

Over the next two decades, critics questioned whether the FTC is in the best position to determine whether trade practices are "immoral" or "unscrupulous," leading the FTC to gradually change its analysis to focus on the harm and benefits to customers. Congress codified this new approach in 1994, amending the Federal Trade Commission Act to define "unfair" as a practice that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[26]

The FTC also has alleged that security practices that violate companies' privacy policies constitute deceptive trade practices under the Federal Trade Commission Act. Between 2002 and 2014, the FTC brought more than fifty cases against companies whose security and privacy practices, it claimed, were unfair or deceptive.[27] Typically, companies settle these enforcement actions before they go to court, agreeing to a consent order that, among other things, allows the FTC to closely oversee the companies' data security practices.[28]

---

24 Federal Trade Commission Act § 5(a)(1), 15 U.S.C. § 45(a)(1) (2012).

25 Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8324, 8355 (July 2, 1964).

26 15 U.S.C. § 45(n).

27 *See* GINA STEVENS, CONG. RESEARCH SERV., R43723, THE FEDERAL TRADE COMMISSION'S REGULATION OF DATA SECURITY UNDER ITS UNFAIR OR DECEPTIVE ACTS OR PRACTICES AUTHORITY 6 (2014).

28 *See* PATRICIA BAILIN, IAPP, STUDY: WHAT FTC ENFORCEMENT ACTIONS TEACH US ABOUT THE FEATURES OF REASONABLE PRIVACY AND DATA SECURITY PRACTICES, https://iapp.org/media/pdf/resource_center/FTC-WhitePaper_V4.pdf [http://perma.cc/8VWV-85N7].

Because section 5 of the Federal Trade Commission Act does not explicitly mention data security, some critics have asserted that the FTC lacks jurisdiction to bring data security enforcement actions. Among the most vocal opponents of such actions is Wyndham Worldwide Resorts, which was hacked in 2008 and 2009.[29] After investigating the attacks, the FTC brought an enforcement action against Wyndham, alleging that Wyndham's data security measures were inadequate and, therefore, unfair, and that the company deceived customers by failing to provide the security measures that it guaranteed in its privacy policy.[30] Among the practices that the FTC found most objectionable was the storage of credit card information in clear text, the lack of a requirement for complex passwords on Wyndham's computer systems, and Wyndham's failure to use firewalls and other common data security solutions.[31]

Unlike most companies that face an FTC data security enforcement action, Wyndham did not settle with the FTC. Instead, the FTC brought a civil action against Wyndham in the U.S. District Court for the District of New Jersey.[32] Wyndham moved to dismiss the case, arguing that the Federal Trade Commission Act does not give the FTC the authority to regulate data security.[33] Wyndham noted that Congress has passed statutes that provide the FTC with the authority to regulate cybersecurity in particular areas, including financial institutions, websites that collect information from children under thirteen, and credit agencies. Accordingly, Wyndham argued, such "tailored grants of substantive authority to the FTC in the cybersecurity field would be inexplicable if the Commission already had general substantive authority over this field."[34] The district court rejected this argument, and on appeal, the U.S. Court of Appeals for the Third Circuit agreed. The court reasoned that all of those tailored laws served different purposes than the general Federal Trade Commission Act, and therefore, "none of the recent privacy legislation was 'inexplicable' if the FTC already had some authority to regulate corporate cybersecurity through § 45(a)."[35] The Third Circuit also rejected Wyndham's argument that the FTC's numerous attempts to convince Congress to enact laws that provide it with specific data

29 FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015).
30 *Id.*
31 *Id.* at 241.
32 *Id.* at 242.
33 *Id.*
34 *Id.* at 247.
35 *Id.* at 248.

protection powers demonstrates that section 5 does not provide it with such authority.

Wyndham also argued that the FTC failed to provide clear data security standards with "ascertainable certainty,"[36] in violation of the Due Process Clause. The court also rejected this argument, concluding that Wyndham was not entitled to ascertainable certainty. Instead, the court concluded, "the relevant question in this appeal is whether Wyndham had fair notice that its conduct could fall within the meaning of the statute."[37] Wyndham, the court wrote, is "only entitled to notice of the meaning of the statute and not to the agency's interpretation of the statute."[38]

The *Wyndham* case is important because it demonstrates two primary flaws with the FTC's data security enforcement. First, *Wyndham* raised valid questions about whether section 5 of the Federal Trade Commission Act provides the FTC with authority to regulate data security. The Third Circuit is the only federal appellate court to rule on the issue, so there is a very real chance that another circuit would disagree, creating a circuit split that ultimately would be resolved by the U.S. Supreme Court. Second, and more importantly, *Wyndham* demonstrated that the FTC provides little concrete guidance as to what constitutes adequate data security. This is perhaps the most significant shortcoming with the FTC's current data security enforcement system. Even if a company is well-intentioned and attempts to comply with all applicable data security laws, it has no guarantee that the FTC would believe that its efforts are adequate. What kinds of data should be encrypted in transit and at rest? What level of encryption should a company use? How often should companies require employees to reset passwords? How long should passwords be? Should a company use two-factor authentication for remote access? What about in-office access? How often should companies provide cybersecurity training to employees? Should a company design an incident response plan? These are just some of the many questions that companies have on a routine basis. Binding, concrete guidance on these issues would be incredibly helpful, and likely would increase the overall number of cybersecurity measures that companies put in place. If a company knows that a cybersecurity safeguard will help to satisfy regulators' expectations, the investments in that safeguard will be easier to justify.

---

36 *Id.* at 253–54.
37 *Id.* at 255.
38 *Id.*

Approximately a dozen states have supplemented the FTC's general data security enforcement with laws that impose data security requirements on companies that process the data of the state's residents.[39] However, most of these laws simply require a company to develop "reasonable" security, providing no more certainty than the FTC. The two exceptions are Nevada, which requires compliance with payment card industry data security standards, and Massachusetts, which requires companies to develop detailed data security plans in writing.[40] However, these state-level laws do little to address the significant uncertainty that arises due to the lack of nationwide, concrete standards for data security. Furthermore, if other states follow their lead and enact their own specific data security regulations, companies would be forced to apply a number of different data security standards, based on the state in which the individual lives. Why should, say, the personal data of a Massachusetts resident receive more protection than the data of a New Hampshire resident? Cybersecurity simply is not an area where state-level regulation is effective.

## III. A POSITIVE, UNITARY FRAMEWORK

Now that we have a better idea of the concepts that are involved in cybersecurity and the shortcomings of the current legal framework, we can begin to create a legal framework that provides companies with the certainty necessary to invest heavily in cybersecurity.

Cyberspace, by its very architecture, is a network of both private-sector and public-sector infrastructure. Unlike traditional regulatory areas, such as food safety, where the government is more than an overseer of the private sector, the government is a partner *with* the private sector. The government developed the initial infrastructure of the Internet, and the private sector invested billions of dollars to build that initial infrastructure into the transformative force that it is today. Accordingly, unlike other areas, in which traditional top-down regulation is effective, cybersecurity requires a different mindset. Cybersecurity requires a continuation of the partnership between the government and companies. Indeed, an insecure Internet harms the private sector by slowing the growth and progress of the

---

39 Hogan Lovells, *Outlook for State Data Security Laws: More than Breach Notification*, IAPP (Dec. 16, 2014), https://iapp.org/news/a/outlook-for-state-data-security-laws-more-than-breach-notification [http://perma.cc/2VX5-FJJ3].

40 *Id.*

Internet; it is in the best interests of every company to work with the government for a more secure cyberspace.

In line with that collaborative mindset, below are four suggested starting points for building such a legal framework. I note that I do not address whether Congress should immunize companies from liability arising from sharing cyberthreat information with the federal government. Such proposals are subject to significant debate among policymakers, companies, and privacy advocates. The goal of this Article is to highlight policies that have not received as much public attention and debate.

### A. Create a Safe Harbor for Responsible Cybersecurity

As I argued in the previous section, the FTC's current data security enforcement provides little certainty for well-intentioned companies that would like to comply with all legal requirements. Ideally, the FTC would issue specific regulations that set minimum standards such as password lengths, firewall capabilities, and categories of data that require encryption in transit and at rest.

A likely response to such a proposal is that every data security incident involves unique circumstances, and therefore, it is impossible to provide minimum standards that apply in all circumstances. For instance, costly firewalls may be more necessary for companies that handle sensitive information, such as health records, and may be more affordable for larger companies than for smaller companies. Moreover, larger companies are more likely to be able to afford dedicated information security staff.

Point taken. It would be difficult to proscribe nationwide, minimum data security standards for all companies. Such rules could lead to unreasonable penalties for small companies, or those that do not typically process significant amounts of personal information and, therefore, are not in a position to make significant investments.

Instead of setting a national minimum cybersecurity standard, Congress should pass a law that directs the FTC to develop cybersecurity criteria for a national safe harbor program. If a company demonstrates, through an annual independent audit, that it has satisfied all of those safe harbor criteria, then it cannot be the subject of a regulatory action or lawsuit—at either the federal or state level—arising from a data breach or another cybersecurity incident, unless the regulator or plaintiff can demonstrate that the breach was due to the company's intentional actions or gross negligence.

A safe harbor program would provide companies with significant incentive to make costly investments in cybersecurity hardware, software, and staff. Although companies would not be required to make these investments, doing so would provide them with reasonable certainty that they would be protected from lawsuits and regulatory actions.

In fact, this would not be the first technology-related safe harbor. The Digital Millennium Copyright Act ("DMCA") addresses concerns about online copyright piracy by granting Internet service providers and websites with immunity for copyright infringement claims arising from their users' actions, contingent upon the providers removing the infringing content upon receiving notice.[41] The DMCA safe harbor affords service providers with a significant incentive to remove infringing content.

Critics likely would argue that the safe harbor would unfairly shield companies from being held responsible for data breaches that are caused by their inadequate security. Such criticism would fail for two reasons. First, companies still could face regulatory actions and lawsuits if they are found to have been grossly negligent. The safe harbor would not provide an absolute shield; rather, it would provide companies with qualified protection in exchange for upfront investments in cybersecurity. Even if a company has qualified for the safe harbor, significant lapses could lead to its being held responsible in court or before a regulatory agency.

Second, the statute should direct the FTC to set very high standards for companies to qualify for the safe harbor. These should not be the minimum necessary safeguards for cybersecurity; instead, the safe harbor should only reward companies that invest in and implement the best of the best cybersecurity safeguards, as determined by the FTC. The safe harbor requirements should be designed to be difficult to achieve; qualified protection from lawsuits and regulatory actions is incredibly valuable, and companies should be required to meet a very high bar before receiving that protection.

The failure of a number of technology-related laws is that they do not quickly adapt to new changes in technology. For instance, Congress took years to update the Video Privacy Protection Act, which restricts the disclosure of video rental information, to address online streaming video services such as

---

41 17 U.S.C. § 512 (2012).

Netflix.[42] Congress often takes years to pass Legislation; by the time that a technology-related bill has been enacted, there is a good chance that it will be outdated. For that reason, the FTC—and not Congress—should set specific safe harbor requirements in regulations, and routinely update those requirements. The FTC is better positioned than Congress to set these requirements because it has more technical expertise, and promulgating regulations typically takes less time than passing a new statute.

B. Create a Nationwide Breach Notification Standard

As described in Part II of this Article, I question the utility of data breach notifications. Complying with the specific notification rules of forty-seven states and the District of Columbia is time-consuming, and there is no demonstrable evidence that notifications actually mitigate the harm caused by data breaches. However, eliminating breach notifications altogether likely would face significant opposition from privacy advocacy groups. Politically, such a change likely would be a non-starter.

As a compromise, Congress should pass a national data breach notification law that preempts the state notification laws. By creating a single standard, companies would no longer be forced to analyze the dozens of different procedures and definitions in the state laws. Individuals still would receive notice of significant breaches, but the process would be far less time-consuming for companies, allowing them to focus their time and resources on preventing further damage from the breach.

The specific requirements of a national data breach notification law likely would be subject to intense debate and negotiation among companies and privacy advocates. Below are the key elements that a national breach notification law should address:

**Risk of harm:** Some state breach notification laws only require companies to notify individuals if they determine that there is a reasonable likelihood that the breach will lead to harm, such as identity theft. Other state laws require notice in all circumstances, even if there is no risk of harm. Ideally, a national breach notice law would only require companies to notify individuals if there is some risk of identity theft or other harm. If there truly is not a risk of harm, it would be counterproductive to notify and unnecessarily scare customers. Moreover, if customers

---

42 Video Privacy Protection Act Amendments Act of 2012, Pub. L. No. 112–258, 126 Stat. 2414 (codified at 18 U.S.C. § 2710(b)(2)).

receive too many breach notices, they will be less likely to take the notices seriously.

**Definition of "personal information":** Similarly, the federal law should only apply to breaches of sensitive categories of personal information. Social Security numbers, unencrypted credit card numbers, and other information that could be used in identity theft should fall within the scope of the law. However, breaches that only disclose a name or email address likely do not present significant risk.

**Minimum number of affected individuals:** A small breach, involving only a few individuals, should not trigger a nationwide breach notification. The federal breach law should only apply if a minimum number of people—such as 500 or 1000—are affected.

**Encryption:** Like every state breach notice law, the federal law should not apply if the information was encrypted.

**Length of time:** Companies should be required to notify individuals of data breaches only after the companies have had an opportunity to investigate the incident and fully remediate the harm. A company's first priority should be preventing further breaches or damage.

C. Provide Tax Incentives for Cybersecurity

Very little public debate about cybersecurity has focused on the use of tax incentives to promote investments. That should change. The federal tax code offers tax incentives for education, wind energy, electric vehicles, and other areas that the government has determined to be a priority for investment.[43] Yet the tax code does not provide a penny in tax incentives for investments in cybersecurity.

This is partly due to the nascence of the cybersecurity field. The federal tax code received its last comprehensive overhaul in 1986, decades before cybersecurity emerged as a common term and serious challenge. However, the failure also is due to fiscal concerns. In response to an Executive Order directing departments to analyze potential cybersecurity policies, the Treasury Department wrote that tax incentives for cybersecurity "would come at the expense of foregone revenue for the government or reallocation of existing fiscal obligations," and recommended against further consideration of tax incentives.[44]

---

43 *See generally Credits and Deductions*, IRS, https://www.irs.gov/Credits-&-Deductions [http://perma.cc/K9DP-PNCE] (last updated Feb. 1, 2016).

44 *See* TREASURY DEP'T, SUMMARY REPORT TO THE PRESIDENT ON CYBERSECURITY

The Treasury Department is correct that, in the short term, tax incentives may result in a reduction in revenues to the federal government. However, such a view is short-sighted. If structured properly, tax incentives could dramatically increase companies' investments in cybersecurity safeguards, preventing costly data breaches and stimulating economic growth. Indeed, a report by the Atlantic Council estimates that an insecure Internet would reduce global economic net benefit by $90 trillion; a fully secure Internet would lead to a net gain of $190 trillion.[45]

Cybersecurity tax incentives could be structured in a number of different ways. The government could provide companies with a tax credit for investments in qualified cybersecurity expenditures up to a certain annual amount. The challenge for policymakers will be agreement on which cybersecurity investments qualify for the tax credit. An effective program would broadly include hardware, software, services, and staffing that help to promote the confidentiality, integrity, and accessibility of systems, networks, and data, consistent with the definition of "cybersecurity" in Part I of this Article. Policymakers also would need to determine the maximum size of cybersecurity tax credits. A $50,000 annual tax credit may provide a significant incentive for a small business to invest in cybersecurity, but that credit would be a rounding error for the budget of a Fortune 500 company. Accordingly, the maximum tax credit could be tied to an objective measure of a company's size, such as its annual revenues or number of employees.

Alternatively, the federal government could provide a tax credit that encourages investments in cybersecurity companies. This could be modeled after a Maryland program that provides a 33% tax credit for investments of up to $250,000 in certain cybersecurity businesses.[46] Such a program, at the national level, likely would lead to an increase in cybersecurity innovation.

### D. Offer National Cybersecurity Insurance

After a data breach, companies often are surprised to learn that their general commercial insurance policies may not cover

---

INCENTIVES PURSUANT TO EXECUTIVE ORDER 13636 (2013).

45 *Atlantic Council / Zurich Insurance Report Finds the Global Benefits of Cyber Connectivity Expected to Outweigh Costs by $160 Trillion Through 2030*, ATLANTIC COUNCIL (Sept. 9, 2015), http://www.atlanticcouncil.org/news/press-releases/atlantic-council-zurich-insurance-report-finds-the-global-benefits-of-cyber-connectivity-expected-to-outweigh-costs-by-160-trillion-through-2030 [http://perma.cc/RE9P-KESC].

46 *See Cybersecurity Investment Incentive Tax Credit (CIITC)*, MD. DEP'T COM., http://commerce.maryland.gov/fund/programs-for-businesses/cyber-tax-credit [http://perma.cc/QHP9-VX4B].

the expenses involved with remediation and defending against legal claims.[47] Some insurers have developed cybersecurity insurance policies that specifically insure companies for certain cybersecurity events. So far, the policies have received lukewarm reviews from companies and the cybersecurity community due to the cost and the number of exclusions that apply if companies have not implemented adequate safeguards.[48] DHS has conducted workshops and issued reports on the "nascent" cybersecurity insurance market, and insurers told DHS that their cybersecurity offerings are limited due to "a lack of actuarial data; aggregation concerns; and the unknowable nature of all potential cyber threat vectors."[49] These problems have placed cybersecurity insurance out of reach for many companies. In a 2015 survey of small businesses, Endurance International Group found that although 81% of small business owners are concerned about cybersecurity, only 5% of the small businesses have purchased cybersecurity insurance.[50]

This coverage gap provides an opportunity for policymakers to give companies more protection from catastrophic data breaches, while at the same time encouraging companies to invest in cybersecurity safeguards. The solution is a modified version of the National Flood Insurance Program ("NFIP"). Congress enacted the NFIP in 1968 to address concerns about building homes on rivers and other floodplains. NFIP flood insurance is available to property owners in communities that have adopted minimum floodplain management regulations that help to minimize the likelihood that a building would be

---

47 *See* Paul F. Roberts, *Cyber Insurance: Only Fools Rush in*, ITWORLD (Oct. 27, 2014), http://www.itworld.com/article/2839393/cyber-insurance-only-fools-rush-in.html [http://perma.cc/LUH2-PN6P] ("Insurers have responded by writing exclusions into [commercial general liability] and other nuts and bolts commercial policies, like so-called E&O (errors and omissions) and D&O (directors and officers) liability policies. Those exclusions carve out cyber claims and push them into new, specialized insurance products.").

48 *Don't Waste Your Money on Cyber Breach Insurance*, INFORMATIONWEEK (Sept. 26, 2012), http://www.darkreading.com/dont-waste-your-money-on-cyber-breach-insurance/d/d-id/1138422 [http://perma.cc/7GMW-BFDR] ("If line-of-business and legal leaders unilaterally decide to get a breach policy without input from IT, they may miss exclusions in the policy that require a higher level of controls than what the organization currently has in place.").

49 DEP'T OF HOMELAND SEC., INSURANCE INDUSTRY WORKING SESSION READOUT REPORT (2014).

50 *New Survey Finds a Vast Majority of U.S. Small Business Owners Believe Cybersecurity Is a Concern and Lawmakers Should Do More To Combat Cyber-Attacks*, ENDURANCE INT'L GRP. (May 4, 2015), http://www.prnewswire.com/news-releases/new-survey-finds-a-vast-majority-of-us-small-business-owners-believe-cybersecurity-is-a-concern-and-lawmakers-should-do-more-to-combat-cyber-attacks-300076543.html [http://perma.cc/39R5-94F6].

damaged or destroyed in a flood.[51] The Federal Emergency Management Agency administers the NFIP and promulgates regulations that set the minimum safeguards for local communities that wish to participate in the program. As of 2014, 5.35 million NFIP policies are in force.[52] In 2005, when Hurricane Katrina hit the southern states, the NFIP paid $17.8 billion in loss dollars.[53]

NFIP serves as a roadmap for the solution to the cybersecurity insurance problem. The government could create a cybersecurity insurance program, structured similarly to the NFIP. A government agency with experience in cybersecurity, such as DHS, would administer the insurance program and promulgate minimum cybersecurity safeguards that a company must implement to qualify for the insurance. If implemented properly, the program would help businesses mitigate risk, while encouraging companies to invest in cybersecurity infrastructure and services. Such a program would not only benefit businesses, but it would be a net win for the American public, as the cybersecurity safeguards would result in fewer cybersecurity incidents.

## CONCLUSION

Some of the proposals in this Article, such as the national data breach notification standard, have been discussed for many years but have not gained significant traction.[54] Other proposals, such as the safe harbor and insurance program, have not been discussed significantly, and may come out of left field for many policymakers. This is because our cybersecurity debate has focused too long on punitive measures rather than collaboration between the private and public sectors.

Our cybersecurity policy is built on decades-old infrastructure that does not account for the unique, public-private nature of cyberspace. Regulating companies into oblivion is not the most effective way to optimize investments in cybersecurity. Instead,

---

51 *See* FED. EMERGENCY MGMT. AGENCY, FEMA 496, JOINING THE NATIONAL FLOOD INSURANCE PROGRAM (2005), http://www.floods.org/ace-files/documentlibrary/State_Local%20Resources%20and%20Tools/3.6_FEMA_496_JoiningNFIP.pdf [http://perma.cc/AYP6-U4SM].

52 *Total Policies in Force by Calendar Year,* FEMA, https://www.fema.gov/total-policies-force-calendar-year [http://perma.cc/94SH-HN94] (last updated Nov. 19, 2015).

53 *Loss Dollars Paid by Calendar Year,* FEMA, https://www.fema.gov/loss-dollars-paid-calendar-year [http://perma.cc/XH76-BGJH] (last updated Nov. 19, 2015).

54 *See* Jeff Kosseff, *Analysis of White House Data Breach Notification Bill*, INSIDEPRIVACY (Jan. 15, 2015), http://www.insideprivacy.com/uncategorized/analysis-of-white-house-data-breach-notification-bill/ [http://perma.cc/7FKA-9YXC].

we need a legal framework that encourages companies to work with the government to invest in cybersecurity. Such a change will benefit not only the companies, but society as a whole, helping to secure individuals' personal information.