Chapter 1

An Introduction to the Law of Cyber Risk

Edward R. McNicholas & Vivek K. Mohan

*Sidley Austin LLP***

§ 1:1 In General

The law of cybersecurity in the United States has been evolving rapidly, shaped by the significant harms suffered as a result of cybersecurity incidents, by federal and state regulators attempting to protect consumers, by law enforcement's response to criminal activities, and by the slow advance of common law duties. This chapter introduces some of the key tensions that are driving the law of cybersecurity, and some of the most important practical considerations for those who seek to manage cyber risk more effectively.

---

* Vivek K. Mohan was affiliated with Sidley Austin LLP during the original writing of this chapter. He is now a lawyer in private practice in California.

At the most basic level, the law of cybersecurity is developing in response to the exponential growth in Internet—and Internet of Things—technologies. Technology is rapidly cementing its place as an essential pillar in everyday life, and technology-enabled critical infrastructure hums away behind the scenes. These technological advances have brought immeasurable societal gains; but from a risk perspective, the cyber threat exposure continues to grow as hackers take advantage of low barriers to entry and vulnerable targets, pressing their offensive advantage. Control over this growth is lacking and likely impossible, but the struggle to manage lawless cyber risk in a manner consistent with the rule of law continues to drive the law's measured—at times leaden—advance.

The conflicting forces of disruptive growth and legal order have left the private sector in the United States subject to a complex and often overlapping set of laws and regulations that affirmatively impose obligations and prescribe limitations with regard to cybersecurity practices. As the following chapters describe, the United States has tended to take a sectoral approach toward regulation and governance in cyberspace, prescribing particular requirements for healthcare, financial services, telecommunications, defense, energy, professionals, and others. Although the sectoral model does allow regulators to develop and leverage expertise and relationships with regulated entities, this can result in siloed approaches to managing cyber risk that vary dramatically by sector.

These variations in cybersecurity efforts at times lead to incongruous interactions with government agencies following a cyber incident. Companies are rightly worried that even while certain elements of the government view companies as the victims of data breaches perpetrated by criminal actors, other agencies can simultaneously view these same companies as potential perpetrators, neglecting their obligations to protect networks and the personal and other data they hold.

In the absence of an overarching federal regulator, the private sector has taken concerted steps to address cyber risks, most notably through industry standards and by enhancing contractual protections in vendor relationships. While contracts now impose increasingly complex affirmative cybersecurity requirements on vendors, the reality is that most companies act as both vendors and clients. These vendor-client relationships naturally span sectors, as data flow across our information economy; as such, sector-specific regulation must confront the complex web of cross-sector interdependence that characterizes modern economic realities.

The remainder of this chapter outlines the key issues facing the law of cybersecurity today. Following this general introduction, chapter 2 provides a more robust survey of the general legal framework for cybersecurity; chapters 3 and 4 describe the efforts of the executive

branch; and chapter 5 provides detailed information about various regulated sectors of the economy.

While this treatise is primarily focused on the legal regime within the United States, we must mention the General Data Protection Regulation (GDPR), a set of rules passed by the European Union and enacted into law by its Member States. Effective May 2018, GDPR preparedness has been an area of intense focus in recent years for companies that collect personal information in Europe, as the law carries with it the potential for fines of up to 4% of global annual turnover. The substantive security requirements of GDPR are flexible, but the law's as-yet untested requirements to provide notification to regulators and data subjects within seventy-two hours of "becoming aware" will present an area of significant interest and development in 2018.[1]

§ 1:2 General Duties: Reasonable Conduct and Notice of Cybersecurity Incidents

Despite the lack of a comprehensive cybersecurity governance regime, the U.S. legal framework does impose certain general duties that are applicable to cybersecurity issues. The common law has always imposed baseline duties to avoid negligence and conduct one's business in a reasonable manner so as not to harm others. The baseline of reasonable conduct, however, has rapidly proved inadequate to provide useful guidance for managers of cyber risk in our advanced information economy.

The Federal Trade Commission (FTC), together with state agencies empowered by specific statutory mandates, has set the de facto bar for affirmative data security requirements for entities that are not subject to more specific regulatory requirements (such as those that exist in the financial services, healthcare, energy, or other regulated industries). The FTC's assertion of authority over information security, however, is limited by its statutory powers under section 5 of the FTC Act to prohibit "unfair or deceptive acts or practices" that injure consumers—an expansion of authority that has received close judicial review and approval.[2]

The FTC has used its section 5 authority to bring enforcement actions predicated on claims of "deception" as well as claims alleging "unfairness." Enforcement actions resting on deception can be

---

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *See* Articles 32–34.
2. 15 U.S.C. § 45 *et seq*.

brought against companies that make false promises about information practices. In a result perhaps contrary to the FTC's intention to promote transparent information security, most companies now refrain from making any such affirmative statements or heavily caveat such commitments.

Not surprisingly, the FTC increasingly relies upon its authority to pursue claims alleging that a company has committed an unfair act and practice—that is, an act or practice that imposes unavoidable harms on consumers, without countervailing benefits. Although notions of "fairness" may not seem directly related to a field where criminals and other malicious actors attack and compromise networks—after all, the government does not go after banks that have been robbed—the FTC has systematically built a series of enforcement decisions to support actions against breached companies grounded in unfairness. These cases have provided helpful guidance about particular practices that are so egregious as to be deemed unfair. These cases have not gone uncontested. Companies have gone to court to challenge the FTC's ability to dictate a de facto federal code of unfair information security practices; but the ruling of the Third Circuit in August 2015 in *Wyndham Worldwide* affirmed the FTC's ability to use its section 5 unfairness authority in this context.[3]

The FTC's consumer protection mission, however, does little to address the most feared cyber risks to U.S. companies: attacks that target intellectual property and trade secrets, not consumer personal information. The government and media have devoted considerable attention to such industrial espionage. In 2014, federal prosecutors in Pennsylvania even went so far as to announce charges against alleged Chinese military hackers for theft of trade secrets. While the charges are largely symbolic in that the Chinese defendants are highly unlikely to ever face a judge in the United States, the importance of the issue is indisputable; these indictments arguably led at least in part to a U.S.-China Cyber Agreement in the fall of 2015 in which both countries agreed to provide information and assistance regarding malicious cyber activities and refrain from conducting such activities themselves.[4] The issues of international cybersecurity risks, however, remain unresolved, as Russian threats to our electoral systems and the potential for cyber conflicts erupting from international trouble spots such as North Korea continue to plague the Internet.

---

3. FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).
4. *See* THE WHITE HOUSE, FACT SHEET: President Xi Jinping's Visit to the United States (Sept. 25, 2015), https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states. Commentators have questioned the efficacy of the agreement in practice.

Despite the widespread significance of such attacks, companies that have been the target or victim of intellectual property theft alone have sometimes come to the conclusion that it would not be desirable to report such a compromise. In an attempt to remedy the lack of public transparency over the scope and impact of such cyber theft of intellectual property, the Securities and Exchange Commission (SEC) has issued guidance explaining obligations for public companies to report material cyber risks and adverse cyber incidents. Although the compromise of particularly valuable intellectual property may trigger such reporting obligations, these reports do not provide complete transparency; indeed, such references are frequently at such a level of generality that it is difficult or impossible to gauge their impact. In February 2018, the SEC supplemented its cybersecurity guidance, counseling companies to ensure appropriate controls and processes were in place to respond to cybersecurity incidents, including assessing materiality for purposes of public disclosure. The SEC's guidance also makes clear that recent publicly reported incidents of trading by insiders in possession of potentially material nonpublic information regarding data security incidents or product security vulnerabilities will be closely examined by the Commission.[5] Likewise, regulators such as the New York Department of Financial Services (NYDFS) have required companies to disclose any cybersecurity events that may materially impact normal operations, regardless of whether personal data is involved.

The SEC is also more frequently conducting investigations into public issuers following cyber incidents and has pursued at least two distinct lines of inquiry: first, whether material risks were appropriately disclosed and reported; and second, whether internal controls for financial reporting relating to information security adequately reflect the potential risk posed to the accuracy of financial results. As a result of recent investigations, it is possible—and perhaps likely—that industry standard guidance for cybersecurity risk may arise from SEC mandates formed through the course of its investigations and attendant enforcement actions. The SEC's interest in establishing industry standards is increasingly evident in the context of entities that are directly subject to its regulatory remit—the SEC's Office of Compliance Inspections and Examinations' Risk Alerts evince increasingly prescriptive and detailed requirements.[6]

---

5. SEC, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release Nos. 33-10459; 34-82746 (Feb. 21, 2018).
6. *See, e.g.*, SEC, National Exam Program Risk Alert, Observations from Cybersecurity Examination, Vol. VI, Issue 5 (Aug., 7, 2017), https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf; SEC, National Exam Program Risk Alert, Cybersecurity: Ransomware Alert, Vol. VI,

Congress and executive agencies are also attempting to encourage the sharing of information about cybersecurity incidents, particularly since the passage of the Cybersecurity Act of 2015.[7] This statute provides authorization for monitoring, use of so-called "defensive measures," and sharing of "cyber threat indicators" (with private and governmental entities) pursuant to the Act, and further provides limited liability protections for such monitoring and information sharing. While the full impact of this law and associated activities undertaken to mitigate cyber risks is yet to be seen, it is an important step toward enabling the private sector and federal government to more easily conduct necessary activities with reduced legal risk.

The Cybersecurity Act has also helped to create a bit more centralization in the federal government's approach to cybersecurity by establishing a portal at the Department of Homeland Security (DHS) and its National Cybersecurity & Communications Integration Center (NCCIC) to facilitate private-public cyberthreat information sharing and clarifies NCCIC's statutory role in evaluating and responding to cybersecurity risks and threat indicators.

The challenge that the field of cybersecurity law still faces, though, is supporting the development of a robust, publicly transparent knowledge base regarding malicious actors in cyberspace and their capabilities. This will give the markets an ability to assess and evaluate these risks, while at the same time maintaining enough secrecy so that the fight can be effective.

While the nature of cyber risks remains largely similar across industry sectors, regulators in particular sectors have fashioned custom solutions in light of their history and tradition of regulation and enforcement. Although one could criticize this siloed approach, maintaining the uniqueness of different sectors has allowed for a robust institutional experimentalism, which will only benefit the law if it is able to propagate the most resilient approaches across different sectors.

Even as formal regulation remains sparse, particular requirements are evolving in response to cyber risks. As an example, no general requirement exists under state or federal law to appoint a chief information security officer (CISO) or similarly titled or situated official, although a security officer is required under HIPAA, and entities subject to NYDFS oversight are subject to a similar requirement. Financial regulators have used their authority to survey entities and to require a reason if a position of CISO has not been created. Likewise,

---

Issue 4 (May 17, 2017), https://www.sec.gov/files/risk-alert-cybersecurity-ransomware-alert.pdf; SEC OCIE Cybersecurity Examination Initiative, Vol. IV, Issue 8 (Sept. 15, 2015), https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.

7. Codified at 6 U.S.C. § 1501 *et seq*.

the FTC and state attorneys general may look to the lack of a CISO in determining whether a company that is otherwise under investigation has made adequate investments in information security. And courts may of course push the law of cybersecurity along the common law path in considering whether the absence of a CISO could be negligence. In practice, each of these possible developments may well interact with each other as the need for a CISO becomes more clear, but this issue is but one of the dozens of important open questions in defining the general federal duties for information security.

§ 1:3 Executive Actions and the Approach of Law Enforcement

The most worrisome of cyber threats are without doubt those undertaken by state actors in order to wage war through cyberspace. One may well be able to assume the U.S. military and intelligence agencies have been long focused on countering such threats and protecting those aspects of the United States that are vulnerable to such attacks. Such threats, however, defy ready categorization as they imperil both military and commercial assets, and threaten harm not only to combatants but also to civilian infrastructure, private enterprise, and the general population. Despite the trans-partisan nature of such cyber risks, congressional action has been glacial, with the notable exception of the Cybersecurity Act of 2015, although even that Act has been criticized by some for failing to provide adequate protection for participating companies and by others for failing to provide sufficient privacy safeguards. Federal legislation to establish a national and uniform data breach notification requirement or clear federal standards for reasonable information security languish in congressional committees with little chance of passage.

In the face of congressional inaction, both Presidents Trump and Obama have used executive powers repeatedly to initiate important federal movement on cybersecurity. The first of several key actions was Executive Order 13636 issued in February 2013; titled "Improving Critical Infrastructure Cybersecurity,"[8] it directs DHS to address cybersecurity and minimize risk in the sixteen critical infrastructure sectors identified by Presidential Policy Directive 21.[9] The Order further directed the National Institute of Standards and Technology (NIST) to develop a cybersecurity framework, the final draft of the first iteration of which was released in February 2014.[10]

---

8. Exec. Order No. 13,636, Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11,739 (Feb. 12, 2013); *see also* Appendix C.
9. *See* http://www.dhs.gov/critical-infrastructure-sectors.
10. *See* Appendix A.

The NIST Cybersecurity Framework provides voluntary guidance to help organizations manage cybersecurity risks, and "provides a means of expressing cybersecurity requirements to business partners and customers and helps identify gaps in an organization's cybersecurity practices." While the framework is voluntary and aimed at critical infrastructure, an expectation is increasing that the framework (which is laudably accessible and adaptable) will become a de facto requirement for many companies. Alongside the release of the Framework, AT&T CEO Randall Stephenson was quoted as saying that "[a]ny large company that isn't imposing cybersecurity standards" on service providers "has a vulnerability that they're missing."[11] The full impact of Executive Order 13636 and the NIST Framework remains to be seen; however, it appears likely that as the private sector moves towards full implementation, these executive actions will fundamentally transform the expected baseline policies and procedures for private entities in cybersecurity risk mitigation.

President Obama also issued Executive Order 13691, titled "Promoting Private Sector Cybersecurity Information Sharing," which directed the Secretary of Homeland Security to encourage the development and adoption of "Information Sharing and Analysis Organizations" (ISAOs) to further facilitate the sharing of information about cyber threats.[12]

Again in February 2016, President Obama launched a Cybersecurity National Action Plan to create a federal Chief Information Security Officer to guide the implementation of increased security across the federal government, and issued an executive order establishing the Commission on Enhancing National Cybersecurity within the Department of Commerce. The Commission comprises technology, national security, and business leaders, and is charged with developing "detailed recommendations to strengthen cybersecurity in both the public and private sectors" by December 1, 2016.[13]

President Trump's administration appears to be heading toward a cybersecurity strategy that is consistent with President Obama's approach, issuing Executive Order 13800 just months into his term.[14]

---

11. *See* Holly J. Gregory, *White House Releases NIST Cybersecurity Framework*, HARV. L. SCH. F. ON CORP. GOVERNANCE & FIN. REG. (Feb. 23, 2014, 9:00 AM), http://blogs.law.harvard.edu/corpgov/2014/02/23/white-house-releases-nist-cybersecurity-framework/.
12. Exec. Order No. 13,691, Promoting Private Sector Cybersecurity Information Sharing, 80 Fed. Reg. 9349 (Feb. 13, 2015); *see also* Appendices F and G.
13. Exec. Order No. 13,718, Commission on Enhancing National Cybersecurity, 81 Fed. Reg. 7441 (Feb. 9, 2016); *see also* Appendix M.
14. Exec. Order No. 13,800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, 82 Fed. Reg. 22,391 (May 11, 2017).

That Order builds on the NIST Framework by requiring its use by agencies and making clear the President's commitment to hold agency heads accountable for the cybersecurity within their agencies. The Order further requires detailed reporting from agencies and mandates processes to reduce botnets, enhance the response to electrical grid incidents, assess warfighting and defense industrial base capabilities, enhance international engagement on cybersecurity cooperation, and ensure adequate workforce development.

Federal law enforcement agencies, in particular, have taken up the President's continuing call to arms to respond to cybersecurity incidents and have been aggressively investigating and prosecuting cyber criminals. The U.S. Secret Service (more commonly known for its responsibilities relating to presidential protection) is charged by statute to lead investigations that relate to certain financial and cyber crimes, and has developed robust technical and investigative capabilities.[15] The Secret Service is an agency under DHS, which is itself charged by statute and executive order with improving the overall cybersecurity posture and resiliency of the United States.

The Federal Bureau of Investigation (FBI) has also positioned itself as a key federal law enforcement agency to focus on cyber issues. The FBI, which now ranks cybersecurity near terrorism at the top of its list of priorities, has devoted considerable investigative resources to the field, and brings a global reach.

Taken together, these agencies are focused on assisting the victims of cyber incidents and bringing the perpetrators of cyber crimes to justice with the cooperation of prosecutors (and, where necessary and appropriate, international cooperation that can include the use of Mutual Legal Assistance Treaties (MLATs) as well as extradition proceedings). The Secret Service and FBI have developed sophisticated capabilities in detecting and investigating criminal cyber incidents that provide significant practical assistance to private entities both before and after a cybersecurity incident.

Such cooperation with prosecutors, however, may pose some risks to companies. Full compliance with respect to government monitoring may undercut expectations of privacy that companies wish to afford to their customers, employees, or others with whom they contract. In the post-Snowden era, it is not clear that consumers will embrace companies who are seen to share information too closely with the government. Beyond the potential consumer implications, clear legal immunity for such involvement has yet to be enacted, and law enforcement may well insist upon a broader notification of potential victims than a private company would otherwise undertake.

---

15. *See, e.g.*, 18 U.S.C. §§ 1029, 1030.

Further, law enforcement may in certain circumstances propose a response that does not align with a company's erstwhile privacy commitments and public relations strategy, causing additional tensions and creating a potential impact on goodwill.

Even as law enforcement works to dispel such fears, the executive branch's overall approach to cybersecurity remains distinctly ambiguous. For every step that law enforcement takes to enhance its capabilities to assist entities in the private sector that have been the victim of cyber crime, the FTC is likely to take steps toward playing the role of a de facto privacy and cybersecurity regulator and civil enforcement agency. Representative of the dichotomy that exists in the approach taken by criminal law enforcement agencies and the FTC is the response to recent high-profile cybersecurity incidents. While the Secret Service and FBI have stepped in to assist the victim companies, the FTC has launched investigations into the cybersecurity posture of the companies themselves. Even the SEC has taken an interest in investigating victims of cyber crime, although their true appetite for pursuing enforcement actions is unclear and would be predicated on an even more strained reading of statutory authorities than that of the FTC. Ultimately, it remains to be seen whether these agencies will pursue enforcement actions seeking to impose enduring cyber security mandates on impacted companies, or monetary damages.

§ 1:4 General Duties: State Approaches

The same struggle between government as protector against cyber risk and government as punisher of cyber negligence is mirrored at the state level. The role of state law enforcement in prosecuting state cyber crime laws and helping companies respond to attacks by cyber criminals has not evolved in as robust of a fashion as their interest in pursuing corporate victims of data breaches. "Mini-FTC Acts" statutes similar to those empowering the FTC also authorize state attorneys general to regulate cybersecurity, and they have taken an approach similar to the FTC.

State legislatures have also hardly waited for federal legislation; instead they are leading the way by enacting new cybersecurity laws in the absence of robust federal guidance. States have enacted statutory requirements that require companies to implement and abide by certain information security precautions that the states consider to be reasonable. These laws impose a range of obligations on companies, and can have the impact of setting a de facto national standard for companies doing business across the United States. They are often no more clear than underlying common-law duties, but these state statutory hooks have become more definitive, particularly with the release of the 2009 information security regulations promulgated in

Massachusetts.[16] These regulations were the first to require a comprehensive written information security plan (WISP); a WISP must include specific technical, administrative, and physical controls regarding protection of personal information, thereby establishing something close to a baseline for information security. Massachusetts further requires that companies have written contractual protections in place prior to transferring personal data to third parties, a requirement that has also been implemented in states such as California. These measures, however, have tended to protect only personal information, not corporate data.

Even before such information security measures, California in 2002 enacted the first of what came to be known as "data breach notification laws"—laws that codify a duty to warn of the loss of control of personal data that could result in potential harm.[17] Now, fifty state and four territorial similar laws exist, imposing an obligation on private sector entities to provide notifications to impacted individuals and state regulators when personal information has been compromised. While the state laws vary in key respects—including notification thresholds and requirements—they usually require notification when there has been a compromise of some combination of an individual's name and a second, sensitive data element such as date of birth or credit card account number.

Despite a continuing parade of major cybersecurity incidents and apparent bipartisan support for a benchmark federal data breach notification standard, the broader climate of congressional inaction has stymied such legislative efforts. While legislation has not advanced out of Congress, the practical necessity of clear national data breach singular notification standards and other measures to establish uniform cybersecurity standards remains apparent with federal data breach notification required only in certain sectors, such as healthcare entities covered by the Breach Notification Rule of the Health Insurance Portability and Accountability Act (HIPAA).[18]

§ 1:5 The Role of Litigation

The law of cybersecurity, however, is not determined by statutes and regulations alone. While the number of cybersecurity incidents and awareness of the dangers continue to grow, litigation is only now

---

16. 201 MASS. CODE REGS. §§ 17.00–.05.
17. CAL. CIV. CODE § 1798.81(c).
18. HIPAA's Breach Notification Rule, which is covered in more depth in section 5:3, imposes significant reporting requirements as well as provides for civil and criminal penalties for the compromise of protected health information (PHI).

becoming a source of significant liability for corporations that have suffered a compromise of intellectual property or personal information. Even when companies prevail in litigation, response costs for major consumer-facing breaches of personal information have run in the hundreds of millions of dollars, and include the not-insubstantial cost of forensic investigations, of response to government investigations and inquiries, of providing notice and credit monitoring to impacted individuals, and of settlements with impacted third parties, such as banks and insurance companies.

Class action litigation against corporations that have suffered such an incident has largely failed in the early stages.[19] Many district courts in the United States have been generally unwilling (or, some would argue, unable) to find a cognizable harm, a necessary predicate for "standing," a legal concept required to sustain a lawsuit in the United States. But there is a notable trend emerging with some appellate courts recognizing standing for data breach classes,[20] with the Supreme Court's ruling in *Spokeo* re-emphasizing the longstanding rule that "the injury-in-fact requirement requires a plaintiff to allege an injury that is both 'concrete *and* particularized,'" but also providing support for finding standing in some circumstances.[21] These considerations are covered in more depth in section 2:7. It bears noting that while corporations have to date had significant success pursuing this lack-of-standing legal theory and litigation strategy, this doctrine may evolve if courts recognize dignitary harms associated with the unauthorized disclosure of personal information.[22] Likewise, technical violations of statutory duties that do not result in financial damages could be recognized as grounds for nominal damages that, when multiplied across a large class, could pose a significant deterrent. Doctrines could also evolve to recognize some special property protections for the "electronic curtilage" of our online personal spaces in the same way that the common law protected the physical curtilage—that is, the area around a home—so that a breach of personal information would violate some property right in electronic data. Or companies could sort out the matter with complex contractual provisions that apportion cyber liability. Whatever its route, whether through statute, contract, or tort or property law, litigation

---

19. *See, e.g., In re* Target Corp. Customer MDL, No. 14-2522 (D. Minn. Sept. 15, 2015).
20. *See, e.g.*, Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015) (finding standing); Lewert v. P.F. Chang's China Bistro, Inc., No. 14 C 4787, 14 C 4923 (7th Cir. Apr. 14, 2016) (same).
21. Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016) (quoting Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 180–81 (2000)).
22. *See* section 2:7.2.

will significantly influence how the law of cybersecurity apportions the harms of cybersecurity incidents, even as statutory and regulatory developments continue to evolve and coalesce.

§ 1:6 Legal Considerations and the Use of Emerging Cybersecurity Technologies

Technological change will reliably outpace the general advancement of the law, and the law of cybersecurity is developing at a time of particularly rapid and material technological innovation, spurred on by the tremendous rewards that the markets are offering for real security. As the law will be shaped by the technologies available, the law also plays an important role in encouraging—or discouraging—the development and use of certain cybersecurity technologies.

Federal law does not provide a generally applicable affirmative requirement to deploy or implement a specific minimum set of security technologies (however, sector-specific requirements, such as HIPAA's strong nudge toward the use of encryption to protect personal health information (PHI), do exist). Despite this lack of federal statutory authority, an evolving body of case law, shaped by enforcement actions brought by the FTC and state attorneys general, as well as a vigorous plaintiff's bar, has had the effect of setting a baseline for what information security measures a company should expect to put into place. For example, Massachusetts data security law, as noted above, imposes a requirement that companies holding certain personal information deploy technologies with certain specific capabilities, and document their plans to protect such information.

The law relating to the use of cybersecurity technologies will also turn on how the technology operates. The potential legal risks associated with the operation of such technologies were not addressed by the Cybersecurity Act of 2015 (which provides authorization to use "defensive measures," but declines to provide liability protection for such use) and remain potentially significant sources of exposure. Offensive "hack-back" and "active defense" technologies will continue to face significant scrutiny under the law, regardless of how effective or harmful they may be as a practical, technical matter. Likewise, generally, many private sector entities can regularly use traffic and packet signature monitoring to analyze data that enters or passes across their networks to detect, and where appropriate and permissible, contain or block malicious traffic. Typically, the legal justification for monitoring such information generated internally stems from representations made in corporate policies that eliminate employees' expectations of privacy over information transmitted on corporate networks. The treatment of information entering corporate networks is also governed by externally facing privacy or security policies, as

well as terms of use, which may include provisions relating to how such data is analyzed, shared, and used.

Evolving corporate cybersecurity technologies must also comply with the Electronic Communications Privacy Act of 1986 (ECPA), a broad law that has spawned several treatises' worth of discussion regarding the privacy of electronic information. ECPA is directly applicable when private operators of electronic communications services, such as companies running email servers, decide to deploy cybersecurity technologies that analyze the content payloads of communications.[23] Although the law generally allows private entities to use privacy-sensitive security technologies such as intrusion detection and prevention systems to protect their networks, it is not without limits. Moreover, complicated ECPA and other legal issues can arise when private entities act on information from the government; indeed, at some level of information sharing and action, the private entity could become a government agent, conducting a search governed by the Fourth Amendment.[24] Companies cannot afford to ignore ECPA or Fourth Amendment considerations, as civil and criminal penalties may apply and be substantial in size (as automated technologies could potentially conduct millions, or billions, of prohibited searches on a packet-by-packet basis). Congress's failure to update ECPA in light of the rapidly evolving nature of cybersecurity threats and defenses continues to create material uncertainty that can derail the development and deployment of new cybersecurity technologies.

---

23. *See, e.g.*, Memorandum to Fred F. Fielding, Counsel to the President, from Steven G. Bradbury, Principal Deputy Assistant Attorney Gen., Office of Legal Counsel, Re: Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion Detection System (EINSTEIN 2.0) to Protect Unclassified Computer Networks in the Executive Branch (Jan. 9, 2009); *see also* Memorandum Opinion to an Associate Deputy Attorney Gen., from David J. Barron, Acting Assistant Attorney Gen., Office of Legal Counsel, Re: Legality of Intrusion-Detection System to Protect Unclassified Computer Networks in the Executive Branch (Aug. 14, 2009).

24. The tests articulated by the Supreme Court in Jackson v. Metro. Edison Co., 419 U.S. 345 (1974), and Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602 (1989), continue to provide the foundational legal standards to determine whether a private "search" has taken place for purposes of the Fourth Amendment. *Jackson* requires consideration of whether there is a "close nexus" between the state and the challenged action, and *Skinner* further mandates consideration of "the degree of the government's participation in the private party's activities in light of all the circumstances." *Jackson*, 419 U.S. at 351; *Skinner*, 489 U.S. at 614–15. These have been interpreted by courts in the context of searches conducted by private parties that provide services covered by ECPA. *See, e.g.*, United States v. Richardson, 607 F.3d 357 (4th Cir. 2010).

Despite these limitations, DHS, the U.S. Secret Service, and others have actively encouraged the use of new technologies informed by the shared experiences of the government and private companies about the threat environment. The creation of partnerships between the federal government and industry is an important way in which the government is encouraging the use and development of cybersecurity protection systems, although legal restrictions on such information sharing will require continuing attention in order to ensure appropriate separation between public and private networks.

§ 1:7 Privacy, Cybersecurity, and Surveillance

Few would doubt that the protection of privacy must of course shape the law's approach to cybersecurity. Cybersecurity can, and should, be accomplished with due regard for personal privacy; a robust privacy program enhances security, and security against unauthorized intrusions is an essential element of protecting the privacy of data.

Many of the statutes discussed in this treatise can be classified as both "privacy laws" and "cybersecurity laws." Privacy laws are not discussed separately from security laws because they are often two faces of the same coin, and while this treatise focuses on the security side, it must in part explain the privacy side as well.

The public discourse about cybersecurity has unfortunately tended to conflate the distinct legal issues of cybersecurity and surveillance into a single conversation. Cybersecurity and surveillance are more accurately distinguished, particularly with regard to the difference between surveillance and the legal rights and obligations of the private sector in relation to data security. Data breach laws, threat-sharing environments, and incident response protocols, to list but a few examples, do not necessarily involve surveillance.

Some approaches to cybersecurity can involve significant surveillance; however, it is certainly hoped that the advancement of surveillance will be checked and balanced by the evolution of the law of privacy. The noble desire to protect cyberspace must not advance at the expense of personal freedom, and must successfully be coordinated with the constitutional limitations of the Fourth Amendment and our evolving sense of personal space, even as our personal space extends further into cyberspace. In particular, the law must appreciate the potentially differential impact of cybersecurity technologies on civil liberties with respect to the vulnerable elements of our society. It could scarcely be considered an advance if the law of cybersecurity allowed the government to examine all Internet searches simply to stop credit card theft, or if the law allowed such unfettered surveillance that most workers would live their waking hours in a totalitarian "electronic panopticon" simply to stop viruses. Such important

topics should inform important checks on the development of certain cybersecurity technologies, but such concerns are not the primary focus of this practical effort to inform legal management about cybersecurity risk.

§ 1:8 Open Questions

Unpredictability often eclipses foresight. At present, the law of cybersecurity involves many more open than resolved questions, and the trend of increasing uncertainty is likely to intensify in the coming years, as technology develops, risk evolves, and the amount of data continues to grow—particularly as we add more and more sensors to the world in building the Internet of Things. The U.S. political system has heretofore failed to respond adequately on what should be a non-partisan issue, but it may be possible that needed legislation will come to pass that will enable better collaboration between the private and public sector, enhance robust security baselines, and better embrace the complex interdependencies of our information economy.

The current points of tension are clear. Pressure on the issues of intellectual property theft is likely to continue to rise to the top of the international diplomacy agenda for the United States as its competitive position risks erosion vis-à-vis aggressive emerging economies. Surveillance issues are also likely to continue to be a sticking point between the United States and its European counterparts. The growth of cloud data centers and the need to protect them are similarly likely to continue to be a point of tension. The U.S. government's cybersecurity partnerships with corporations, in combination with conflicting approaches to the law of data protection in the United States, Europe, and Asia, may also inhibit the development of the sort of globally interoperable cybersecurity solutions that are necessary to protect global information systems. Investment in the protection of computer systems is also likely to be a continued regulatory focus, as regulators seek to understand the impact of effective information security requirements and reporting, perhaps through the use of the NIST cybersecurity framework. New cyber risks may entirely alter this path. The potential for serious physical consequences from cyber attacks cannot be doubted after the Stuxnet code destroyed Iranian nuclear centrifuges. Similarly, one cannot dismiss the threats of widespread cyber attacks with the potential both to impact critical system infrastructure and to cause significant physical harm and human casualties—what former U.S. Secretary of Defense Leon Panetta referred to as a "cyber Pearl Harbor." The threat of a weaponized cyberspace will indeed continue to loom as rogue states and terrorist actors attempt to pervert the most successful human invention for global engagement into a weapon of mass destruction.

While the broader outlook for cybersecurity is uncertain, it is clear that intervening advancements in factual knowledge and technological developments will continue to propel this field to the front of the national consciousness—and consequently, to the attention of legislators, regulators, the class action bar, and courts—for the foreseeable future.