**Chapman Law Review**

Volume 19 | Issue 2 Article 4

2016

# Cybersecurity: Executive Orders, Legislation, Cyberattacks, and Hot Topics

Kelly Russo
*American Bar Association*

Harvey Rishikof
*American Bar Association*

Follow this and additional works at: http://digitalcommons.chapman.edu/chapman-law-review

 Part of the Law Commons

Recommended Citation

Kelly Russo & Harvey Rishikof, *Cybersecurity: Executive Orders, Legislation, Cyberattacks, and Hot Topics*, 19 Chap. L. Rev. 421 (2016).
Available at: http://digitalcommons.chapman.edu/chapman-law-review/vol19/iss2/4

This Article is brought to you for free and open access by the Fowler School of Law at Chapman University Digital Commons. It has been accepted for inclusion in Chapman Law Review by an authorized editor of Chapman University Digital Commons. For more information, please contact laughtin@chapman.edu.

# Cybersecurity: Executive Orders, Legislation, Cyberattacks, and Hot Topics

*Kelly Russo*[*] *and Harvey Rishikof*[**]

## INTRODUCTION

For all actors—government, business, and individual—cybersecurity has evolved significantly over the last fifteen years due to the rise of the Internet and the need for the free flow of information.[1] Due to statutory divisions, we refer to cybersecurity as cybercrime, cyberespionage, and cyberwar. However, the evolution of security regulations can be examined through four periods, beginning with pre-9/11 and progressing through the cyber era of today.

As the Internet expanded during the 1990s, it forced industry to focus on connecting systems and expanding the flow of information, while the law, the Telecommunications Act of 1996, left the network largely unregulated.[2] Some legislative attempts were made, but most failed. During this period, threats usually came from low-budget, mischievous hackers, rather than criminals or nations. From the perspective of the U.S. government, terrorism and related security issues were almost exclusively issues dealt with overseas; it was an age of innocence.

After 9/11, a series of security-related laws and regulations were passed as attempts were made to lock down cyberspace. The Department of Homeland Security, Department of Justice, and Department of Defense began a nascent regulatory framework to strengthen security. The focus was "centered primarily on the

---

* Kelly Russo is an attorney with the Cybersecurity Legal Task Force at the American Bar Association in Washington D.C. She graduated from Wake Forest University, (B.A. 2012 cum) (J.D. 2015). While in law school, Ms. Russo served as the Marshal on the Moot Court Board, and was an Elite 8 Finalist at the Regional Jessup International Law Competition.

** Harvey Rishikof, American Bar Association Chair, Advisory Standing Committee on Law and National Security, is former legal counsel to the Deputy Director of the FBI, former Administrative Assistant to the Chief Justice of the United States, and former Dean of Roger Williams University School of Law. The opinions and views expressed in this Article are his own and do not reflect the opinions or views of any entity of the U.S. government.

1 CROWELL & MORING, REGULATORY FORECAST 2016, at 8–9 (2016), https://www.crowell.com/files/Regulatory-Forecast-2016-Crowell-Moring.pdf [http://perma.cc/S2GX-G2NK].

2 *Id.*

16 'critical infrastructure' sectors vital to the U.S., such as energy, chemicals, communications, financial services, and the defense industrial base."[3] Almost exclusively, regulators focused on the security of physical spaces; however, some regulations were created to defend information systems from hackers disrupting critical operations. The legislation passed during this era included the USA Patriot Act of 2001, which permitted the use of more extensive investigative tools, harsher penalties, and intra-governmental information sharing. In 2001, the Department of Homeland Security ("DHS") was created. In 2002, the Federal Information Security Management Act of 2002 established a cybersecurity framework for federal data systems. Then, in 2004, the Intelligence Reform and Terrorism Prevention Act of 2004, among other things, created the Director of National Intelligence.[4]

In response to these developments, the ABA Cybersecurity Legal Task Force was created in 2012 under Former ABA President Laurel Bellows. It was established to examine ways to help lawyers protect their practices and their clients' confidential information and intellectual property during cyber events, as well as position the ABA to contribute to national dialogue about cyber issues.[5] It is tasked with addressing the tough questions about the appropriate role and responsibility of lawyers in cyber-related incidents and to examine ways that lawyers and businesses can protect their practices and their clients' confidential information and intellectual property.[6] It is composed of representatives of ABA entities having an interest in the cyber domain as well as leaders in the private and public sectors responsible for cybersecurity.[7]

The Mission Statement for the Task Force was clear:

> [to] identify and compile resources within the ABA that pertain to cybersecurity, and will focus and coordinate that ABA's legal and policy analyses and assessments of proposals relating to cybersecurity. . . . (1) Facilitate collaboration and information exchange among constituent ABA entities and with relevant public and private organizations; (2) Serve as a clearinghouse among ABA entities regarding cybersecurity activities, policy proposals, advocacy, publications and resources; (3) Study and analyze executive and legislative branch cybersecurity proposals; (4) Identify cyber-related issues for appropriate action by the ABA, including filling gaps in

---

3 *Id.*

4 *Id.*

5 *See generally* JILL D. RHODES & VINCENT I. POLLEY, THE ABA CYBERSECURITY HANDBOOK (2013).

6 *Id.*

7 *Id.*

> policy, encouraging ABA entities to develop new policy as appropriate, and sharing best practices with members and their firms; and (5) Advise and assist ABA Governmental Affairs Office on cybersecurity advocacy and responses to government actions.[8]

During the next period, regulations were focused more on protecting data, as data breaches affected a broad range of organizations, from corporations to the U.S. Office of Personnel Management. Regulators questioned the government's role in ensuring cybersecurity and protecting private information. Information sharing between the public and private sector increasingly became the zone to ensure cybersecurity. Data theft in the last few years was perpetrated by criminals, spies, nations, terrorists, and "hactivists," and "creating common, overarching standards for security, reporting, and response has proven to be a

---

8 *About the Task Force*, A.B.A., http://www.americanbar.org/groups/leadership/office_of_the_president/cybersecurity/aboutcyber.html [http://perma.cc/87ZK-G7UC]. The Task Force was quite productive establishing principles, writing reports, and passing resolutions. Their Resolution of November of 2012 was comprised of the following five principles:

> (1) Public-private frameworks are essential to successfully protect United States assets, infrastructure, and economic interests from cybersecurity attacks; (2) Robust information sharing and collaboration between government agencies and private industry are necessary to manage global cyber risks; (3) Legal and policy environments must be modernized to stay ahead of or, at a minimum, keep pace with technological advancements; (4) Privacy and civil liberties must remain a priority when developing cybersecurity law and policy; (5) Training, education, and workforce development of government and corporate senior leadership, technical operators, and lawyers require adequate investment and resourcing in cybersecurity to be successful.

A.B.A. CYBERSECURITY LEGAL TASK FORCE, REPORT TO THE BOARD OF GOVERNORS 1 (2012), http://www.americanbar.org/content/dam/aba/marketing/Cybersecurity/aba_cybersecurity_res_and_report.authcheckdam.pdf [http://perma.cc/Y9V8-NQ9A]; *see also* A.B.A. CYBERSECURITY LEGAL TASK FORCE, REPORT AND RESOLUTION 118 1 (2013), http://www.americanbar.org/content/dam/aba/administrative/law_national_security/resolution_118.authcheckdam.pdf [http://perma.cc/947M-FK7R] (containing a Resolution that condemns "intrusions into computer systems and networks utilized by lawyers and law firms" and urges federal, state, and other governmental bodies to examine and amend existing laws to fight such intrusions); A.B.A. CYBERSECURITY LEGAL TASK FORCE, REPORT TO HOUSE OF DELEGATES ON RESOLUTION 109 2 (2014), http://www.americanbar.org/content/dam/aba/events/law_national_security/2014annualmeeting/ABA%20-%20Cyber%20Resolution%20109%20Final.authcheckdam.pdf [http://perma.cc/DA4X-SKGX] ("This Resolution addresses cybersecurity issues that are critical to the national and economic security of the United States (U.S.). It encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected."); A.B.A. CYBERSECURITY LEGAL TASK FORCE, REPORT TO THE HOUSE OF DELEGATES ON RESOLUTION 116 1 (2015), http://www.americanbar.org/content/dam/aba/images/law_national_security/Aug-2015-Cyber-Res.pdf [http://perma.cc/EXE7-TYXF] ("It urges the federal, state, local, tribal, and territorial legislatures and government agencies to provide the funding necessary to develop, implement, and maintain appropriate cybersecurity programs for the courts and to train court personnel on methods to counter threats and protect judicial information systems from cyber intrusions or data breaches.").

challenge . . . ."[9] This period was marked by tensions between the need for openness and creativity and the role of security and safety. The Department of Defense implemented the Defense Federal Acquisition Regulation Supplement Safeguard Rule in 2013 requiring defense contractors to implement IT security controls. In 2014, the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity was released, outlining the elements of a comprehensive cybersecurity program.[10] Then, in 2015, President Obama issued an executive order that allowed the administration to impose sanctions on those that threaten U.S. infrastructure,[11] and finally the Cybersecurity Information Sharing Act of 2015 was passed to improve information sharing between the government and private sector.[12]

As we begin the year 2016, "data and information sharing will likely be woven more deeply into daily life."[13] Regulators will need to address the issue of privacy and the right to control information. Businesses and the government will be called on to implement security measures for a growing cyberworld. One of the most difficult challenges will be regulating global business as we attempt to navigate international efforts to ensure worldwide security. In this period, security measures will focus less on reacting to events and more on preventative measures. It will be all about finding the balance between privacy and security as we merge big data with small data.[14] So how has the executive branch been navigating this balance thus far?

## I. EXECUTIVE ORDERS REGARDING CYBERSECURITY

### A. President Clinton

President Clinton signed the first executive order, Executive Order 13035, pertaining to the cyber sector on February 11, 1997.[15] This order established the Advisory Committee on High-Performance Computing and Communications, Information Technology, and the Next Generation Internet.[16] The committee consisted of twenty-five or fewer non-federal members appointed

---

9 CROWELL & MORING, *supra* note 1, at 9.

10 CROWELL & MORING, *supra* note 1.

11 *Id.*

12 Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015).

13 CROWELL & MORING, *supra* note 1.

14 Small data refers to personal information belonging to an individual. Big data refers to information associated with corporations or government entities.

15 Exec. Order No. 13035, 62 Fed. Reg. 7131 (Feb. 14, 1997), http://www.gpo.gov/fdsys/pkg/FR-1997-02-14/pdf/97-3992.pdf [http://perma.cc/D5WB-R4GJ].

16 *Id.*

by the President. The purpose of this committee was to provide the National Science and Technology Council with guidance and information regarding "high-performance computing and communications, Information Technology, and the Next Generation Internet."[17] This included an independent assessment of progress in designing and implementing the Next Generation Internet Initiative and the High-Performance Computing and Communications Program. The order stated that the Department of Defense would provide the financial and administrative support to the committee.[18]

Building on this framework, President Clinton also signed Executive Order 13133 on August 5, 1999, establishing the Working Group on Unlawful Conduct on the Internet, to report on the extent to which existing federal law offered an adequate basis for "effective investigation and prosecution of unlawful conduct that involves the use of the Internet."[19] The Order also sought information and recommendations regarding new technological tools that might be necessary for effective investigation and prosecution of unlawful Internet use, as well as the availability of new or existing tools to educate the population and prevent unlawful conduct involving the Internet.[20] The first attempts to organize the federal space met much resistance.

B. President Bush

President George W. Bush began with signing Executive Order 13231 on October 16, 2001, entitled "Critical Infrastructure Protection in the Information Age," with the purpose of encouraging "continuous efforts to secure information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems."[21] The order established the "President's Critical Infrastructure Protection Board," to recommend policies and programs to "provide security and continuity to national security information systems."[22] In doing so, the Board would consult and coordinate with the private sector, as well as state and local governments, to ensure that systems were established and maintained with the capacity to share threat warning, analysis,

---

17 *Id.*

18 *Id.*

19 Exec. Order No. 13133, 64 Fed. Reg. 43895 (Aug. 5, 1999), http://www.gpo.gov/fdsys/pkg/FR-1999-08-11/pdf/99-20924.pdf [http://perma.cc/W458-2QGZ].

20 *Id.*

21 Exec. Order No. 13231, 3 C.F.R. § 13231 (2002), http://fas.org/irp/offdocs/eo/eo-13231.htm [http://perma.cc/QAA4-ZF6T].

22 *Id.*

and recovery information. Again, there was much resistance from both inside and outside of government.[23]

C. President Obama

Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," was signed by President Obama on October 7, 2011, in the wake of the WikiLeaks exposés.[24] It encouraged reforms to improve the security of cyber networks that house sensitive information.[25] It established multiple interagency groups to collaborate on security initiatives and put the burden of ensuring classified network security on "all agencies that operate or access classified computer networks."[26] The Order also recognized the importance of information sharing and established the Senior Information Sharing and Safeguarding Steering Committee as well as the Classified Information Sharing and Safeguarding Office, to ensure safe sharing of information.[27] Executive Order 13587 assigned the Secretary of Defense and the Director of the National Security Agency to serve as the Executive Agent for Safeguarding Classified Information on Computer Networks.[28] It also created a government-wide Insider Threat Task Force to detect, deter, and mitigate cyberthreats.[29]

President Obama's Executive Order 13636, entitled "Improving Critical Infrastructure Cybersecurity," was signed on February 12, 2013, to "improve cybersecurity information sharing and collaboratively develop and implement risk-based standards."[30] The Order mandated the development of a "technology-neutral voluntary cybersecurity framework," in addition to promoting the adoption of cybersecurity practices and timely cyberthreat sharing.[31] It also directed the incorporation of privacy and civil liberties protections and the exploration of using existing regulations and policies to promote cybersecurity.[32] The Executive Order instructed the National Institute for Standards and Technology to collaborate with the private sector to establish best

---

23 *Id.*

24 *See* Exec. Order No. 13587, 3 C.F.R. § 13587 (2011), https://www.gpo.gov/fdsys/pkg/CFR-2012-title3-vol1/pdf/CFR-2012-title3-vol1-eo13587.pdf [http://perma.cc/6XPH-AYRJ].

25 *Id.*

26 *Id.*

27 *Id.*

28 *Id.*

29 *Id.*

30 Exec. Order No. 13636, 78 Fed. Reg. 11739 (Feb. 19, 2013), https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf [http://perma.cc/55CS-QW22].

31 *Id.*

32 *Id.*

practices and create a cybersecurity framework.[33] It also directed DHS to promote the implementation of the framework.[34]

President Obama, seeing the need, signed Executive Order 13691, entitled "Promoting Private Sector Cybersecurity Information Sharing," on February 13, 2015.[35] The Order presented a framework for enhanced information sharing with the purpose of encouraging private sector companies to work together and work with the federal government to identify cyberthreats.[36] The Order first "encourage[d] the voluntary formation of [organizations engaged in the sharing of information related to cybersecurity], to establish mechanisms to continually improve the capabilities and functions of these organizations, and to better allow these organization to partner with the Federal Government on a voluntary basis."[37] The Order instructed DHS to create a non-profit organization to establish voluntary standards for the information sharing and analysis organizations ("ISAOs") and authorized the Department to enter into information sharing agreements with ISAOs.[38] Privacy concerns were also addressed, as the Order instructed private sector ISAOs to abide by voluntary standards of privacy protections when information sharing.[39]

To grant the presidency more tools, President Obama signed Executive Order 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," on April 1, 2015.[40] This Executive Order regarded the recent cyberthreats as a national security emergency.[41] It authorized the Secretary of the Treasury, in collaboration with the Attorney General and Secretary of State, to impose sanctions on those engaged in cyber-enabled activities that "are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States" and have the purpose or effect of "harming . . . entities in a critical infrastructure sector"

---

33 *Id.*

34 *Id.*

35 Exec. Order No. 13691, 80 Fed. Reg. 9349 (Feb. 20, 2015), https://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf [http://perma.cc/TH2R-P6C4].

36 *Id.*

37 *Id.*

38 *Id.*

39 *Fact Sheet: Executive Order Promoting Private Sector Cybersecurity Information Sharing*, WHITE HOUSE (Feb. 12, 2015), https://www.whitehouse.gov/the-press-office/2015/02/12/fact-sheet-executive-order-promoting-private-sector-cybersecurity-inform [http://perma.cc/7DTG-4UJW].

40 Exec. Order No. 13694, 80 Fed. Reg. 18077 (Apr. 1, 2015), https://www.gpo.gov/fdsys/pkg/FR-2015-04-02/pdf/2015-07788.pdf [http://perma.cc/738U-S6TZ].

41 *Id.*

with "significant disruption to the availability of a computer or network," or "causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain."[42] The Executive Order also authorized the imposition of sanctions on those who knowingly receive or use trade secrets stolen by cyber-enabled activities (or provide material support) for financial gain when the theft threatens national security, foreign policy, or the financial stability of the country.[43]

As one can see, the executive orders increasingly engaged the federal bureaucracy and searched for ways to engage the private sector.

## II. CURRENT PENDING LEGISLATION

But one key to the puzzle remained: the need for legislation. Executive power alone would not be sufficient. The following bills on cybersecurity pending in the 114th Congress were attempts to solve the issues. While several bills were proposed, those discussed below are the most comprehensive and the only then-pending cyber legislation with significant bipartisan support.

On Friday, December 18, 2015, lawmakers merged the first three information sharing cyber bills mentioned below into an omnibus spending plan, which was signed by President Obama. The Cybersecurity Act of 2015 includes an iteration of the Cybersecurity Information Sharing Act ("CISA"), which includes components from both the Protecting Cyber Networks Act ("PCNA") and the National Cybersecurity Protection Advancement Act ("NCPAA").[44]

### A. Protecting Cyber Networks Act, H.R. 1560

This bill was sponsored by Republican Devin Nunes from California and was introduced on March 24, 2015. It was passed 307-116 in the House on April 22, 2015 and was received in the Senate on April 27, 2015.[45] The bill's purpose was to encourage businesses to share information regarding cybersecurity risks by providing them protection from liability.[46] Under the PCNA, the

---

42 *Id.*

43 *Id.*

44 Andrew Blake, *CISA Cyber Bill Squeezed into Omnibus Spending Plan*, WASH. TIMES (Dec. 16, 2015), http://www.washingtontimes.com/news/2015/dec/16/cisa-cyber-bill-squeezed-omnibus-spending-plan/ [http://perma.cc/A7FG-YQNK].

45 *H.R. 1560 - Protecting Cyber Networks Act,* CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/house-bill/1560/actions [http://perma.cc/SE8Q-DEK6].

46 *See id.*; Chris Preimesberger, *House Finally Passes Cyber-Networks Protection Act*, EWEEK (Apr. 22, 2015), http://www.eweek.com/security/house-finally-passes-cyber-networks-protection-act.html [http://perma.cc/PC4E-WED9].

cyber information would be shared with civilian agencies, rather than DHS (as is the case with the NCPAA discussed below). The bill would require that businesses, prior to sharing information regarding a cybersecurity threat, "take reasonable efforts to remove personal information identifying individuals related to the threat."[47] Additionally, the bill required the Privacy and Civil Liberties Oversight Board to address Congress and the President every two years with regard to the sufficiency of procedures to address privacy concerns.[48]

The PCNA lists authorized uses of the information shared including: "cybersecurity, preventing death or serious bodily harm, preventing the exploitation of minors, preventing and prosecuting violent felonies, fraud and identity theft, and espionage and the theft of trade secrets."[49] Conversely, the NCPAA, discussed below, allows shared information to be used only for cybersecurity purposes.[50]

While the NCPAA empowers DHS's National Cybersecurity and Communications Integration Center ("NCCIC") to serve as the main hub for public and private-sector information sharing, the PCNA does not designate a hub, but rather gives the President the power to establish a government hub or hubs with which the private sector can share information while explicitly prohibiting information sharing with the Department of Defense.[51]

Critics of the bill argue that it does not include strong enough liability protections for non-federal entities.[52] The PCNA states, "[n]o cause of action shall lie or be maintained in any court against any non-federal entity, and such action shall be promptly dismissed, for the sharing or receipt of a cyber threat indicator or defensive measure if such sharing or receipt is conducted in good faith."[53] This "good faith" standard is regarded as a lower standard (than "willful misconduct," for example) of proof and opens businesses up to a greater risk of litigation.[54]

Critics also attacked the bill's privacy protections, arguing that the bill would give companies the ability to share data with

---

47 Protecting Cyber Networks Act, H.R. 1560, 114th Cong. (2015).

48 *Id.* § 107.

49 David Inserra & Riley Walters, *House Cyber Information Sharing Bills: Right Approach but Require Fixes,* HERITAGE FOUND. (Apr. 10, 2015), http://www.heritage.org/research/reports/2015/04/house-cyber-information-sharing-bills-right-approach-but-require-fixes [http://perma.cc/85GH-HNEH].

50 *Id.*

51 David Eppstein, Cyber Bills Compared (Dec. 17, 2015) (unpublished working paper) (on file with author); *see also* H.R. 1560 § 103.

52 Inserra & Walters, *supra* note 49.

53 H.R. 1560 § 106(b).

54 *Id.*

intelligence agencies, allowing them to ignore laws like the Privacy Act of 1974 and the Electronic Communication Privacy Act of 1986.[55] However, proponents of the bill argued that there are strong privacy protections because the bill limits the categories of sharable information to only the listed cyberthreat indicators and requires two scrubs of personal information from the shared information: one by the private sector business and one by the government.[56]

B. National Cybersecurity Protection Advancement Act, H.R. 1731

This bill was sponsored by Republican Michael McCaul from Texas and was introduced on April 13, 2015.[57] The House Homeland Security Committee passed it nearly unanimously.[58] It was designed to provide liability protections to those businesses who voluntarily share data regarding cyberthreat indicators and defensive measures with one another and with DHS's NCCIC. The bill would grant liability for private businesses to perform network awareness sweeps of their own data systems and would permit the NCCIC to share information concerning cybersecurity threats with private businesses, in addition to other non-federal bodies.[59] Without these liability protections, businesses sharing information pursuant to this bill could expose themselves to class actions or regulatory enforcement actions.[60]

The NCPAA included several provisions limiting the privacy threat of information sharing, such as a prohibition on federal use of shared data to engage in surveillance for the purpose of tracking persons' individually identifiable information.[61] The bill also required DHS to create and review annually privacy policies and processes that direct the "receipt, retention, use, and disclosure" of information shared with NCCIC in accordance with the bill.[62] Another privacy protection in the NCPAA would require private businesses to remove all personal information

---

55 Andy Greenberg, *Privacy Critics Go 0-2 with Congress' Cybersecurity Bills,* WIRED (Mar. 26, 2015, 4:16 PM), http://www.wired.com/2015/03/privacy-critics-go-0-2-congress-cybersecurity-bills/ [http://perma.cc/DJ35-NY9A].

56 *H.R. 1560,* Legislative Digests, HOUSE REPUBLICANS (Apr. 22, 2015), http://www.gop.gov/bill/h-r-1560-the-protecting-cyber-networks-act/ [http://perma.cc/643H-35KM].

57 National Cybersecurity Protection Advancement Act*,* H.R. 1731, 114th Cong. (2015).

58 *Id.*

59 H.R. 1731 - National Cybersecurity Protection Advancement Act of 2015, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/house-bill/1731 [http://perma.cc/82MJ-RBRU].

60 Daniel Farris & Lindsay Kessler, *House Passes the National Cybersecurity Protection Advancement Act,* JDSUPRA BUS. ADVISOR (Apr. 25, 2015), http://www.jdsupra.com/legalnews/house-passes-the-national-cybersecurity-69958/.

61 H.R. 1731 § 3.

62 *Id.*

that is not related to the cyberthreat before sharing the information with the NCCIC or private bodies.[63] The NCCIC would then be required to conduct a second screening in order to ensure that there is no personal information unrelated to the cyberthreat before sharing the information with other government or private groups.[64]

This bill was viewed by technology, telecommunications, and infrastructure businesses as "a critical compliment to the PCNA."[65] It also was viewed as favorably expansive, allowing the NCCIC to include tribal governments, information sharing and analysis groups, and the private sector, in addition to expanding the NCCIC's functions to include global cybersecurity measures with international partners.[66] Its liability protection had been given positive reviews as well. The NCPAA states that a "non-federal entity . . . shall not be liable in any civil or criminal action brought under this subsection unless such non-federal entity engaged in willful misconduct or gross negligence with respect to sharing or conduct and such gross negligence or willful misconduct proximately caused the injury."[67] The standard of "willful misconduct or gross negligence" is a strong standard and protects businesses, and thus incentivizes the sharing of cyber information.[68]

While the liability provisions of the NCPAA were strong and widely praised, critics suggested that the bill could be improved by broadening the authorized uses of the shared information, as the NCPAA restricts the government use to just "cybersecurity purposes."[69] Critics suggested allowing the government's use of properly shared information as long as *one* significant use is for cybersecurity purposes, pointing to the authorized uses in the PCNA as a model.[70]

### C. Cybersecurity Information Sharing Act of 2015, S. 754

Republican Senator Richard Burr from North Carolina sponsored this bill. It is the Senate counterpart to the PCNA and was introduced on March 17, 2015, and passed 74-21 in the Senate on October 27, 2015.[71] CISA would provide liability

---

63 *Id.*
64 *Id.*
65 Farris & Kessler, *supra* note 60.
66 *Id.*
67 H.R. 1731.
68 Inserra & Walters, *supra* note 50.
69 *Id.*
70 *Id.*
71 Cybersecurity Information Sharing Act, S. 754, 114th Cong. (2015); *S.754 – Cybersecurity Information Sharing Act of 2015*, CONGRESS.GOV, https://www.congress.gov/

protections to companies of the private sector that share information about security breaches or vulnerabilities with particular government entities. Like the PCNA, CISA would authorize voluntary sharing of information between the government and private companies through a portal established by DHS.[72] Also similar to PCNA, CISA would protect information shared against disclosure under the Freedom of Information Act and similar state laws.[73] Both the PCNA and the CISA would also provide protection from private suits and would codify Federal Trade Commission and Department of Justice policy that cybersecurity information sharing does not encroach upon antitrust laws.[74]

Critics of the CISA, including major technology companies, like Apple, Twitter, and Reddit, argued that the bill has major privacy and Internet security concerns. First, they argue that CISA would allow surveillance of Internet users and does not include adequate privacy protections of personal information. Second, it does not include any recourse for consumers if their personal information were to be improperly shared with the federal government. Third, the liability protections in the bill would discourage businesses from improving their own security measures.[75]

All three of these information sharing bills contain a federal preemption clause, meaning they would supersede any state statutes or provisions of state law that regulate an activity expressly authorized under one of these bills. This could limit states' ability to combat cyberthreats, which are sometimes arguably better equipped to collaborate with the private sector to prevent cyberthreats.

### D. Cybersecurity Act of 2015

The Cybersecurity Act of 2015, which is Division N of the most recent omnibus spending bill, was passed by Congress and signed by President Obama on December 18, 2015.[76] The Act

---

bill/114th-congress/senate-bill/754 [http://perma.cc/L7HQ-VKN7].

72 Eppstein, *supra* note 51; *see also Summaries for the Cybersecurity Information Sharing Act of 2015,* GOVTRACK.US, https://www.govtrack.us/congress/bills/114/s754/summary [http://perma.cc/G3LD-7R2L].

73 Greg Nojeim & Jadzia Butler, *Guide to Cybersecurity Information Sharing Act Amendments*, CTR. FOR DEMOCRACY & TECH. (Oct. 23, 2015), https://cdt.org/blog/guide-to-cybersecurity-information-sharing-act-amendments/ [http://perma.cc/HP74-PRZC].

74 David Navetta & Utsav Mathur, *Sharing Cyber Threat Information: A Legal Perspective,* ISSA 29 (Jan. 2015), http://www.dataprotectionreport.com/wp-content/uploads/sites/489/2015/01/Sharing-Cyber-Threat-Information_ISSAS0115.pdf [http://perma.cc/U5PQ-5BMK]; *see also* Eppstein, *supra* note 51.

75 *See Summaries for the Cybersecurity Information Sharing Act of 2015, supra* note 72.

76 Cybersecurity Act of 2015, Pub. L. No. 114-113, 129 Stat. 2936.

establishes a voluntary cybersecurity information sharing procedure that encourages public and private entities to share cyberthreat information with one another.[77] Despite the outpour of divided reactions from various supporters and critics, the Act is meant to serve as a piece of compromise legislation, as provisions of both the PCNA and NCPAA influence it. However, it does not include language from the two pieces of pending legislation discussed below.[78]

Under the Act, the federal government is instructed to establish procedures for sharing classified and unclassified cyberthreat indicators and defensive measures with the private sector.[79] The Act's key information sharing provision states, "[a] non-Federal entity may, for a cybersecurity purpose and consistent with the protection of classified information, share with, or receive from, any other non-Federal entity or the Federal Government a cyber threat indicator or defensive measure."[80] The private sector may only share data that falls within the Act's definitions of "cyber threat indicator" or "defensive measure." The Act defines a cyberthreat indicator as "information that is necessary to describe or identify [a cyberthreat]."[81] A defensive measure is "an action, device, procedure, signature, technique, or other measure" that "detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability."[82] Additionally, before sharing any information, the private sector entity must remove information that it "knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual."[83]

The Act tasks DHS with the job of creating a mechanism by which the government can receive cyberthreat indicators and defensive measures from the private sector. In real time, DHS must then share the information with the appropriate federal entities, including the Office of the Director of National Intelligence and the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and Treasury.[84] It also allows the President to designate other federal entities (in addition to DHS)

---

77 *Id.*

78 *See generally* David J. Bender, *Congress Passes the Cybersecurity Act of 2015*, NAT'L L. REV. (Dec. 20, 2015), http://www.natlawreview.com/article/congress-passes-cybersecurity-act-2015 [http://perma.cc/ATZ5-TRUN].

79 Cybersecurity Act of 2015 § 103, 129 Stat. at 2940–41.

80 *Id.* § 104(c)(1), 129 Stat. at 2942.

81 *Id.* § 102(6), 129 Stat. at 2938.

82 *Id.* § 102(7), 129 Stat. at 2938.

83 *Id.* § 104(d)(2)(A), 129 Stat. at 2943.

84 *Id.* § 102(3), 129 Stat. at 2937; *see also id.* § 105(a)(3)(A), 129 Stat. at 2945.

to develop an information sharing process, excluding the Department of Defense.[85]

The Act provides several privacy protections for those entities that choose to participate in information sharing. First, it limits the government's use of the shared information to use only for a "cybersecurity purpose," meaning "the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability."[86] Second, the Act prevents federal agencies from disseminating the shared information, which the Act exempts from disclosure under the Freedom of Information Act.[87] Third, the private sector is immune from liability for sharing or receiving cyberthreat indicators or defensive measures.[88]

There have been varying degrees of support and opposition in response to the passing of the Cybersecurity Act. Supporters of information sharing believe that the increase in information sharing will improve the overall cybersecurity of our country. They argue that the Act has ample privacy protections and is voluntary. Critics call the Act a "surveillance bill" that encroaches upon privacy rights, and Section 104 of the Act, the key provision relating to Internet surveillance, has become a popular topic of discussion.[89] Section 104 allows network operators to take three steps only "for cybersecurity purposes." Network operators can (1) monitor, (2) operate defensive measures, and (3) share information. Additionally, with written consent, a network operator can allow an outside entity to monitor its network and operate defensive measures.[90] Those that oppose Section 104 argue that it gives a network operator too much power with little to no guidance or limitations. For example, the Act allows monitoring for "cybersecurity purposes," which is arguably broad and unclear.[91]

---

85 *Id.* § 105(c)(2)(B), 129 Stat. at 2948.

86 *Id.* § 102(4), 129 Stat. at 2937.

87 *Id.* § 105(d)(3), 129 Stat. at 2950.

88 *Id.* § 106(a)–(b), 129 Stat. at 2951–52.

89 *See* Tom Risen, *Obama Signs Cybersecurity Law in Spending Package*, U.S. NEWS & WORLD REP. (Dec. 18, 2015, 5:49 PM), http://www.usnews.com/news/articles/2015-12-18/obama-signs-cybersecurity-law-in-spending-package [http://perma.cc/97TL-5CQM].

90 *Id.* § 104, 129 Stat. at 2940–43.

91 Orin Kerr, *How Does the Cybersecurity Act of 2015 Change the Internet Surveillance Laws?,* WASH. POST (Dec. 24, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/12/24/how-does-the-cybersecurity-act-of-2015-change-the-internet-surveillance-laws/ [http://perma.cc/5LYK-BWQD].

## E. Bills Not Incorporated into the Act of 2015

### 1. Data Security and Breach Notification Act of 2015

Not incorporated into the Cybersecurity Information Sharing Act of 2015 were two pieces of pending legislation dealing with state power and resources. On December 9, 2015, the House Financial Services Committee approved the Data Security Act of 2015 by a 46-9 vote. This act would supplant 47 state laws with a single national statute, requiring minimum-security protections at businesses in the private sector and establishing a national requirement for data breach notification. The private sector is generally in favor of a single law because it will provide a uniform standard to comply with, as opposed to various state laws. The legislation "identifies security controls organizations should adopt, including those involving access controls and restrictions, use of encryption of sensitive information and monitoring systems. The bill also directs businesses to require their third-party service providers to implement appropriate safeguards for sensitive information."[92]

The Data Security Act would allow businesses in different sectors to adopt security procedures that would work best with their specific needs. Regulatory enforcement would occur among several different agencies, including the Federal Trade Commission, the Comptroller of the Currency, the Federal Reserve System, and the Securities and Exchange Commission, among others. Business entities covered by the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act would be exempt from the Data Security Act.[93]

Critics of the legislation, including Democratic Representative Denny Heck from Washington, believe it takes the power to regulate security among insurers away from states' insurance commissioners, whom Heck contends work smoothly together. The legislation would also usurp laws in twelve states that call for businesses in their jurisdiction to adopt particular IT security procedures.[94] Massachusetts Assistant Attorney General Sara Cable testified before Congress earlier this year and contended that preempting state laws "represents a significant retraction of existing protections for consumers at a time when such protections are imperative. Minimum data security standards are

---

92 Eric Chabrow, *House Panel OK's National Breach Notification Bill,* GOV INFO SECURITY (Dec. 9, 2015), http://www.govinfosecurity.com/house-panel-oks-national-breach-notification-bill-a-8734 [http://perma.cc/QN57-KDUJ].

93 *Id.*

94 *Id.*

important and necessary, but the proposed standards leave consumers' data vulnerable."[95] This led Democrat Maxine Waters of California to present an amendment that would allow states to provide more stringent security requirements. However, the panel struck down the amendment on a voice vote, as Massachusetts was the only state that had stronger data security requirements than those presented in the Data Security Act.[96]

Critics also believe that this one-size-fits-all approach to cybersecurity will not be effective. Jennifer Safavian, an executive vice president at the Retail Industry Leaders Association, stated in a letter sent to the Committee's leaders that "[h]aphazardly slapping rules that were written 15 years ago for the financial industry on retailers, restaurants and thousands of small businesses is not the kind of data security legislation that will safeguard our economy."[97]

Privacy advocates, as well as consumer protection organizations, argue that the legislation would weaken consumer protections by stifling new and/or developing state laws that extend data security and breach notification protections to online account login systems. They argue that the bill would also abolish all opportunities of redress for consumers.[98] In a December 7, 2015 letter to the Committee's leaders, seventeen privacy and protection groups wrote: "If this bill were to pass, state attorneys general would be limited to seeking civil penalties and injunctive relief, even in cases where consumers suffer extensive harm as a result of a breach of highly sensitive information."[99]

2. State and Local Cyber Protection Act of 2015, H.R. 3869

On December 10, 2015, the House unanimously passed a bill that would provide state and local government with federal funds to battle cybercrime.[100] The bill's sponsor is Republican Representative Will Hurd from Texas. He is a former CIA officer who focused on cybersecurity and now chairs the House Oversight Subcommittee on Information Technology. Hurd stated, "[l]ocal governments often do not have access to the technical capabilities and training required to address highly

---

95 *Id.*

96 *Id.*

97 *Id.* (quoting Jennifer Safavian).

98 *Id.*

99 *Id.* (quoting letter from privacy and consumer protection groups).

100 *H.R.3869 – State and Local Cyber Protection Act of 2015*, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/house-bill/3869/actions?q=%7B%22search%22%3A%5B%22%5C%22hr3869%5C%22%22%5D%7D&resultIndex=1 [http://perma.cc/H8LG-EYUH].

exploitable cybersecurity vulnerabilities."[101] The bill amends the Homeland Security Act of 2002 to require the NCCIC, DHS's cyber group, to assist state and local governments with technical and strategic training to enhance their cyber defense.[102] The NCCIC is tasked with aiding state and local governments with identifying vulnerabilities in their systems, providing guidelines and information related to information security, conducting trainings on cybersecurity, and providing technical assistance with regard to implementing security systems.[103] The bill is now awaiting further action in the Senate.[104]

## III. CYBERATTACK HOT TOPICS LEFT OPEN

Although the Cybersecurity Act of 2015 is a sound first step, there are a number of issues that still need to be resolved. With the evolution of technology, ensuring sound cyber protections and preventing attacks has become increasingly important and increasingly difficult. Even the federal government is having difficulties enlisting the tech industry to help fight terrorism. While the tech community is willing to help, it is reluctant to reveal private information and data to the government for fear of user distrust and the misuse of sensitive information. White House representatives traveled to Silicon Valley in early January 2016 in an effort to convince tech companies of the importance of working with the government to keep our country safe. Needless to say, there was push back. A chief security officer at the tech company Twistlock pleaded with the "Obama administration to consider alternative forms of intelligence gathering now that encryption technology has become so common."[105] There is a "Washington" v. "Silicon Valley" divide concerning how best to deal with cybersecurity.

Nevertheless, the tech community is willing to work with the government as long as proper protections are in place. After the meeting, Facebook noted that tech companies and the government were "united in [their] goal to keep terrorists and terror-promoting material off the Internet."[106] This strained

---

101 Katie Bo Williams, *House Unanimously Passes Bill Boosting Resources to Fight Cybercrime,* HILL (Dec. 10, 2015, 6:06 PM), http://thehill.com/policy/cybersecurity/ 262870-house-unanimously-passes-dhs-cyber-bill [http://perma.cc/8MMR-W244].

102 State and Local Cyber Protection Act of 2015, H.R. 3869, 114th Cong. § 2.

103 *Id.*

104 Williams, *supra* note 101.

105 W.J. Hennigan & Paresh Dave Tracey Lien, *White House Presses Silicon Valley to Aid in Terrorism Fight*, SEATTLE TIMES (Jan. 9, 2016, 3:49 PM), http://www.seattle times.com/nation-world/white-house-presses-silicon-valley-to-aid-in-terrorism-fight/ [http://perma.cc/L24N-U4C3].

106 *Id.*

safety/privacy conversation between White House representatives and Silicon Valley tech experts serves as an example of the many complications involved in cybersecurity. While terrorism is one worry associated with the ever-evolving cyberworld, the following issues of privacy, encryption, liability, and cyber insurance are at the forefront of concerns and debates.

### A. Privacy: Who Owns the Information?

While there are many benefits to increasing data, connectivity, and other cyberservices, the developments in the cyberworld pose difficult challenges to ensuring privacy of sensitive information. Julie Brill of the U.S. Federal Trade Commission ("FTC") is one of the leaders in analyzing privacy and data security issues. In her recent speech at the Washington Governor Jay Inslee's Cyber Security and Privacy Summit, Brill stressed, "[c]onsumers want to know – and should be able easily to find out – what information companies are collecting, where they're sending it, and how they're using it. This kind of information is important to consumers' decisions about whether to use digital products and services in the first place."[107] She also mentioned the work the FTC has done to protect the privacy interests of consumers. For example, the FTC has brought actions against companies for inappropriately collecting private information from mobile devices and for revealing confidential health and other sensitive information.[108] In addition to the work of the FTC, other federal regulators, as well as state governments have enhanced privacy protections for consumers, but there is much more work to be done.[109]

One of the most widely discussed privacy issues with regard to cybersecurity centers around cyber information sharing between private entities and the government. Privacy and civil liberties groups cite many issues surrounding companies' duty to remove personally identifiable information ("PII") before sharing with the government. Critics are also skeptical about what the government does with this information when it is received and whether or not it is safely stored.[110] This debate is at the heart of the intersection of small and big data.

---

107 Julie Brill, U.S. Fed. Trade Comm'r, Privacy and Data Security in the Age of Big Data and the Internet of Things 1, 7 (Jan. 5, 2016) (transcript can be found at https://www.ftc.gov/system/files/documents/public_statements/904973/160107wagovprivacysummit.pdf [http://perma.cc/5D9X-WAQH]).

108 *Id.* at 3.

109 *Id.* at 4.

110 *See* Tal Kopan, *Obama to Sign Cybersecurity Bill as Privacy Advocates Fume*, CNN (Dec. 18, 2015, 1:51 PM), http://www.cnn.com/2015/12/18/politics/cybersecurity-house-senate-omnibus/ [http://perma.cc/5VXU-DS6K].

Privacy and civil liberties groups claim privacy concerns as the reason for their opposition towards the new cybersecurity bill signed by President Obama on December 18, 2015. They argue that the definition of acceptable information to share is too broad and the burden placed on companies to erase PII is not strict enough.[111] Nonetheless, the final version of the cybersecurity bill "compels entities to remove information they 'know' is extraneous personal information."[112] This is a higher standard than previous versions of the bill that used "reasonably believe" instead.[113]

Furthermore, DHS is sponsoring the nonprofit group Mitre Corporation's development of the Structured Threat Information eXpression ("STIX"). This would provide a "common language and mechanism for quickly analyzing, sharing, and receiving cyber threat information."[114] The adoption of a common sharing scheme would improve privacy, as there would be clearer guidelines as to what vulnerable information is shared and what is not.

Privacy issues also arise in the context of data breach reporting after a cyberattack has occurred. While there is no federal data breach statute, almost all of the states have data breach notification laws. Most state breach notification statutes are similar, however some do vary in several ways including: what constitutes a breach, what data is considered PII, and when a notification should be filed.[115] Most states agree on the general definition of PII—the attachment of certain information connected to someone's first and last name. However, states have not uniformly agreed upon what constitutes PII. For example, some states do not consider medical information, health insurance information, and email addresses to be PII.[116]

As the Internet and data sharing defy borders, privacy concerns do not affect the U.S. in isolation. The European Union's new data privacy law and the newly passed U.S. Cybersecurity Act set the tone for a pending U.S.-EU data sharing agreement to replace the Safe Harbor, which expedited

---

111 Tal Kopan, *Obama to Sign Cybersecurity Bill as Privacy Advocates Fume,* CNN (Dec. 18, 2015, 1:51 PM), http://www.cnn.com/2015/12/18/politics/cybersecurity-house-senate-omnibus/index.html [http://perma.cc/6DJ8-2YTM].

112 *Id.*

113 *Id.*

114 David Inserra & Paul Rosenzweig, *Cybersecurity Information Sharing: One Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace,* BACKGROUNDER, Apr. 1, 2014, at 6, http://www.heritage.org/research/reports/2014/04/cybersecurity-information-sharing-one-step-toward-us-security-prosperity-and-freedom-in-cyberspace [http://perma.cc/EU29-SVTW].

115 JUDITH MILLER ET AL., A PLAYBOOK FOR CYBER EVENTS 39 (2d ed. 2014).

116 *Id.* at 39–40.

the transfer of data between businesses and international networks. The EU's new data privacy regulations have been deemed more burdensome for U.S. companies and aim to protect the consumer. This could affect U.S. companies operating in the EU if they are held to the new standards. In the coming months, we will see how the EU-U.S. negotiations play out and how that will affect international privacy concerns.[117]

B. Encryption: How Is Access to Be Granted to Information?

Encrypting data alters readable information into unreadable information except to authorized readers. This prevents anyone who steals data from reading it, rendering the stolen data worthless to cybercriminals. In addition to protecting data, companies encrypt data because it may exempt a company from particular regulatory requirements, such as some state data breach notification statutes. Some downsides to encryption include the time and effort it takes to encrypt all data, the cost, and the potential for slowed operating performance. While encryption/decryption occurs automatically for authorized readers, the process can require significant computing power and memory that can slow computer systems and affect productivity within the company. Therefore, it is most common for companies to encrypt some, but not all data.[118]

It is important to note that encryption does not fully protect a company, as encryption only protects data and not the security of networks and systems. Furthermore, companies must securely store and protect decryption keys/algorithms that could get in the hands of cybercriminals.[119]

Lawmakers have considered the argument in favor of strong encryption requirements as a means of protecting data from cyberattacks, as well as the argument against encryption by those who argue that it could hamper law enforcement efforts, as communication via encryption could allow terrorist and other criminals to avoid surveillance.[120] The problem with providing law enforcement "back door" access is that cybercriminals could easily misuse it, or sophisticated cybercriminals could communicate via unsanctioned encrypted data that does not

---

117 Stephen Dockery, *EU Data Law Shows Way Forward for Next Safe Harbor Agreement*, WALL ST. J. (Dec. 18, 2015, 3:25 PM), http://blogs.wsj.com/riskandcompliance/2015/12/18/eu-data-law-shows-way-forward-for-next-safe-harbor-agreement/.

118 JUDITH MILLER ET AL., *supra* note 115, at 12–13.

119 *Id.* at 14.

120 Joe Uchill, *Both Sides of Data Encryption Debate Face Off in Congress,* CHRISTIAN SCIENCE MONITOR (Apr. 30, 2015), http://www.csmonitor.com/World/Passcode/2015/0430/Both-sides-of-data-encryption-debate-face-off-in-Congress [http://perma.cc/YJ6P-M24J].

contain a back door, and thus, would prevent law enforcement from accessing the data.

In his article, "Be Careful What You Wish For: Device Hacking and the Law," cybersecurity expert Benjamin Wittes theoretically discusses the legal implications of allowing the government to bypass encryption systems, as opposed to requiring decryption. This would occur through the "exploitation of existing vulnerabilities to accomplish legally authorized wiretapping."[121] Wittes warns that allowing the government to bypass encryption systems would deprive the private sector of key legal protections. The scope of the information hacked would have no limit. It would also be unclear as to whether the carrier would be required to assist the government in installing the malware. He believes that in the context of a lawsuit, courts would ask whether the government's request for technical assistance is "unduly burdensome for companies," which has not been clearly defined. All in all, Wittes believes that lawful hacking would lead to the "government's commandeering companies into compromising their users' devices."[122]

This debate has its roots in the Communications Assistance to Law Enforcement Act of 1994, when telephone companies were required to assent to lawful wiretaps. As noted by the recent Harvard Berkman Center report, *Don't Panic: Making Progress on the "Going Dark" Debate*, the world of the Internet of Things has changed the playing field for encryption, and that is not that easy to achieve as world wide web standards and key elements of communication such as metadata and weak software provide many avenues for the state. As before, there is much debate over the ground truth concerning technical issues and the implications for the market and policy.[123]

Apple is now litigating the scope of the technical assistance language in the Wiretap Act, which requires carriers to assist government agents in lawful wiretaps. One potential public policy impact of requiring Apple to push government malware is that it could lead to a serious lack of trust in Apple and other service providers. Wittes believes that the case will likely turn on how difficult it would be for a company like Apple to

---

121 Benjamin Wittes, *Be Careful What You Wish for: Device Hacking and the Law*, LAWFARE (Jan. 6, 2016, 3:14 PM), https://www.lawfareblog.com/be-careful-what-you-wish-device-hacking-and-law [http://perma.cc/Y8MC-M9HT].

122 *Id.*

123 Matt Olsen et al., *Forward* to BERKMAN CENTER, DON'T PANIC: MAKING PROGRESS ON THE "GOING DARK" DEBATE (2016).

unobtrusively send malware to its users. He mentions that it may also turn on who writes the malware.[124]

Despite the lawsuits, media attention, and airtime the topic of encryption has received at both the Republican and Democratic presidential debates, at this point there is no strong legislative push to give law enforcement access to encrypted data.[125]

C. Liability: Who Will Pay for Information Violations?

One of the most prevalent topics with regard to liability is information-sharing relevant to liability protections. In order to encourage businesses to share cyberthreat information with the government and other private sector companies, there must be liability protections to shield companies from lawsuits surrounding the shared data. The U.S. Department of Justice and the Federal Trade Commission jointly issued a Policy Statement in April 2014 acknowledging that antitrust laws do not attach liability to cybersecurity information sharing "as long as the sharing does not encroach on competitively sensitive information related to price, cost or output."[126] The agencies reasoned that the type of information shared in cyber information sharing is typically "very technical in nature and very different from the sharing of competitively sensitive information."[127] The White House agreed and President Obama stressed the importance of information sharing in Executive Order 13636.[128] Currently, companies are shielded from liability when sharing "cyber threat indicators," arguably a narrow liability protection.

Liability concerns for breached companies also involve private suits. It varies from state to state whether private actions can be brought against breached companies. Some do not allow any private suits, while others allow suits to recover damages. Suits are brought by clients, customers, vendors, and other business associates of the breached company. Courts are split on whether the data must be misused before a plaintiff can sue.[129] The new legislation affords some indemnification if the information is shared with DHS, but it is unclear what potential liability awaits from other regulatory agencies such as the FTC or the SEC.[130]

---

124 Wittes, *supra* note 121.

125 Matthew Mcdonald, *Making Sense of the Encryption Debate*, PHYS.ORG (Dec. 22, 2015), http://phys.org/news/2015-12-encryption-debate.html [http://perma.cc/C6GB-L685].

126 Navetta & Mathur, *supra* note 74.

127 *Id.*

128 *Id.*

129 MILLER ET AL., *supra* note 115, at 40.

130 Cybersecurity Act of 2015 § 106(a)–(b), Pub. L. No. 114-113, 129 Stat. 2936, 2951–52.

D. Cyber Insurance: How Will Risk over Information Be Allocated?

There are many expenses that a company may incur from a cyberattack. The expenses may involve: notification of clients, government agencies, credit monitoring services, forensic costs involved in the investigation, and legal costs surrounding claims or suits, as well as business interruption or the payment of judgments or settlements. The average cost of a cyberattack was $7.2 million in March 2011 and has likely risen since then. The majority of cost comes from the time and resources expended surrounding notification requirements.[131]

While resilient security systems may prevent most cyberattacks, there are some cyber intrusions that cannot be prevented, such as a zero-day attack.[132] In order to protect one's company from incurring the exorbitant costs that follow unpreventable breaches, cyber insurance has become more and more common. There are several types of insurance with varying degrees of protection. It is important to understand all the exclusions and gaps in coverage. Oftentimes multiple plans are necessary in order to have adequate protection. Insurance services organization commercial property policies may cover losses as a result of a virus, but oftentimes the policy requires the data to have been destroyed or corrupted.[133] General liability insurance covers only physical injury, in addition to liability as a result of publication of private material.[134] Professional liability insurance is limited by the term "professional services" or by exclusions.[135] Policies like the surety and fidelity computer crime policy oftentimes do not cover losses resulting from theft of private information, indirect consequential loss, and potential income.[136]

Cyber liability insurance is often offered as a stand-alone insurance policy with combined third-party liability and first-party coverage. It is designed to cover insureds that transmit and store private consumer data.[137] It is extremely important to review the coverage one's company has in place before an attack occurs in order to ensure adequate coverage. At this time, cyber liability insurance coverage can include: data breach/privacy crisis management (i.e. investigation, data notification, legal costs etc.), media liability (i.e. defacement of

131 RHODES & POLLEY, *supra* note 5, at 192–93.

132 *See What is a Zero-Day Vulnerability*, PC TOOLS, http://www.pctools.com/security-news/zero-day-vulnerability/ [http://perma.cc/T73X-HAMX].

133 *See* RHODES & POLLEY, *supra* note 5, at 192–93.

134 *Id.* at 193.

135 *Id.*

136 *Id.* at 192–93.

137 *Id.* at 194.

website and intellectual property rights infringement), extortion liability (i.e. losses due to threat of extortion), and network security (i.e. damages due to denial of access, costs related to theft of third-party data).[138] One advantage from a system perspective is that as insurance coverage expands, more elements of the private sector will enhance coverage to meet policy requirements.

## CONCLUSION

Cybersecurity is hard because it requires the forging of the "geek-wonk" bridge. It involves the blending of technical and policy cultures. Moreover, to engage society in this arena, we have four large social hammers—legislation, insurance premiums, tax policy, and lawsuits. Increasingly we are seeing movement in each of these policy areas. In short, both carrots and sticks are being deployed against corporate America.

But our adversaries are not resting. The recently released report from the Defense Security Service provides a snapshot into the current state of the world's cybersecurity situation, detailing specific regions and industries at risk.[139] The report states that in the last year there has been an eight percent increase in reported foreign collection attempts to obtain sensitive or classified data in the U.S. cleared industrial base.[140] East Asia and the Pacific was the top collector region and the threat level from this region was labeled "critical."[141] The electronics sector topped the list as the most targeted sector, while the commercial sector remained the top collector affiliation.[142] Academic solicitation was reported as the top method of operation.[143] In order to prevent these threats and enhance national and global cybersecurity, the government and the private sector must balance security and privacy interests through a concise set of agreed-upon standards and approaches necessary to build worldwide cybersecurity. Waiting is no longer an option.

---

138 Sarb Sembhi, *An Introduction to Cyber Liability Insurance Cover,* COMPUTER WEEKLY (July 29, 2013), http://www.computerweekly.com/news/2240202703/An-introduction-to-cyber-liability-insurance-cover [http://perma.cc/C92D-CJPL].

139 DEF. SEC. SERV., 2015 TARGETING U.S. TECHNOLOGIES: A TREND ANALYSIS OF CLEARED INDUSTRY REPORTING 10 (2014), http://www.dss.mil/documents/ci/2015_DSS_Trend_Report.pdf [http://perma.cc/M68R-DUNG].

140 *Id.*

141 *Id.*

142 *Id.*

143 *Id.* at 12.