Navigating the Cybersecurity Act of 2015

*Jasper L. Tran**

INTRODUCTION

The year 2014 was known as "the year of the cyber breach."[1] The year 2015 was not much different. High profile cyberattacks have been "a main topic of conversation in the boardroom and at the dinner table."[2] Every day, hackers target American businesses for purposes of cyberespionage and theft, stealing intellectual property, trade secrets, and sensitive government information.[3]

Congress slowly responded with several cybersecurity bills from both the House of Representatives and the Senate.[4] Most notably, the Senate introduced the Cybersecurity Information Sharing Act ("CISA" or S. 754),[5] while the House introduced the Protecting Cyber Networks Act ("PCNA" or H.R. 1560).[6] These bills share the same purpose: creating a pathway enabling private entities to share cyber information. How to share cyber information is what distinguishes the bills from one another. For instance, PCNA allows the private sector to share cyber information with the federal government but not through the NSA or the Department of Defense ("DOD"). On the other hand, CISA seeks to enhance and provide liability protections for information sharing between corporate entities, between corporate entities and the government, and between different

---

* Humphrey Policy Fellow, Google Policy Fellow. Sincere thanks to Tom Bell, Jeff Kosseff, Scott Schakelford, Denis Binder, Stephen Flores, Mike Hornak, David Groshoff, Drew Simshaw and other participants of the 2016 Symposium of the *Chapman Law Review* for their thoughtful comments. All views expressed herein are mine only, not those of my employer, sponsor, or affiliates. Contact me at tran4lr@gmail.com.

1 U.S. HOUSE OF REPRESENTATIVES PERMANENT SELECT COMM. ON INTELLIGENCE, THE PROTECTING CYBER NETWORKS ACT (H.R. 1560) (2015), http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/new%20bill%20summary%20pdf.pdf [http://perma.cc/2FW8-9EUR].

2 *Id.*

3 *Id.*

4 *See, e.g.*, Cyber Information Sharing Act, S. 754, 114th Cong. (2015); Cyber Threat Sharing Act of 2015, S. 456, 114th Cong. (2015); Protecting Cyber Networks Act, H.R. 1560, 114th Cong. (2015). *See generally infra* Parts I, II.

5 *See infra* Section I.B.1.

6 *See infra* Section II.B.1.

government agencies. This Article discusses these two bills in detail in Parts I and II.

As Congress considered the legislation, the President issued Executive Order 13636,[7] entitled "Improving Critical Infrastructure Cybersecurity,"[8] directing the National Institute of Standards and Technology ("NIST") to develop a "voluntary framework . . . for reducing cyber risks to critical infrastructure."[9] Accordingly, the NIST released a framework ("NIST Framework") in February 2014,[10] sharing many similar provisions of CISA and PCNA on information sharing.[11] This Article discusses Executive Order 13636 in Part III.

Given the federal government's strong interest in implementing a new cybersecurity information-sharing framework, CISA and PCNA, along with other cybersecurity bills, were combined into the Cybersecurity Act of 2015 ("CA'15"), discussed in detail in Part IV. The NIST Framework following Executive Order 13636 is already in place. Part V discusses my initial concerns about CA'15, and ethical implications and recommendations for practicing attorneys.

I. FROM THE SENATE: THE CYBERSECURITY INFORMATION SHARING ACT

A. CISA's History

In 2009, President Barack Obama declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation," and recognized that the United States is "not as prepared as we should be, as a government or as a country."[12] In 2013, the Center for Strategic and International Studies conducted a study and concluded that cybercrime costs the United States roughly $100 billion annually.[13] In 2014,

---

7 Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

8 *Executive Order -- Improving Critical Infrastructure Cybersecurity*, WHITE HOUSE (Feb. 12, 2013), https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity [http://perma.cc/8Z8X-TRQT] [hereinafter WHITE HOUSE'S *Executive Order*].

9 *Executive Order 13636: Cybersecurity Framework*, NAT'L INST. STANDARDS & TECH. (Nov. 12, 2013), http://www.nist.gov/cyberframework/ [http://perma.cc/E44P-WLXY].

10 *Id.*

11 *See generally* WHITE HOUSE'S *Executive Order*, *supra* note 8.

12 *Remarks by the President on Securing Our Nation's Cyber Infrastructure*, WHITE HOUSE (May 29, 2009), https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure [http://perma.cc/DNH4-DJW6].

13 Siobhan Gorman, *Annual U.S. Cybercrime Costs Estimated at $100 Billion*, WALL ST. J. (July 13, 2013, 6:49 PM), http://www.wsj.com/news/articles/SB10001424127887324328904578621880966242990.

PricewaterhouseCoopers surveyed and found that 69% of U.S. executives worry about the impact of cyberthreats to their company's growth, as compared to 49% of global executives who reported the same concern.[14]

From 2006 to 2015, incidents of loss, theft, and exposure of personally identifiable information increased by 1100%.[15] There were 3207 reported incidents of data breaches in 2012 and 813 million records exposed in 2013.[16] The year 2014 alone accounts for 67,168 cyber incidents against federal agencies, 27,624 of which involved personally identifiable information.[17] In 2015, the U.S. Office of Personnel Management suffered the theft of personal information[18] of 4.2 million current and former federal employees, and of 19.7 million applicants for background investigations.[19] These numbers only account for known incidents released to the public—the real numbers are likely much higher.

The threats are escalating,[20] calling for a nationwide security reform. The Senate responded by introducing CISA to enhance and provide liability protections for information sharing between corporate entities, between corporate entities and the government, and between different government agencies.[21]

CISA first appeared in the 113th Congress on July 10, 2014, as S. 2588, introduced by Senator Dianne Feinstein (D-CA).[22] It

---

14 PRICEWATERHOUSECOOPERS, U.S. CYBERCRIME: RISING RISKS, REDUCED READINESS 5 (2014), http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf [http://perma.cc/UJ85-WMMF].

15 *S. 754 – Cybersecurity Information Sharing Act of 2015*, SENATE REPUBLICAN POL'Y COMMITTEE (Aug. 3, 2015), http://www.rpc.senate.gov/legislative-notices/s-754_cybersecurity-information-sharing-act-of-2015 [http://perma.cc/GAC5-M8GA] [hereinafter SENATE REPUBLICAN POL'Y COMMITTEE].

16 Fred Donovan, *Confirmed: 2014 Is the Worst Year Ever for Data Breaches*, FIERCE IT SECURITY (Nov. 20, 2014), http://www.fierceitsecurity.com/story/confirmed-2014-worst-year-ever-data-breaches/2014-11-20 [http://perma.cc/H7AS-73WK].

17 Andrea Peterson, *This Terrifying Chart Explains Why Cybersecurity Is Such a Big Problem for the Government*, WASH. POST (June 18, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/06/18/this-terrifying-chart-explains-why-cybersecurity-is-such-a-big-problem-for-the-government/ [http://perma.cc/BFJ2-5PNY].

18 Such personal information includes full name, birth date, home address, and Social Security numbers. *Cybersecurity Resource Center: Cybersecurity Incidents*, U.S. OFF. PERSONNEL MGMT., https://www.opm.gov/cybersecurity/cybersecurity-incidents/#WhatHappened [http://perma.cc/Z3N7-YMKW].

19 *Id.* The 19.7 million figure does not include an additional "1.8 million non-applicants, primarily spouses or co-habitants of applicants." *Id.*

20 *See* SENATE REPUBLICAN POL'Y COMMITTEE, *supra* note 15. In fact, cybersecurity experts warn that a very big cyber attack is coming, predictably affecting everyone in America "and we don't even know it." Christopher Mims, *The Hacked Data Broker? Be Very Afraid*, WALL ST. J. (Sept. 8, 2015), http://www.wsj.com/articles/the-hacked-data-broker-be-very-afraid-1441684860.

21 *See generally infra* Section I.B.1.

22 *S.2588 – Cybersecurity Information Sharing Act of 2014*, CONGRESS.GOV, https://

passed the Senate Select Committee on Intelligence by a 12–3 vote, but did not reach a full senate vote before the end of the congressional session.[23] CISA reappeared again in the 114th Congress on March 12, 2015, as S. 754 by Senator Richard Burr (R-NC) and passed the Senate Intelligence Committee by a 14–1 vote.[24] S. 754 combines two Senate bills: CISA, and S. 456, the Cyber Threat Sharing Act of 2015 ("CTSA").[25]

B. CISA in Detail

It is important to note that CISA is strictly voluntary, i.e., there is no duty to share.[26] It expressly prohibits the federal government from coercing parties into sharing.[27] It also provides a safe harbor for participating entities, when they share information according to CISA's provisions; CISA does not shield entities from potential liability for failing to act. Parties taking advantage of CISA could use defensive measures, but they are prohibited from hacking back (i.e., harming a third party's system).[28] Furthermore, shared information can be used to prosecute cybercrimes and as evidence for crimes involving physical force.[29]

1. CISA's Notable Provisions[30]

CISA's purpose is "[t]o improve cybersecurity in the United States through enhanced sharing of information about

---

www.congress.gov/bill/113th-congress/senate-bill/2588?q=%7B%22search%22%3A%5B%22%5C%22s2588%5C%22%22%5D%7D&resultIndex=2 [http://perma.cc/EQE6-8UVS].

23 *See* Gregory S. McNeal, *Controversial Cybersecurity Bill Known as CISA Advances out of Senate Committee*, FORBES (July 9, 2014, 6:55 AM), http://www.forbes.com/sites/gregorymcneal/2014/07/09/controversial-cybersecurity-bill-known-as-cisa-advances-out-of-senate-committee/ [http://perma.cc/7A3V-G6GS].

24 *See* Andy Greenberg, *CISA Cybersecurity Bill Advances Despite Privacy Concerns*, WIRED (Mar. 12, 2015, 7:18 PM), http://www.wired.com/2015/03/cisa-cybersecurity-bill-advances-despite-privacy-critiques/ [http://perma.cc/L3A7-WGU3].

25 Taylor Armerding, *Cybersecurity Legislation Still Draws Intense Opposition*, CIO (Sept. 23, 2015, 7:08 AM), http://www.cio.com/article/2985469/security/cybersecurity-legislation-still-draws-intense-opposition.html [http://perma.cc/A77Z-MVNP].

26 Patrick Eddington, *OPM, CISA, and the Cybersecurity Oxymoron*, JUST SECURITY (July 2, 2015, 10:08 AM), https://www.justsecurity.org/24360/opm-cisa-cybersecurity-oxymoron/ [http://perma.cc/K8R8-RXS4].

27 John Evangelakos et al., *Sullivan & Cromwell Discusses the Cybersecurity Act of 2015*, CLS BLUE SKY BLOG (Jan. 6, 2016), http://clsbluesky.law.columbia.edu/2016/01/06/sullivan-cromwell-discusses-the-cybersecurity-act-of-2015/ [http://perma.cc/6ZG8-F8FV].

28 *Data, Privacy & Security Practice Report – January 19, 2016*, KING & SPALDING (Jan. 16, 2016), http://www.kslaw.com/News-and-Insights/PublicationDetail?us_nsc_id=9483.

29 *This Week the Cybersecurity Information Sharing Act Is on the Senate Floor & Apple Vehemently Opposes it,* PATENTLY APPLE (Oct. 21, 2015), http://www.patentlyapple.com/patently-apple/2015/10/this-week-the-cybersecurity-information-sharing-act-is-on-the-senate-floor-apple-vehemently-opposes-it.html [http://perma.cc/U6GM-H6NL].

30 The provisions described are from the version available in September 2015.

cybersecurity threats."[31] Section 1 sets out the title of the bill as the "Cybersecurity Information Sharing Act of 2015," and includes a table of contents of ten total sections.[32]

a. Sections 2 and 3

Section 2 defines various terms: agency, antitrust laws, appropriate federal entities, cybersecurity purpose, cybersecurity threat, cyberthreat indicator, defensive measure, entity, federal entity, information system, local government, malicious cyber command and control, malicious reconnaissance, monitor, private entity, security control, security vulnerability, and tribal.[33] Particularly, subsection 2(4) defines "cybersecurity purpose" as "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."[34]

Notably, subsection 2(7) defines "defensive measure" as "an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability," excluding "a measure that destroys, renders unusable, or substantially harms an information system or data on an information system."[35] The authorization to employ defensive measures forbids an entity from gaining unauthorized access to a computer network.[36]

Section 3 discusses the federal government's timely sharing of information through procedures developed and promulgated by the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General, in consultation with the heads of the appropriate federal entities.[37]

b. Section 4: Authorizations

Section 4 discusses authorization for preventing, detecting, analyzing, and mitigating cybersecurity threats: subsection 4(a) on authorization for monitoring, subsection 4(b) on authorization for operation of defensive measures, subsection 4(c) on authorization for sharing or receiving cyberthreat indicators or measures,

---

31 Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015).
32 *Id.* § 1.
33 *Id.* § 2.
34 *Id.* § 2(4).
35 SENATE REPUBLICAN POL'Y COMMITTEE, *supra* note 15.
36 *Id.*
37 S. 754 § 3(a).

subsection 4(d) on protection and use of information, and subsection 4(e) on antitrust exemption.[38]

Specifically, subsection 4(a) "[e]nables a private entity to monitor information systems for a cybersecurity purpose."[39] Subsection 4(b) "[e]nables a private entity to operate a defensive measure that is applied to information systems for cybersecurity purposes and narrowly permits the type of defensive actions a private entity may take."[40] Subsection 4(c) enables "a private entity to share with, or receive from, any other entity or the federal government a threat indicator or defensive measure . . . for cybersecurity purposes."[41]

Subsection 4(d) requires "an entity monitoring an information system, operating a defensive measure, or providing or receiving a cyber threat indicator or defensive measure . . . to protect against unauthorized access to or acquisition of such" information.[42] Subsection 4(d) also requires an entity (i) to "review information and to remove personal information not directly related to a cybersecurity threat" before sharing cybersecurity information, and (ii) "to implement and utilize technical capability to remove any personal information not directly related to a cybersecurity threat."[43]

Subsection 4(e) provides for an antitrust exemption, i.e., there is no antitrust violation "for 2 or more private entities to exchange or provide a cyber threat indicator, or assistance relating to the prevention, investigation, or mitigation of a cybersecurity threat . . . ."[44]

c. Section 5: Information Sharing

Section 5 establishes procedures for the government to "facilitate cybersecurity information sharing not later than 60 days after enactment of the bill."[45] Subsection 5(a) requires the federal government to "provide guidelines on the types of information that qualifies as a cybersecurity threat indicator and information protected under applicable privacy laws that are unlikely to be directly related to a cybersecurity threat."[46]

---

38 *Id.* § 4.
39 SENATE REPUBLICAN POL'Y COMMITTEE, *supra* note 15.
40 *Id.*
41 *Id.*
42 S. 754 § 4(d)(1).
43 SENATE REPUBLICAN POL'Y COMMITTEE, *supra* note 15.
44 S. 754 § 4(e)(1).
45 SENATE REPUBLICAN POL'Y COMMITTEE, *supra* note 15.
46 *Id.*

Subsection 5(b) requires the federal government to provide "guidelines relating to privacy and civil liberties that shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a federal entity obtained in connection with the cybersecurity activities."[47] Section 5(b) also requires the government "to periodically review the guidelines and content comprising cybersecurity information."[48]

Subsection 5(c) requires the Secretary of the Department of Homeland Security ("DHS") to "develop and implement a capability and process within DHS to accept cyber threat information through an automated system in real time."[49]

Subsection 5(d) clarifies "that information sharing will not constitute a waiver of any applicable privilege or protection," but rather, is voluntary, and "rights to proprietary information will not be infringed upon."[50] Specifically, subsection 5(d) does not allow the government "to use cyber information to investigate and prosecute 'serious violent felonies.'"[51]

d. Sections 6 Through 10

Section 6 protects a private entity from liability "for the monitoring of information systems or sharing or receipt of cyber threat indicators and defensive measures."[52]

Subsection 7(a) requires federal agencies to "submit information to various inspectors general in order to examine and oversee the implementation of cybersecurity information sharing, including content, effectiveness, and privacy and civil liberties."[53] Subsection 7(b) requires the Privacy and Civil Liberties Oversight Board to submit a report assessing the Act's effects and sufficiency to Congress and the President once every two years.[54]

Subsection 8(i) exempts entities from liability "for choosing not to engage in the voluntary activities" the act authorizes.[55] Subsection 8(k) provides for the bill's narrow construction and preemption of federal and state laws.[56]

---

47 *Id.*
48 *Id.*
49 *Id.*
50 *Id.*
51 *Id.*
52 *Id.*
53 *Id.*
54 Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. § 7(b) (2015).
55 *Id.* § 8(i).
56 *Id.* § 8(k). For a discussion on preemption, see Eric Lindenfeld & Jasper L. Tran,

Section 9 requires the Director of National Intelligence to submit a report on cyberthreats to the Senate Select Committee on Intelligence and the House Permanent Select Committee.[57]

Section 10 eliminates a new exemption in the Freedom of Information Act created specifically for cyber information; thus, information shared through the bill could still qualify under existing FOIA exemptions.[58]

2. CISA's Cost

CISA needs about twenty people to "administer the program, prepare the required reports and manage the exchange of information."[59]

The Congressional Budget Office ("CBO") estimates CISA's cost at about "$20 million over the 2016-2020 period, assuming appropriation of the estimated amounts."[60] Also, the "aggregate costs of the mandates on public entities would [likely] fall below the threshold for intergovernmental mandates."[61]

The Obama administration did not take a public stance on CISA prior the passage of the CA'15.[62]

II. FROM THE HOUSE: THE PROTECTING CYBER NETWORKS ACT

A. PCNA's History

Meanwhile, the House responded to the escalating cybersecurity threats with its own version of a cybersecurity bill—the PCNA. Congressman Devin Nunes (R-CA), along with eight cosponsors, first introduced PCNA to the House on March 24, 2015, and the House passed PCNA by a 307–116 vote on April 22, 2015.[63]

Beyond Preemption of Generic Drug Claims, 45 SW. L. REV. 241, 244 (2015).

57 S. 754 § 9.

58 SENATE REPUBLICAN POL'Y COMMITTEE, *supra* note 15.

59 *Congressional Budget Office Cost Estimate: S. 754 Cybersecurity Information Sharing Act of 2015,* CONG. BUDGET OFF. (Apr. 14, 2015), https://www.cbo.gov/sites/default/files/114th-congress-2015-2016/costestimate/s7540.pdf [http://perma.cc/F7P4-8J6X].

60 *Id.*

61 *Id.*

62 SENATE REPUBLICAN POL'Y COMMITTEE, *supra* note 15. However, the Obama administration has supported the House's companion bill, H.R. 1560 entitled "Protecting Cyber Networks Act," in an administration policy statement. *See* EXEC. OFFICE OF THE PRESIDENT, STATEMENT OF ADMINISTRATION POLICY: H.R. 1560 - PROTECTING CYBER NETWORKS ACT (Apr. 21, 2015), https://www.whitehouse.gov/sites/default/files/omb/ legislative/sap/114/saphr1560r_20150421.pdf [http://perma.cc/SZ74-JZS8] [hereinafter STATEMENT OF ADMINISTRATION: H.R. 1560]. *See generally infra* Section II.B.1.

63 Protecting Cyber Networks Act, H.R. 1560, 114th Cong. (2015). The eight cosponsors are Adam B. Schiff (D-CA), Lynn A. Westmoreland (R-GA), James A. Himes

B. PCNA in Detail

Providing strong protections for privacy and civil liberties, PCNA essentially enables the private sector to voluntarily share cyberthreat indicators with each other and with the federal government, but not through the NSA or the DOD.[64] In discussing PCNA's provisions, I will also note similarities between the PCNA and CISA.

1. PCNA's Notable Provisions

PCNA's purpose is to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats. Section 1 sets out the short title of the bill as the "Protecting Cyber Networks Act," and includes a table of contents of the eleven following sections.[65] Sections 2 and 4 amend Title I of the National Security Act of 1947.[66]

a. Sections 2 Through 4

PCNA's section 2, like part of CISA's section 5,[67] discusses the sharing of cyberthreat indicators and defensive measures in real time by the DOD and NSA with the private sector, including declassifying the information and sharing at an unclassified level.[68] Particularly, the federal government must remove "personal information or information identifying a specific person that does not directly relate to a cyber threat."[69]

PCNA's section 3, like CISA's section 4,[70] discusses authorizations for "preventing, detecting, analyzing, and mitigating cybersecurity threats" of private and non-federal entities. Particularly, "[s]ubsection (a) does not authorize the Federal Government to conduct surveillance of any person."[71] Notably, subsection 3(b) does not authorize any defensive

---

(D-CT), Peter T. King (R-NY), Frank A. LoBiondo (R-NJ), Terri A. Sewell (D-AL), Mike Quigley (D-IL), and Patrick Murphy (D-FL). *H.R.1560 - Protecting Cyber Networks Act,* CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/house-bill/1560/actions [http://perma.cc/TT7Q-58MA].

64 *See generally infra* Section II.B.1.

65 H.R. 1560.

66 *Id.* §§ 2(a), 4(a).

67 *See supra* Section I.B.1.

68 U.S. HOUSE OF REPRESENTATIVES PERMANENT SELECT COMM. ON INTELLIGENCE, THE PROTECTING CYBER NETWORKS ACT: SECTION-BY-SECTION ANALYSIS http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/new%20section%20by%20section%20pdf.pdf [http://perma.cc/TZ9P-DLQ8] [hereinafter HR1560 SECTION-BY-SECTION].

69 *Id.*

70 *See supra* Section I.B.1.

71 HR1560 SECTION-BY-SECTION, *supra* note 68.

measure that "destroys, renders unusable or inaccessible . . . or substantially harms" other networks, which includes "hacking back" or other forms of cyber activities that use computers or networks without their owner's consent.[72]

PCNA's section 4, like CISA's section 5,[73] discusses sharing of cyberthreat indicators and defensive measures with appropriate federal entities.[74] PCNA's subsection 4(b) requires the Attorney General to outline privacy and civil liberties guidelines.[75] Subsection 4(d) specifies the purposes the federal government may use a cyberthreat indicator received from non-federal entities:

> cybersecurity purpose; preventing or prosecuting a threat of death or seriously bodily harm or an offense arising out such a threat; preventing or prosecuting a serious threat to a minor, including sexual exploitation; or preventing or prosecuting espionage, economic espionage, serious violent felonies, and violations of the Computer Fraud and Abuse Act.[76]

b. Sections 5 Through 7

Section 5 establishes a private cause of action as the exclusive means for seeking a remedy for a violation of the Act by the federal government.[77] It provides for statutory damages, reasonable attorney fees, and a statute of limitations for the federal government's violation of the privacy and civil liberties guidelines under subsection 4(b).[78]

PCNA's section 6, like part of CISA's section 6,[79] protect a private entity from causes of action for the monitoring of an information system or sharing of cyberthreat indicators or defensive measures.[80] Notably, section 6 defines "willful misconduct" as "an act or omission that is taken (A) intentionally to achieve a wrongful purpose; (B) knowingly without legal or factual justification and; (C) in disregard of a known or obvious risk that is so great as to make it highly probable that the harm will outweigh the benefit," and establishes the standard to prove willful misconduct.[81]

---

72 *Id.*
73 *See supra* Section I.B.1.
74 HR1560 SECTION-BY-SECTION, *supra* note 68.
75 *Id.*
76 *Id.*
77 *Id.*
78 *Id.*
79 *See supra* Section I.B.1.
80 HR1560 SECTION-BY-SECTION, *supra* note 68.
81 Protecting Cyber Networks Act, H.R. 1560, 114th Cong. § 6(c) (2015).

PCNA's section 7, like CISA's section 7, requires submission of reports for oversight of government activities.[82]

c. Sections 8 Through 11

PCNA's section 8, like CISA's section 9,[83] requires the Director of National Intelligence, in consultation with the Intelligence Community, "to submit a report to congressional intelligence committees on cybersecurity threats."[84]

Section 9 contains various construction and preemption provisions to make clear that, essentially, PCNA does not authorize the government to target a person for surveillance.[85] Section 9 also does not "limit or modify any existing information-sharing relationships outside of [PCNA] or prohibit any new information-sharing relationships outside of [PCNA]."[86]

Section 10 amends the United States Code, 5 U.S.C. § 552(b) and 10 U.S.C. § 2224.[87]

PCNA's section 11, like CISA's section 2,[88] narrowly defines various terms: agency, appropriate federal entities, cybersecurity purpose, cyberthreat, cyberthreat indicator, defensive measure, federal entity, information system, local government, malicious cyber command and control, malicious reconnaissance, monitor, non-federal entity, private entity, real time and real-time, security control, security vulnerability, and tribal.[89]

PCNA's section 11(4) defines "cybersecurity threat" as:

> an action, not protected by the first amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, confidentiality, integrity, or availability of an information system or information that is stored on, processed by, or transiting an information system[,] . . . [excluding] any action that solely involves a violation of a consumer term of service or a consumer licensing agreement."[90]

---

82 H.R. 1560 § 7; *see also supra* Section I.B.1.
83 *See supra* Section I.B.1.
84 HR1560 SECTION-BY-SECTION, *supra* note 68.
85 *Id.*
86 *Id.*
87 H.R. 1560 § 10; HR1560 SECTION-BY-SECTION, *supra* note 68.
88 *See supra* Section I.B.1.
89 H.R. 1560 § 11; HR1560 SECTION-BY-SECTION, *supra* note 68.
90 H.R. 1560 § 11(4).

2. PCNA's Cost

The CBO estimates PCNA's implementation cost at "$186 million over the 2016-2020 period, assuming appropriation of the estimated amounts."[91]

Although the Obama administration publicly supported PCNA,[92] out of the gate, both bills, especially S. 754, faced opposition from many organizations on the grounds of violating privacy and civil rights.[93] Names like "cyber-surveillance" were tossed around.[94]

III. FROM THE PRESIDENT: THE "VOLUNTARY" FRAMEWORK FOLLOWING EXECUTIVE ORDER 13636

As Congress considered legislation, the President in February 2013 issued Executive Order 13636, entitled "Improving Critical Infrastructure Cybersecurity," directing the NIST to develop a "voluntary" framework for reducing cyber risks to critical infrastructure.[95] Accordingly, the NIST released a framework in February 2014,[96] sharing many similar provisions of CISA and PCNA on information sharing.[97] Before the passage of CA'15, Executive Order 13636 was the only serious action taken by the government to strengthen U.S. cybersecurity, but the NIST Framework is voluntary in nature, encouraging—rather than requiring—action on the private sector's part.

"The private sector faces a rapidly shifting terrain without clear standards."[98] Following the Federal Trade Commission's

---

91 *H.R. 1560, Protecting Cyber Networks Act*, CONG. BUDGET OFF. (Apr. 13, 2015), https://www.cbo.gov/publication/50110 [http://perma.cc/6XB8-KNL3]. The CBO also addresses the small and potentially insignificant amount of "criminal prosecutions, which could increase federal revenues from fines as well as direct spending from the Crime Victims Fund," and the possibility of the government's liability "if an agency or department were to violate the privacy and civil liberty guidelines required by the bill." *Id.*

92 *See* STATEMENT OF ADMINISTRATION: H.R. 1560, *supra* note 62.

93 *See, e.g.*, *Consumer Advocates Letter to Senate on Cybersecurity Information Sharing Act,* CTR. FOR DEMOCRACY & TECH. (Oct. 21, 2015), https://cdt.org/insight/consumer-advocates-letter-to-senate-on-cybersecurity-information-sharing-act/ [http://perma.cc/SL4L-434Q].

94 *See, e.g.*, Robyn Greene, *Cybersecurity Information Sharing Act of 2015 Is Cyber-Surveillance, Not Cybersecurity*, NEW AM.: OPEN TECH. INST. (Apr. 9, 2015), https://www.newamerica.org/oti/cybersecurity-information-sharing-act-of-2015-is-cyber-surveillance-not-cybersecurity/ [http://perma.cc/3JZW-VGWM].

95 *Executive Order 13636: Cybersecurity Framework, supra* note 9.

96 *See id.*

97 *See generally* WHITE HOUSE'S *Executive Order*, *supra* note 8.

98 *Cybersecurity: Private Sector Faces Increasing Regulatory Risk from Agency Enforcement and Informal "Guidance" Becoming Standard of Care*, FEDERALIST SOC'Y (Oct. 15, 2015), http://www.fed-soc.org/events/detail/cybersecurity-private-sector-faces-increasing-regulatory-risk-from-agency-enforcement-and-informal-guidance-becoming-standard-of-care [http://perma.cc/TZE2-E43J] [hereinafter FEDERALIST SOC'Y].

("FTC") recent win in *FTC v. Wyndham*,[99] regulatory agencies are expanding "oversight through informal guidance and threat of enforcement."[100]

In October 2015, the Federalist Society and partners from the private sector met to discuss current cybersecurity trends and what the private sector faces in 2015 and 2016, as well as the following questions:

> Will the President's Executive Order, and the NIST Cybersecurity Framework, become the de facto standard for the private sector? Is the federal government regulating through the threat of enforcement by [the] FTC, FCC, and other federal agencies, instead of through more regular administrative processes? What should companies make of emerging agency "guidance" from agencies like the FDA, SEC, [the National Highway Traffic Safety Administration], and DoD, on operations and innovation in areas like the Internet of Things, mobile applications and devices, cloud services, [and] connected cars?[101]

IV. THE CURRENT LAW OF THE LAND: THE CYBERSECURITY ACT OF 2015

On December 18, 2015, President Obama signed into law the Cybersecurity Act of 2015 as part of the Omnibus Appropriations Act.[102] CA'15 contains the majority of CISA's provisions, but with three notable exceptions: (1) network operators have monitoring privileges; (2) network operators can operate defensive measures; and (3) network operators can share cyberthreat information with others.[103]

---

99 F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015) (affirming the district court's decision upholding the FTC's data protection authority).

100 FEDERALIST SOC'Y, *supra* note 98.

101 *Id.*

102 Everett Rosenfeld, *The Controversial 'Surveillance' Act Obama Just Signed*, CNBC (Dec. 22, 2015, 12:34 PM), http://www.cnbc.com/2015/12/22/the-controversial-surveillance-act-obama-just-signed.html [http://perma.cc/C4Z4-VYWJ].

103 Orin Kerr provided some context for the provider exception, stating:

> The statutory surveillance laws . . . generally prohibit Internet surveillance subject to certain exceptions. Each of the laws has what is known as the provider exception. The provider exception allows telecommunications providers to conduct surveillance on their networks, and if necessary to disclose user communications, when it is 'a necessary incident . . . to the protection of the rights or property of the provider of that service.'

Orin Kerr, *How Does the Cybersecurity Act of 2015 Change the Internet Surveillance Laws?*, WASH. POST: THE VOLOKH CONSPIRACY (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/6UXK-UD6E].

The exceptions in CA'15 contain the following definitions:

(1) "monitor" is defined as "to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system";[104]

(2) "defensive measure" is defined as "an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability," but does not include "a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system";[105] and

(3) "cyber threat indicator" is defined as "information that is necessary to describe or identify" the following item(s) or any combination thereof: malicious reconnaissance; malicious cyber command and control; a security vulnerability; a method of defeating a security control; a method of causing a user to enable the defeat of a security control; the actual or potential harm caused by an incident; or any other attribute of a cybersecurity threat.[106]

Orin Kerr has noted that CA'15:

> [S]ubstantially broadens the powers of network operators to monitor and disclose beyond the existing provider exception and trespasser exception. The new language focuses mostly on the purpose of the monitoring and disclosure, with relatively little in place about the scope of monitoring or disclosure (although there is a requirement of scrubbing personal data if known). And it seems to allow monitoring for cybersecurity purposes generally, including outsourcing of that role to others, instead of limiting the exception to monitoring to protect the provider's own network.[107]

Specifically, exception (1) contains unclear language that can be "broadly" interpreted; exception (2) is "largely a retread of the existing provider exception"; and exception (3) "expands on the provider exception because the disclosure does not need to be for the protection of the operator's own network."[108]

---

104 Cybersecurity Act of 2015, Pub. L. No. 114-113, § 102(13), 129 Stat. 2242, 2938. Information system is defined elsewhere as "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." 44 U.S.C. § 3502(8) (2012).

105 § 102(7), 129 Stat. at 2937.

106 § 102(6), 129 Stat. at 2937; *see also* § 102(11), 129 Stat. at 2938.

107 Kerr, *supra* note 103.

108 *Id.*

On the other hand, Jennifer Granick has noted that the language in CA'15 could trump forthcoming federal regulatory efforts as well as state privacy laws.[109]

V. CONCERNS, ETHICAL IMPLICATIONS, AND RECOMMENDATIONS

The NIST Framework following Executive Order 13636 was already in place when CA'15 was signed into law. Given that the Obama administration publicly supported H.R. 1560,[110] it was foreseeable that CA'15 would be signed by President Obama to become the law of the land. CA'15 might be as good as it can get with bipartisan and presidential approval—the best Congress can do with the ongoing political gridlock.

I have several initial concerns. First, sharing information does little to prevent successful cyberattacks, given that there have been many already in place. For instance, in 2003, DHS established its U.S. Computer Emergency Readiness Team to collect and analyze data, but its results have been unclear. Second, the process of sharing information with the government and other private entities creates a new opportunity for more hacking and information being stolen. Third, CA'15—and its parent CISA—is still a surveillance bill that could use shared information to spy on U.S. citizens. Fourth, CA'15 has not solved the problem of incentivizing attorneys to disclose their clients' information. Lastly, CA'15 will very likely face constitutional challenges in courts; the battle of right to privacy in the realm of cybersecurity is far from over.[111]

Instead of expanding the provider exception in CA'15,[112] the government should focus its efforts on tackling the lack of incentive problem. New cybersecurity bills or acts are still focused on information sharing, which the NIST Framework from Executive Order 13636 was supposed to accomplish already.

Going forward, I leave with four ethical implications and recommendations for practicing attorneys. First, attorneys and corporations should carefully consider the manner in which an attorney shares client information. Attorneys can share IT

---

109 Jennifer Granick, *OmniCISA Pits DHS Against the FCC and FTC on User Privacy*, JUST SECURITY (Dec. 16, 2015, 6:09 PM), https://www.justsecurity.org/28386/omnicisa-pits-government-against-self-privacy/ [http://perma.cc/A3MF-CXG5].

110 *See* STATEMENT OF ADMINISTRATION: H.R. 1560, *supra* note 62.

111 At the 2016 *Chapman Law Review* Symposium, Denis Binder agreed and commented that there "will definitely be constitutional challenges" to CA'15. For a discussion on the right to privacy, see generally Jasper L. Tran, *The Right to Attention*, 91 IND. L.J. (forthcoming 2016).

112 *See generally supra* Part IV and note 103.

information, such as the manner of a cyberattack, without revealing too much confidential information, such as the content of the attack. How to share such information matters as well; it is better for an attorney to pick up the phone and call when communicating—leaving no paper trail behind.

Second, an attorney sharing cybersecurity information with a party who is not that attorney's client—including the federal government or others in the private sector—could result in a waiver of attorney-client privilege[113] and/or a violation of that attorney's duty of confidentiality.[114] An attorney must guard the privilege, as well as comply with this confidentiality duty.[115] Even inadvertent disclosure of a client's confidential information could waive this privilege. Attorneys want to keep their clients happy, and losing this privilege would not make anyone happy. Even if confidentiality concerns are resolved, the attorney still needs to ensure there are no conflicts of interest involved, which is difficult when there are too many people "in the loop."

Third, there is a lack of incentive for the attorney to disclose his/her client's confidential or sensitive information. There is an industry norm of keeping the information of an attorney's client private. No attorney wants to deviate from the industry norm; the client might mistrust that attorney and replace them with some other attorney whom the client can trust. As noted above, the current CA'15 has not solved this lack of incentive problem.

Fourth, the public announcement of a client's confidential or sensitive cybersecurity information could hurt the current client's business, and even result in an attorney losing future clients. This is often due to how much loss a client has suffered from a recent attack, or because a client was targeted for an attack in the first place—scaring that client's current and potential customers. No attorney wants a reputation for leaking a client's information.

In light of the above recommendations, attorneys can still share information when appropriate—exercising their best judgment.

---

113 *See, e.g.*, FED. R. EVID. 502 ("'[A]ttorney-client privilege' means the protection that applicable law provides for confidential attorney-client communication.").

114 *See, e.g.*, PAUL R. RICE ET AL., ATTORNEY-CLIENT PRIVILEGE IN THE U.S. § 2.1 (2015–2016 ed. 2015) ("The attorney-client privilege is a rule of evidence, with an importance long recognized. It protects the confidentiality of communications between an attorney and client.").

115 *See, e.g.*, MODEL RULES OF PROF'L CONDUCT r. 1.6 (AM. BAR ASS'N 2014).

CONCLUSION

This Article summarizes the legislative history, notable provisions, and current status of CISA, PCNA, Executive Order 13636, and CA'15. The Article ended with four ethical implications and recommendations. And the most important take-away is: when in doubt, attorneys should not share.