THE PRIVACY ISSUES PRESENTED BY THE CYBERSECURITY INFORMATION SHARING ACT

ABSTRACT

On December 18, 2015, President Obama signed the Cybersecurity Information Sharing Act ("CISA") into law. CISA's purpose is to combat cyber threats by promoting information sharing between private entities and government agencies. CISA authorizes the Department of Homeland Security to facilitate the bulk collection of "cyber threat" and "defensive measure" information from the private sector. Within CISA, the definitions of "cyber threat" and "defensive measure" are broad. CISA also provides liability protection to entities that provide the information, and the information that is collected is not subject to open records laws. There is little control on what information is collected or how it is used. The flaws in the Act pose serious privacy risks.

I. INTRODUCTION 396
II. THE CYBERSECURITY INFORMATION SHARING ACT 399
III. THE ISSUES WITH CISA 401
A. RISKS REGARDING DATA COLLECTION 402
B. RISKS REGARDING GOVERNMENT DATA USE 406
IV. CISA IS FLAWED 409
V. CONCLUSION 410

I. INTRODUCTION

On December 18, 2015, President Obama signed the Cybersecurity Act of 2015, or the Cybersecurity Information Sharing Act ("CISA"),[1] into law.[2] The bill was a last second addition to the 2016 omnibus spending bill.[3] The purpose of CISA is to establish a core cybersecurity information-sharing framework between private entities and the federal government.[4] This framework, the participation in which is voluntary, provides for real-time information sharing of "cyber threat indicators" and "defensive measures" between the government and the private sector.[5]

Congress designed CISA to stem the rising tide of data breaches, private and public, by allowing companies to share cybersecurity threat data with the Department of Homeland Security ("DHS").[6] The DHS could then use this data to combat the threats by developing defenses to these attacks and by issuing warnings about the threats they pose.[7] These cybersecurity attacks are a very real threat. As the DHS puts it:

> Cyberspace is particularly difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in

1. Cybersecurity Act of 2015, Pub. L. No. 114-113, 129 Stat. 2242 [hereinafter CISA].

2. Tom Risen, *Obama Signs Cybersecurity Law in Spending Package*, U.S. NEWS AND WORLD REP. (Dec. 18, 2015), http://www.usnews.com/news/articles/2015-12-18/obama-signs-cybersecurity-law-in-spending-package.

3. *Id.*

4. 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.

5. *Id.*

6. *Id.*

7. *Id.*

> complex cyber networks. Of growing concern is the cyber threat to critical infrastructure, which is increasingly subject to sophisticated cyber intrusions that pose new risks. As information technology becomes increasingly integrated with physical infrastructure operations, there is increased risk for wide scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans depend. In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace has become an important homeland security mission.[8]

In 2015 alone, over $1 billion was stolen and 300 million records were leaked.[9] Several high-profile cyber-attacks have highlighted these risks.[10] In 2013, hackers breached Target's payment systems, stealing approximately 40 million credit and debit card accounts.[11] This breach cost Target approximately $250 million.[12] In 2014, a hack at Sony Corp. exposed Hollywood secrets, compromised employee records, and destroyed company data.[13] In October 2015, Sony settled employee claims for $8 million.[14] In 2015, the adult-themed, extramarital affair website Ashley Madison was hacked.[15] Those hackers exposed the personal information of some 32 million users.[16] The United States government is also a target. In an attack that began in 2014 and continued for several months thereafter, hackers accessed and stole the background investigation records of millions of current, former, and prospective federal employees and contractors.[17]

---

8. *Cybersecurity Overview,* U.S. DEPT. OF HOMELAND SECURITY (Sept. 22, 2015), https://www.dhs.gov/cybersecurity-overview.

9. Paul Szoldra, *The 9 Worst Cyber Attacks of 2015*, TECH INSIDER (Dec. 29, 2015), http://www.techinsider.io/cyberattacks-2015-12.

10. *Id.*

11. Associated Press and James Eng, *Target Reaches Settlement with Visa Over 2013 Data Breach*, NBC NEWS (Aug. 18, 2015), http://www nbcnews.com/tech/security/target-reaches-settlement-visa-over-2013-data-breach-n412071.

12. Kevin M. McGinty, *Target Data Breach Price Tag: $252 Million and Counting*, PRIVACY AND SECURITY MATTERS (Feb. 26, 2015), https://www.privacyandsecuritymatters.com/2015/02/target-data-breach-price-tag-252-million-and-counting/.

13. Edward Peterson, *Sony to Pay as Much as $8 Million to Settle Data-Breach Case*, BLOOMBERG (Oct. 20, 2015), http://www.bloomberg.com/news/articles/2015-10-20/sony-to-pay-as-much-as-8-million-to-settle-data-breach-claims.

14. *Id.*

15. Robert Hackett, *What to Know About the Ashley Madison Hack*, FORTUNE (Aug. 26, 2015), http://fortune.com/2015/08/26/ashley-madison-hack/.

16. *Id.*

17. James Eng, *OPM Hack: Government Finally Starts Notifying 21.5 Million Victims*, NBC NEWS (Oct. 1, 2015), http://www nbcnews.com/tech/security/opm-hack-government-finally-starts-notifying-21-5-million-victims-n437126.

The hackers also stole the fingerprints of 5.6 million federal employees.[18] There are countless other examples.[19]

These hackers are technologically advanced.[20] They innovate and adapt to new technologies.[21] Their methods are complex.[22] The attacks range from lone wolf hits to large, coordinated assaults.[23] The attacks can be launched from anywhere in the world and are difficult to combat.[24] CISA is meant to help combat these attacks through more robust and timely sharing of cyber threat information both between the government and the private sector and between private companies themselves.[25]

While its goal may be commendable, CISA has its share of critics.[26] The criticism revolves around privacy and the efficacy of the Act.[27] New America's Open Technology Institute sent a coalition letter to the Senate stating that CISA would "seriously threaten privacy and civil liberties, and could undermine cybersecurity, rather than enhance it."[28] The letter goes on to say that "CISA fails to provide both strong privacy protections and adequate clarity about what actions can be taken, what information can be shared, and how that information may be used by the government."[29] The Institute is not alone; technology giants such as Apple, Google, Amazon and Microsoft also oppose the bill.[30]

---

18. *Id.*

19. *See* Lewis Morgan, *List of Data Breaches and Cyber Attacks in 2015 – over 480 Million Leaked Records*, IT GOVERNANCE (Jan. 8, 2016), http://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2015-over-275-million-leaked-records/.

20. Raja Patel, *Study Reveals the Most Common Attack Methods of Data Thieves*, INFORMATIONWEEK (July 30, 2015), http://www.darkreading.com/partner-perspectives/intel/study-reveals-the-most-common-attack-methods-of-data-thieves/a/d-id/1321544.

21. *Id.*

22. *Id.*

23. *Id.*

24. *Id.*

25. Christopher Harvie & Cynthia J. Larose, *Happy New Year - Cybersecurity Information Sharing Act*, NAT'L L. REV. (Jan. 6, 2015), http://www natlawreview.com/article/happy-new-year-cybersecurity-information-sharing-act.

26. Abigail Tracy, *The Problems Experts and Privacy Advocates Have with The Senate's Cybersecurity Bill*, FORBES (Oct. 29, 2015), http://www forbes.com/sites/abigailtracy/2015/10/29/the-problems-experts-and-privacy-advocates-have-with-the-senates-cybersecurity-bill/#497cecab30fc.

27. *Id.*

28. Robyn Greene, *Coalition Letter from 55 Civil Society Groups, Security Experts, and Academics Opposing CISA*, OPEN TECH. INST. (Apr. 21, 2015), https://www newamerica.org/oti/coalition-letter-from-55-civil-society-groups-security-experts-and-academics-opposing-cisa/.

29. *Id.*

30. Joe Paglieri, *Apple and Other Tech Giants Slam Anti-Hacking Bill for Being Creepy*, CNN (Oct. 26, 2015), http://money.cnn.com/2015/10/26/technology/cisa-cybersecurity-bill-senate/; Jeffrey Schwartz, *Cybersecurity Information Sharing Act Sets Back Privacy*, REDMOND MAG. (Dec. 21, 2015), https://redmondmag.com/blogs/the-schwartz-report/2015/12/security-act-sets-back-privacy.aspx.

Everyone agrees that the world is facing an enormous cyber threat. The question is whether another government information system in general, and CISA specifically, is the right way to addresses that threat.

II. THE CYBERSECURITY INFORMATION SHARING ACT

The purpose of CISA is to detect, prevent, or mitigate cyber security threats or security vulnerabilities.[31] In order to do so, CISA requires the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General to develop procedures for private entities to share information with, between, and among government entities.[32] These procedures are to be developed in consultation with the appropriate Federal entities.[33] Private entities are not required to participate but rather may share and receive any "cyber threat indicator" and "defensive measure" with other entities and the federal government.[34] Entities that participate are given liability protection related to the information that they provide.[35]

CISA mandates that the Attorney General and Secretary of Homeland Security develop information sharing procedures that allow the federal government to receive "cyber threat indicators and defensive measures" from private entities.[36] CISA also mandates that these indicators and measures are shared with the appropriate federal entities in an automated, real-time manner.[37] The Act defines "appropriate federal entities" as the Department of Commerce, the Department of Defense, the Department of Energy, the Department of Homeland Security, the Department of Justice, the Department of the Treasury, and the Office of the Director of National Intelligence.[38] The National Security Agency ("NSA") would also be included since it falls under the Director of National Intelligence.[39]

---

31. *See* S. REP. NO. 114-32, at 1 (2015).
32. CISA § 103(a), (a)(1)-(5).
33. *Id.* § 103(b)(2).
34. *Id.* § 104(c)(1).
35. *Id.* § 106(b). As long as the information is provided "in accordance with this [act]" private entities are protected from liability. *Id* §106(b)(1). If the information is so provided, "[n]o cause of action shall lie or be maintained in any court against any entity, and such action shall be promptly dismissed, for the sharing or receipt of cyber threat indicators or defensive measures under [this act]." *Id.* § 106(b).
36. *Id.* § 105(a).
37. *Id.* § 105(a)(3)(A)(i)-(ii).
38. *Id.* § 102(3).
39. *See* OFF. OF THE DIRECTOR OF NAT'L INTELLIGENCE, http://www.dni.gov/index.php/intelligence-community/members-of-the-ic (last visited April 15, 2016).

One of the tenants of CISA is the timely delivery of cybersecurity threat information to the agencies that need it.[40] The information that is collected must be shared with all of the federal agencies that need it.[41] The Attorney General and the Secretary of Homeland Security, in coordination with other federal agencies, are ultimately responsible for the policies and procedures that govern the data collection process.[42] These procedures are meant to promulgate:

> (1) the timely sharing of classified cyber threat indicators and defensive measures in the possession of the Federal Government with representatives of relevant Federal entities and non-Federal entities that have appropriate security clearances;
>
> (2) the timely sharing with relevant Federal entities and non-Federal entities of cyber threat indicators, defensive measures, and information relating to cybersecurity threats or authorized uses under this title, in the possession of the Federal Government that may be declassified and shared at an unclassified level;
>
> (3) the timely sharing with relevant Federal entities and non-Federal entities, or the public if appropriate, of unclassified, including controlled unclassified, cyber threat indicators and defensive measures in the possession of the Federal Government;
>
> (4) the timely sharing with Federal entities and non-Federal entities, if appropriate, of information relating to cybersecurity threats or authorized uses under this title, in the possession of the Federal Government about cybersecurity threats to such entities to prevent or mitigate adverse effects from such cybersecurity threats; and
>
> (5) the periodic sharing, through publication and targeted outreach, of cybersecurity best practices that are developed based on ongoing analyses of cyber threat indicators, defensive measures, and information relating to cybersecurity threats or authorized uses under this title, in the possession of the Federal Government, with attention to accessibility and implementation challenges faced by small business concerns (as defined in section 3 of the Small Business Act (15 U.S.C. 632)).[43]

40. CISA § 105(a)(3)(A)(ii).
41. *Id.* § 105(a)(3)(A)(i).
42. *Id.* § 105(a)(2).
43. *Id.* § 103(a).

In addition to cybersecurity, the information collected under this program can also be used to respond to, prevent, mitigate, and prosecute certain crimes.[44] These crimes include fraud, identity theft, espionage, censorship, and trade secrets.[45] The information can also be used in order to respond to, prevent, or mitigate a specific threat of death, serious bodily harm, or serious economic harm[46] or to protect a minor from harm or sexual exploitation.[47] These non-cybersecurity related uses are included in CISA despite the fact the bill's purpose is to combat cybersecurity threats. The information is not supposed to be used by the government to monitor lawful activities.[48] Finally, the collected information is not supposed to include any personal information unless that information specifically relates to a cyber threat.[49]

From an oversight perspective, CISA requires the Director of National Intelligence to periodically report to the Intelligence Committees of the House and Senate.[50] These reports should include an assessment of the current cybersecurity risks, the ability of the United States Government to respond to or prevent cyber attacks, an assessment of current intelligence sharing and cooperation relationships with other countries, and an assessment of adding additional technologies in order to enhance the security of the United States.[51]

Taken in total, CISA authorizes the federal government to create a new database in order to track cybersecurity threat information. While addressing the cybersecurity threat seems to make sense, the question is whether this database is the right tool to address the issue.

III. THE ISSUES WITH CISA

The first issue with CISA is how it actually became law. CISA did not pass on its own. Rather, it was added as a rider to the 2016 spending bill.[52] The bill was passed, at least in part, in order to avoid a government shutdown.[53] At some point in the budget negotiations,[54] CISA was added to

44. *Id.* § 105(d)(5)(A).
45. *Id.* § 105(d)(5)(A)(v)(I)-(III).
46. *Id.* § 105(d)(5)(A)(iii).
47. *Id.* § 105(d)(5)(A)(iv).
48. *See id.* § 104(a)(2)(A)-(B).
49. *Id.* § 104(d)(2).
50. *Id.* § 109(a).
51. *Id.* § 109(b)(1)-(5).
52. Bender, *supra* note 4.
53. See Alexandra Howard, *Congress Ties Controversial Cybersecurity Bill to Key Spending Package*, HUFFINGTON POST (Dec. 16, 2015), http://www huffingtonpost.com/entry/cisa-omnibus-spending-bill567176b7e4b0dfd4bcc00143.

the $1.1 trillion appropriations bill and ultimately became law.[55] Prior to becoming law, there were at least two separate versions of the bill: one in the House of Representatives and one in the Senate.[56] Neither version ultimately passed.[57] Opponents of the bill were disappointed that the opportunity for "open and robust negotiation" regarding the controversial bill was lost.[58]

> Passing the Federal budget before the end of the year was a key priority and became a fortuitous opportunity for Congress to slip in the controversial Cybersecurity Information Sharing Act of 2015 into the spending bill, which President Obama on Friday signed into law. IT providers Amazon, Apple, Google, Microsoft and others have opposed measures in CISA, which seeks to thwart crime and terrorism but facilitates mass surveillance via the sharing of information between companies and the government, notably the National Security Agency.[59]

The fact that CISA was not debated on its own merits opens questions into why the final version differed from previous versions.[60]

A. RISKS REGARDING DATA COLLECTION

Now that CISA has become law, the question turns to what effect the law will have, both in terms of combating cyber attacks but also for privacy. Privacy advocates are reluctant to give the NSA another avenue to collect information on United States citizens.[61] Because the NSA has access to the data, there is legitimate concern that CISA is just another surveillance bill

---

54. Laura Barron-Lopez and Matt Fuller, *Lawmakers Finally Reach Deal On Spending Bill, Tax Package*, HUFFINGTON POST (Dec. 16, 2015), http://www huffingtonpost.com/entry/congress-omnibus-deal5670c8cee4b0dfd4bcbfe05f?9ipgy14i.

55. President Obama signed the bill on December 18, 2015. Risen, *supra* note 2.

56. *Compare* S. 754, 114th Cong. (2015) *with* H.R. 1560, 114th Cong. (2015).

57. *See* Pub. L. No. 114-113, 129 Stat. 2242 for the version that ultimately became law..

58. *OTI Deeply Disappointed About Passage of Dangerous Cybersecurity Bill*, OPEN TECH. INST. (Dec. 18, 2105), https://www newamerica.org/oti/oti-deeply-disappointed-about-passage-of-dangerous-cybersecurity-bill/. *See also* Press Release, Wyden Votes 'No' on Harmful Cyber Bill and Weakening Oversight of Surveillance Programs (Dec. 18, 2015), https://www.wyden.senate.gov/news/press-releases/wyden-votes-no-on-harmful-cyber-bill-and-weakening-oversight-of-surveillance-programs ("Ultimately, I cannot vote for this badly flawed CISA bill. The latest version of the CISA is the worst one yet – it contains substantially fewer oversight and reporting provisions than the Senate version did. That means that violations of Americans' privacy will be more likely to go unnoticed.").

59. Schwartz, *supra* note 30.

60. *See infra* Part III.B.

61. Peter Hess, *Controversial New Cybersecurity Law May Compromise Privacy: Critics Argue that CISA is More About Surveillance than Security*, SCIENCELINE (Jan. 24, 2016), http://scienceline.org/2016/01/controversial-new-cybersecurity-law-may-compromise-privacy/.

disguised as cyber security.[62] By its nature, CISA allows the government to collect vast amounts of data.[63] Specifically, CISA authorizes the government to collect information regarding "cybersecurity threats."[64] CISA defines these threats as:

> [A]n 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, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.[65]

This definition is broad and ambiguous. Some very benign activities meet the literal definition of a cybersecurity threat. Under this definition, for example, a parent attempting to access their child's YouTube account would be a "cybersecurity threat." Technically speaking, this would be an unauthorized effort to adversely impact the security of information stored on an information system.[66] In order to combat these "cybersecurity threats," CISA authorizes the collection of information that it defines as "cyber threat indicators" and "defensive measures."[67]

A "cyber threat indicator" is defined as "information that is necessary to describe or identify" one of the following:

> (A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;
>
> (B) a method of defeating a security control or exploitation of a security vulnerability;
>
> (C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

62. Russell Brandon, *Congress Snuck a Surveillance Bill into the Federal Budget Last Night*, VERGE (Dec. 16, 2015), http://www.theverge.com/2015/12/16/10288182/cisa-surveillance-cyber-security-budget-proposal.

63. *Id.*

64. CISA § 104

65. *Id.* § 102(5).

66. The CISA definition of "information system" is equally broad. CISA refers to the definition that is used in 44 U.S.C. § 3502. *See id.* § 102(9)(A). Section 3502 defines an "information system" 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) (2016).

67. CISA § 104(c).

> (D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
>
> (E) malicious cyber command and control;
>
> (F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;
>
> (G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or
>
> (H) any combination thereof.[68]

Like the definition of "cybersecurity threat," this definition is too broad to be meaningful. For instance, the DHS has acknowledged that a violation of a consumer service agreement[69] would technically qualify as a "cybersecurity threat."[70] Internet service providers generally require these agreements in order for customers to access many websites. Because a violation of one of these agreements is technically a "cybersecurity threat," the activity related to these violations could be considered a "cyber threat indicator."[71] The DHS dismisses this technicality by stating that activities that "solely" violate a consumer service agreement do not qualify as "cybersecurity threat[s]."[72] What the term "solely" means is not entirely clear. If a violation of a consumer agreement otherwise meets the definition of a "cybersecurity threat," how is it to be determined if that violation was "solely" a violation of the consumer agreement?

The definition of a "defensive measure" is equally broad. "Defensive measure[s]" are 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

68. *Id.* § 102(6)(A)-(H).

69. This would include Website Usage Agreements and the agreements that are typically required by Internet Service Providers.

70. On February 16, 2016, the DHS released guidance on what would constitute a "cybersecurity threat." In this guidance, DHS acknowledged that many terms included in consumer licensing agreements technically "satisfy the definition of a 'cybersecurity threat.'" DEPT. OF HOMELAND SECURITY, GUIDANCE TO ASSIST NON-FEDERAL ENTITIES TO SHARE CYBER THREAT INDICATORS AND DEFENSIVE MEASURES WITH FEDERAL ENTITIES UNDER THE CYBERSECURITY INFORMATION SHARING ACT OF 2015, at 4 n.6 (Feb. 16, 2016).

71. *See id.*

72. *Id.* ("Many terms of service agreements prohibit activities that satisfy the definition of a 'cybersecurity threat.' However, activities that are 'solely' violations of consumer agreements but do not otherwise meet the definition are not cybersecurity threats under CISA.")

system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability."[73] Boiled down, this definition becomes anything that detects, prevents, or mitigates a cyber threat, real or not. CISA authorizes private entities to operate defensive measures "for cybersecurity purposes."[74] Since CISA defines "cybersecurity purpose" as the "purpose of protecting an information system" or the information on an information system, it is unclear what specifically CISA is authorizing private entities to do.[75] Private entities can already deploy "defensive measures" that "detect, prevent or mitigate" "cybersecurity threats" on their own "information systems" for a "cybersecurity purpose."

The larger problem is that CISA authorizes the government to collect a huge amount of data without a warrant or probable cause.[76] In some cases, CISA allows the government to use that data for non-cybersecurity purposes.[77] Furthermore, because the definition of "cyber threat indicator" is so broad, a private entity could send the government nearly any piece of information. In addition, CISA gives the private entities that provide the government with information liability protection for providing that information.[78] Finally, the data that the government collects is immune from public records laws.[79]

This combination, the broad definition for what information can be provided, the liability protection for the providers, and the exemption from public records laws, allows the government to collect vast amounts of data that they would not otherwise be legally able to obtain. There is no public oversight since the government does not have to disclose what information they have collected.[80] This information could include an individual's private, personally identifiable information.[81] CISA only requires that

73. CISA § 102(7). The "known or suspected" language is also very broad. CISA does not set forth a standard to determine what constitutes valid suspicion.

74. *Id.* § 104(b).

75. *Id.* § 102(4).

76. CISA allows the government to use the information for purposes beyond cybersecurity. The information can also be used to prevent or mitigate specific threats of death, serious bodily injury, and serious economic harm, to protect minors, and for investigating and prosecuting certain crimes. *See id.* §105(d)(5)(A).

77. *See infra* Part III.B.

78. CISA provides liability protection to information providers so long as they provide information "in accordance with this title." CISA § 106(a)-(b).

79. The information that the government collects under CISA "shall be" "exempt from disclosure" and "withheld, without discretion, from the public." *Id.* § 105(d)(3)(A)-(B).

80. *Id.*

81. CISA only requires private entities to remove personal information if they "*know[] at the time of shari*ng" that the personal information is "not directly related to a cybersecurity threat." *Id.* § 104(d)(2) (emphasis added).

private entities filter personal information that *it knows, at the time the data is shared*, is not related to a cyber threat.[82] This provides little protection for an individual whose private information is shared with the government. How does that individual prove that the entity *knew*, at the time the entity provided the information, that the individual was not a threat? It is nearly impossible to *know* that someone is not a threat.

In addition, there is no requirement that private entities that provide the government with personal information correct that data if, after the fact, the entity determines that the information that they provided was incorrect.[83] Therefore, a private entity can provide the government with incorrect personal information and still retain its liability protection. So long as the entity did not *know* that the individual was not a threat when they provided the information, they are in compliance with CISA and would enjoy the liability protection that it provides.[84] The legislation states that "[n]o cause of action shall lie or be maintained in any court against any private entity . . . for the sharing or receipt of a cyber threat indicator or defensive measure" as long as the information is provided "in accordance with [CISA]."[85] Because of the immunity, there is no penalty for giving the government personal information, even if that information is incorrect. Therefore, a private entity could give the government incorrect personal information about an individual that could sit on a government server indefinitely. Further, that individual would not even know that information was there because there is no notification requirement included in CISA.[86]

B. RISKS REGARDING GOVERNMENT DATA USE

Once the government gets the information, it can use it for a host of purposes unrelated to cybersecurity.[87] It can be used by "any Federal agency or department, component, officer, employee, or agent of the Federal Government" in order to investigate and prosecute a host of

82. *See id.*

83. CISA requires the government to develop procedures for notifying "entities and Federal entities" when it knows that information it has received does not constitute a cyber threat indicator. This provision does not apply to the private entities that provide the government information. *Id.* § 105(b)(3)(E).

84. CISA does rescind the immunity in cases of gross negligence or willful conduct on the part of the provider. CISA § 106(c)(1).

85. *Id.* § 106(b), (b)(1).

86. CISA is immune from public records laws. Information shared with the government shall be "withheld, without discretion from the public." *Id.* § 105(d)(3)(B).

87. *See id.* § 105(d)(5)(A)(iii)-(v).

crimes.[88] Those crimes include fraud, identity theft, espionage, censorship, and threats related to minors.[89]

The information can also be used in order to prevent or mitigate "a *specific threat* of death, a *specific threat* of serious bodily harm, or a *specific threat* of serious economic harm."[90] The "specific threat" language is important. The Senate version of the bill only authorized the government to use the data when there was an "*imminent threat.*"[91] The use of the term "specific" rather than "imminent" authorizes the government to hold and use the information longer than it would otherwise have been able to.[92] An imminent threat means just that—imminent. Immediate action is required in order to address an imminent threat. A "specific threat," on the other hand, is different. A specific threat does not necessarily expire; it could conceivably last forever. Therefore, the government, including the NSA, can retain the information much longer under the "specific threat" standard than they could have under an "imminent threat" standard.

This change in standards is one reason that some privacy experts and some legislators are upset about the fact that CISA was tacked on to the budget bill and passed with no real debate.[93] The version passed by the Senate in October 2015 contained the "imminent threat" language.[94] However, the bill that ultimately became law in December changed the language to "specific."[95] Senator Ron Wyden (D-OR) both voted against the process with which CISA was passed and the bill itself.[96] After the bill's passage, a press release was issued regarding why Senator Wyden did not vote for it.

> Republican leaders inserted an extreme version of the Cybersecurity Information Sharing Act (CISA) and the flawed 2016 Intelligence Authorization Act into a broader package of spending and tax bills.

88. *Id.* § 105(d)(5)(A), (A)(ii)-(v).

89. *Id.* § 105(d)(5)(A)(iv)-(v).

90. *Id.* § 105(d)(5)(A)(iii) (emphases added).

91. Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. § 105(d)(5)(A)(iv) (as passed by Senate, Oct. 27, 2015) (emphasis added).

92. The removal of the imminence of harm requirement "opens the door for the FBI to pool the cyber threat indicators it receives under the legislation and repeatedly mine it to investigate activity unrelated to cybersecurity that may not even constitute a crime, and that does not pose any immediate threat. This makes the legislation seem as much a surveillance as a cybersecurity bill." Butler & Nojeim, *supra* note 91.

93. *See* Risen, *supra* note 2.

94. Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. § 105(d)(5)(A)(iv) (as passed by Senate, Oct. 27, 2015).

95. CISA § 105(d)(5)(A)(iii).

96. Press Release, *supra* note 58.

> "These unacceptable surveillance provisions are a black mark on a worthy package that contains the biggest tax cut for working families in decades, an accomplishment I fought for in weeks of negotiations," Wyden said.
>
> "Unfortunately, this misguided cyber legislation does little to protect Americans' security, and a great deal more to threaten our privacy than the flawed Senate version. Americans demand real solutions that will protect them from foreign hackers, not knee-jerk responses that allow companies to fork over huge amounts of their customers' private data with only cursory review.["][97]

This change is indicative of the inherent danger that comes with attaching a bill like CISA to a huge budget bill. The changed language essentially increased the government's authority to collect data and did so without Congressional debate.[98] CISA authorizes the government to use the information it collects for non-cybersecurity purposes, and it authorizes the government to keep that information for as long as it considers there to be a "specific threat."[99] The specific language authorizes "any Federal agency or department" to use the information for:

> (iii) the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or a use of a weapon of mass destruction;
>
> (iv) the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or
>
> (v) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a threat described in clause (iii) or any of the offenses listed in—
>
> > (I) sections 1028 through 1030 of title 18, United States Code (relating to fraud and identity theft);
> >
> > (II) chapter 37 of such title (relating to espionage and censorship); and
> >
> > (III) chapter 90 of such title (relating to protection of trade secrets).[100]

---

97. *Id.*
98. *Id.*
99. CISA § 105(d)(5)(A)(iii).
100. *Id.* § 105(d)(5)(A)(iii)-(v).

CISA is supposed to be a cybersecurity bill, but these are not cybersecurity purposes. Section §105(d)(5)(A)(v) allows the government to use the CISA information in order to *prosecute* the offenses.[101] In these cases, then, the government is using evidence that it acquired without a warrant or even probable cause.

This is an issue. The CISA data is shared with government agencies, including the NSA. In fact, CISA mandates that all of the information be shared with federal agencies in "real-time."[102] In order to save time and facilitate this "real-time" delivery, CISA mandates that the information not be modified prior to dissemination to the various agencies.[103] That means that there is no filtering mechanism to remove personal information or even correct erroneous information. This lack of control puts efforts to filter out personal information at risk and will likely result in government agencies, including the NSA, receiving unauthorized personal data.[104]

> CISA would significantly increase the National Security Agency's (NSA) access to personal information, and authorize the federal government to use that information for a myriad of purposes unrelated to cybersecurity. The revelations of the past two years concerning the intelligence community's abuses of surveillance authorities and the scope of its collection and use of individuals' information demonstrates the potential for government overreach, particularly when statutory language is broad or ambiguous. Notably, Congress has yet to enact reforms that would effectively rein in the government's activities.[105]

The lack of public oversight and the liability protection for private entities aggravate the issue. There is no way for an individual to determine if the NSA, or any other agency, has received or has used unauthorized information. Therefore, there is a significant risk that CISA will result in the unauthorized collection and use of the personal information of American citizens.

IV. CISA IS FLAWED

While the cybersecurity threat facing the nation is serious, CISA is not the answer to the problem. It is unclear how giving the government

---

101. *Id.* § 105(d)(5)(A)(v).

102. *Id.* § 105(a)(3)(A)(i)-(ii).

103. CISA prioritizes the speed of delivery over content control. It restricts actions that delay or impede the dissemination to the agencies. *Id.* § 105(a)(3)(A)(ii), (B)(ii).

104. Greene, *supra* note 28.

105. *Id.*

authorization to build another method for the collection of huge amounts of data would reduce the threat. The information that CISA authorizes the government to collect is too broad. There are too few controls on what information the government collects and on how it uses that information. In fact, CISA specifically authorizes the government to use the information for non-cybersecurity purposes. The information is collected without a warrant or probable cause, yet CISA authorizes the government to use that information in order to prosecute certain crimes. In the end, CISA is a flawed bill that looks more like a surveillance law than a cybersecurity bill.

V. CONCLUSION

The Cybersecurity Information Sharing Act was signed into law on December 18, 2015.[106] The law is an effort to combat cybersecurity threats by increasing information sharing between the private sector and the government.[107] The DHS is tasked with collecting the data and disseminating it to the other federal agencies, including the NSA.[108] The information flowing from the private entities to the government lacks the control required to ensure that there is no unauthorized collection of personal information. There are no effective controls to ensure that the information is not used for an unauthorized purpose, and the bill authorizes the information to be used for purposes not related to cybersecurity. In effect, CISA provides the government with the ability to conduct warrantless searches on the unauthorized personal information that it collects. CISA is simply not the answer to the cybersecurity threat facing the nation.

*John Heidenreich**

106. Risen, *supra* note 2.

107. S. REP. NO. 114-32, at 1 (2015).

108. CISA § 105(c).

* 2016 J.D. candidate at the University of North Dakota School of Law. I would like to thank my wife, Stacy, my parents, Jane and Warren, and my children, Tyler, Hannah, and Seth, for their continued support as I pursue my second career.