CREATING A "CIRCLE OF TRUST" TO FURTHER DIGITAL PRIVACY AND CYBERSECURITY GOALS

Jay P. Kesan[*] *& Carol M. Hayes*[**]

2014 MICH. ST. L. REV. 1475

ABSTRACT

Cyberattacks loom over the technological landscape as a dire threat to Internet commerce, information security, and even national security. Meaningfully improving cybersecurity and ensuring the resilience of systems will require cooperation between members of the private sector and the government. To this end, we propose a framework that creates a circle of trust for the sharing of information about threats and solutions. To emphasize the importance of cooperation to enhance cyber defense, this Article presents a case study of two items: the proposed legislative regime of the Cyber Intelligence Sharing and Protection Act, and President Obama's Executive Order 13,636 with its emphasis on a Cybersecurity Framework that would establish voluntary cybersecurity standards. Through application of our circle of trust framework, we hope to provide a solution that balances the sometimes competing concerns of privacy and cybersecurity.

Our secondary focus is whether such a program should emphasize voluntary or mandatory compliance. A proper balance between the two approaches could improve the dynamics between the public and private sectors in a way that increases respective levels of trust. The Executive Order and CISPA both use a voluntary approach. Under each system as currently proposed, firms could choose to follow the program, but compliance is not mandatory, and there is no penalty for noncompliance. However, mandatory programs with effective enforcement mechanisms are likely to result in higher levels of compliance than purely voluntary programs in many situations. We urge that government intervention in the free

* Jay P. Kesan, Ph.D., J.D., Professor and H. Ross & Helen Workman Research Scholar, University of Illinois College of Law.

** Carol M. Hayes, J.D., Research Associate, University of Illinois College of Law.

market should be kept at a low level, but because cybersecurity issues can have implications for national security, some degree of mandatory regulation would be beneficial.

We believe that cybersecurity can be enhanced without creating a Big Brother world and encourage the development of a circle of trust that brings the public and private sectors together to resolve cybersecurity threats more effectively. It is vital that these issues be addressed soon while there is still a chance to prevent a catastrophic cyber event. It would be ill-advised to rely solely on executive power or on legislation that is quickly drafted and enacted after an emergency. A careful, deliberative process aimed at protecting cybersecurity and civil liberties would ultimately be the most beneficial approach, and these steps must be taken now, before the emergence of a cybersecurity crisis that causes us to suspend reason.

TABLE OF CONTENTS

INTRODUCTION

"We shall meet in the place where there is no darkness." George Orwell, *1984*[1]

When cybersecurity efforts fail, the consequences can be expensive and dangerous. The Center for Strategic and International Studies estimates that every year, cybercrime and economic espionage cost the world economy anywhere from $375 billion to $575 billion, with the loss to the United States alone accounting for about $100 billion of that total.[2] A single breach of Target's systems, where hackers stole payment data for millions of the retail giant's

1. GEORGE ORWELL, 1984, at 25 (Signet Classic prtg. 1950) (internal quotation marks omitted).

2. CTR. FOR STRATEGIC & INT'L STUDIES, NET LOSSES: ESTIMATING THE GLOBAL COST OF CYBERCRIME: ECONOMIC IMPACT OF CYBERCRIME II, at 6, 8 (2014), *available at* http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf. The $100 billion total for the United States is based on data examining cybercrime as a percent of gross domestic product. For the United States, that percentage is 0.64%. *See* Tal Kopan, *Cybercrime Costs $575 Billion a Year, $100 Billion to US*, POLITICOPRO (June 10, 2014), http://www.politico.com/story/2014/06/cybercrime-yearly-costs-107601.html.

customers, resulted in financial losses exceeding $300 million.[3] In August 2014, a security firm discovered that a Russian crime ring stole 1.2 billion user name and password combinations from 420,000 websites in the largest known theft of Internet credentials to date.[4] The theft of this sort of information on a massive scale poses substantial financial danger to consumers who could become victims of identity theft.

Cybersecurity failures can cause much more than financial harm. The safety of individuals can also be threatened. Research has shown that it is possible to hack pacemakers and insulin pumps and cause them to malfunction, though thankfully there have not been any known attacks relating to this danger.[5] Cyber hostilities are also gaining a larger role in international conflicts in a way that can harm civilians. A cyberattack on government communication systems can make it difficult to inform civilians about threats to ensure that they can evacuate to safety when necessary.[6] Because civilian and government Internet infrastructure are so intermixed, cyberattacks aimed at a government are likely to also affect civilians.[7] For example, the primary target of the sophisticated and vicious Stuxnet

---

3. *See* Elizabeth A. Harris & Nicole Perlroth, *For Target, the Breach Numbers Grow*, N.Y. TIMES, Jan. 11, 2014, at B1; Rachel Abrams, *Target Puts Data Breach Costs at $148 Million, and Forecasts Profit Drop*, N.Y. TIMES, Aug. 6, 2014, at B3; *Banks Spent $172M on Reissuing Credit Cards Affected by Target Breach*, BANKING BUS. REV. (Feb. 10, 2014), http://cards.banking-business-review.com/news/us-banks-spend-172m-on-reissuing-credit-cards-affected-by-target-breach-100214-4174469. Target's Chief Financial Officer, John Mulligan, testified before the Senate Judiciary Committee on February 4, 2014, concerning the theft. *Target Executive Apologizes at U.S. Senate Hearing for Data Breach*, REUTERS (Feb. 4, 2014, 10:15 AM), http://www.reuters.com/article/2014/02/04/usa-hacking-congress-idUSL2N0L903Y20140204.

4. Nicole Perlroth & David Gelles, *Russian Hackers Steal Passwords of Billion Users*, N.Y. TIMES, Aug. 6, 2014, at A1.

5. Katherine Booth Wellington, *Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions*, 30 SANTA CLARA HIGH TECH. L.J. 139, 142 (2014).

6. This is similar to what happened during the conflict between Georgia and Russia in 2008. NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 174 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009).

7. Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533, 1535 (2010). Admiral Michael McConnell, the former Director of National Intelligence, estimated that networks and systems owned by civilians currently transport 98% of government communications. *Id.* at 1534.

worm was the systems of nuclear enrichment facilities in Iran, but a flaw in the code allowed the worm to infect thousands of other systems around the world.[8]

The cyber realm is a new battlefield, and vulnerabilities can create a tangible threat to national security. As tensions between Georgia and Russia erupted into violence in 2008, cyberattacks against Georgian government websites made it difficult for the government to communicate with its citizens about the conflict.[9] Malware and cyberattacks have also been used in the Syrian civil war, where the Syrian government uses malware to track rebel activity, and rebels and supporters also hack government systems.[10] Stuxnet, a fearsome cyber weapon that destroyed several nuclear centrifuges in Iran, was allegedly created by Israeli and American experts.[11] There is also evidence that the new Ukrainian government has been the target of cyberattacks, which may be related to the current tensions between Ukraine and Russia.[12]

Some economic studies of cybersecurity have found that there is underinvestment in security in part because many firms view cybersecurity as an externality.[13] With the Target data breach and the massive data theft by a Russian crime ring happening within nine months of each other, stronger protections are clearly necessary, and policy makers should intervene to address this serious failure of the private market. As cyber warfare becomes a more volatile threat to national security, policy makers should also consider how to promote the best cybersecurity research at the government level. Fostering cooperation between the private sector and the government could lead to improvements in cybersecurity for both sectors as they

---

8. Scott Neuman, *As the Worm Turns: Cybersecurity Expert Tracks Blowback from Stuxnet*, NPR (June 1, 2012, 4:15 PM), http://www.npr.org/blogs/thetwo-way/2012/06/01/154162121/as-the-worm-turns-cybersecurity-expert-tracks-blowback-from-stuxnet.

9. NAT'L RESEARCH COUNCIL OF THE NAT'L ACAD., *supra* note 6, at 174.

10. *In Syria, Conflict in Cyberspace Complements Ground War*, NPR (Dec. 31, 2013, 4:08 PM), http://www.npr.org/2013/12/31/258699442/in-syria-conflict-in-cyberspace-complements-ground-war; *see also* Margaret Coker & Jennifer Valentino-Devries, *U.S. Firm's Gear Seen Aiding Syria*, WALL ST. J., May 25-26, 2013, at A8 (discussing information discovered by hacker group Telecomix, which said in 2013 that it periodically probes Syrian telecommunications systems).

11. Ellen Nakashima & Joby Warrick, *Stuxnet Was Work of U.S. and Israeli Experts, Officials Say*, WASH. POST, June 3, 2012, at A1.

12. David E. Sanger, *N.S.A. Nominee Promotes Cyberwar Units*, N.Y. TIMES, Mar. 12, 2014, at A18.

13. Aaron J. Burstein, *Amending the ECPA to Enable a Culture of Cybersecurity Research*, 22 HARV. J.L. & TECH. 167, 176-77 (2008).

contribute to a shared compendium of cybersecurity knowledge. The public and private sectors both have a dire need for improved cybersecurity research, but there is currently a dearth of trust between the two.[14]

In the cybersecurity context, one of the primary contributors to this lack of trust is the fear of information insecurity. The government does not want classified cyber threat information to become widely known, just like the private sector does not want trade secrets or consumer information to become public knowledge. The private sector has become especially adamant about protecting online privacy from potential government overreach over the last few years. In January 2012, public backlash against federal copyright legislation called the Stop Online Piracy Act (SOPA) culminated in a protest blackout of several popular websites, including Reddit and the English language version of Wikipedia.[15] Opponents argued that SOPA posed a huge threat to Internet freedoms and would stifle the flow of information online.[16] Shortly thereafter, SOPA failed in the House,[17] and the Web heaved a collective sigh of relief.

Around the same time that the controversy over SOPA occurred, Congress was also proposing bills addressing cybersecurity issues. One of these, the Cyber Intelligence Sharing and Protection Act (CISPA), was introduced in the House in November 2011, and controversy surrounding the bill came to the public's attention in April 2012.[18] Organizations like the Electronic Frontier Foundation and the Center for Democracy and Technology came out against CISPA, criticizing its broad language.[19] Opposition to CISPA was found on both sides of the political aisle, from Republican Ron Paul

---

14. *See* Ellen Nakashima, *NSA Tries to Regain Industry's Trust to Work Cooperatively Against Cyber-Threats*, WASH. POST (Oct. 10, 2013), http://www.washingtonpost.com/world/national-security/nsa-tries-to-regain-industrys-trust-to-work-cooperatively-against-cyber-threats/2013/10/09/93015af0-2561-11e3-b3e9-d97fb087acd6_story.html.

15. Ned Potter, *Wikipedia Blackout: Websites Wikipedia, Reddit, Others Go Dark Wednesday to Protest SOPA, PIPA*, ABC NEWS (Jan. 17, 2012), http://abcnews.go.com/Technology/wikipedia-blackout-websites-wikipedia-reddit-dark-wednesday-protest/story?id=15373251#.T6v7wescPwA.

16. *See id.*

17. Stop Online Piracy Act, H.R. 3261, 112th Cong. (2011).

18. Declan McCullagh, *How CISPA Would Affect You (FAQ)*, CNET (Apr. 27, 2012, 4:00 AM), http://news.cnet.com/8301-31921_3-57422693-281/how-cispa-would-affect-you-faq/.

19. Cyrus Farivar, *CISPA Advances in House, as EFF Decries Bill's Revisions*, ARS TECHNICA (Apr. 26, 2012, 4:51 PM), http://arstechnica.com/tech-policy/2012/04/cispa-advances-in-house-as-eff-decries-bills-revisions/.

to the American Civil Liberties Union.[20] The Internet had recently triumphed over SOPA, but now some of the same corporate interests that opposed SOPA were *supporting* CISPA, and bloggers were incensed.[21] After several amendments, the House voted to pass CISPA on April 26, 2012, by a vote of 248 to 168.[22] This led to collective unease on the part of Internet privacy proponents, but CISPA spent the rest of the 112th Congress in the Senate Select Committee on Intelligence.

On February 13, 2013, CISPA was reintroduced in the House of the 113th Congress, in a version nearly identical to the version passed by the House in the 112th Congress except for a few cosmetic changes.[23] The day before CISPA's reintroduction, President Obama issued an executive order setting forth a proposed program to support the cybersecurity efforts of privately owned critical infrastructure.[24] The timing of these two actions indicated that the 113th Congress was likely to see a lot of cyber fireworks as the Republican House conflicted with the Democratic White House on this topic, in continuation of the previous term.[25]

However, the forward momentum for cybersecurity legislation seemed to grind to a halt after May 2013, perhaps because of the rapidly escalating controversy over government surveillance that

---

20. Michelle Richardson, *Opposition to CISPA Is Growing!*, AM. C.L. UNION (Apr. 24, 2012), https://www.aclu.org/blog/national-security-technology-and-liberty/opposition-cispa-growing.

21. *See, e.g.*, Violet Blue, *Google Helped with CISPA, Joins Cybersecurity Theatre*, ZDNET (Apr. 18, 2012, 9:15 PM), http://www.zdnet.com/blog/violetblue/google-helped-with-cispa-joins-cybersecurity-theatre/1238.

22. *See* Keith Perine & Jennifer Martinez, *House Passes CISPA Bill*, POLITICO (Apr. 27, 2012, 6:58 AM), http://www.politico.com/news/stories/0412/75670.html.

23. Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. (2013).

24. Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013).

25. During the 112th Congress, the Obama Administration had opposed CISPA, instead throwing its support behind the version of the Cybersecurity Act that was introduced in the Senate in July 2012. OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, STATEMENT OF ADMINISTRATION POLICY: H.R. 3523–CYBER INTELLIGENCE SHARING & PROTECTION ACT 1 (2012), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/sap/112/saphr3523r_20120425.pdf; OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, STATEMENT OF ADMINISTRATION POLICY: S. 3414–CYBERSECURITY ACT OF 2012 1 (2012), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/sap/112/saps3414s_20120726.pdf.

former contractor Edward Snowden brought to light.[26] The Snowden leak is a perfect illustration of the information security fears of both the government and private sector. The leak also deepens our conviction that it is essential to refocus efforts on finding a balance between cybersecurity and digital privacy and fostering trust between the two sectors. CISPA will likely continue to be central to this debate, since Rep. Dutch Ruppersberger (D-MD) introduced CISPA on the first day of the 114th Congress.[27]

In this Article, we will explore the importance of trust in the context of cybersecurity and privacy using a case study of CISPA, Executive Order 13,636 (the Order), and Presidential Policy Directive 21 (PPD-21). Both the market and the law have failed to keep up with the threat, and there is an urgent need for a new legislative paradigm that balances privacy and security without relying on an ad hoc approach to cybersecurity crises. To meet this goal, we propose a new "circle of trust" framework to encourage the creation of legislation that will foster cooperation and trust between the public and private sectors. The circle of trust represents our idea that the most pertinent information should be collected into a compendium of vital information that is shared with properly vetted agencies and firms. An essential part of this circle of trust framework is that the participants should not be compelled to share information beyond what is necessary. Under this framework, both the government and the private sector will still have the autonomy to refuse to share certain classes of information. We believe that a strong sense of information control will enhance privacy and support intersectoral trust. In the absence of intersectoral cooperation and trust, however, cybersecurity failures threaten to cripple modern society, making the adoption of this framework of the utmost importance.

In Part I, we present a new conceptual framework for information sharing that balances concerns of privacy and security in a way that we hope will increase the level of trust between the government and the private sector on cybersecurity issues. In Part II, we examine CISPA and modern privacy law in the United States. In Part III, we examine the issue of presidential authority and discuss the Order and PPD-21. In Part IV, we present our recommendations concerning the application of our proposed framework to legislation

26. *See infra* note 31 and accompanying text.

27. Cyber Intelligence Sharing and Protection Act, H.R. 234, 114th Cong. (2015).

and executive action, with additional emphasis on the hazards of relying on a purely voluntary approach.

I. A CONCEPTUAL FRAMEWORK FOR BALANCING PRIVACY AND SECURITY

Debates of legal policy often turn on a perceived dichotomy between conflicting interests. Internet policy is no exception. In the SOPA example above, the dichotomy is between the interests of property and privacy. SOPA's advocates emphasized the goal of protecting intellectual property rights online, while opponents were alarmed by the degree of invasion into private life that SOPA would authorize.[28] A framework for balancing property and privacy is outside the scope of this Article. Instead, we focus on the ongoing quest to strike a balance between privacy and security.

The idea of privacy in U.S. law became more pronounced around 1890, when Samuel Warren and Louis Brandeis published an article characterizing privacy as a "right to be let alone."[29] At its core, the article by Warren and Brandeis focused on the balance between privacy and the right of others to circulate information.[30] Privacy law has evolved over the last 125 years, with the issues becoming even more complicated in the last twenty years as the Internet grew in popularity. With this Article, we hope to provide a conceptual framework for evaluating information-sharing regimes with the goal of balancing privacy and security and fostering cooperation between the public and private sectors, and to this end we use CISPA and the Order as a case study.

Private information is held by both the private and public sectors, with each side keeping their respective private information secret from the other to the extent necessary and feasible. Private information held by the government may include classified information like sensitive military activities or ongoing government investigations. Private information held by private firms may include trade secrets, customer information, and projects under development. Whenever too much private information from either side is obtained without proper procedures being followed, controversies erupt.

---

28. *See supra* notes 15-16 and accompanying text.

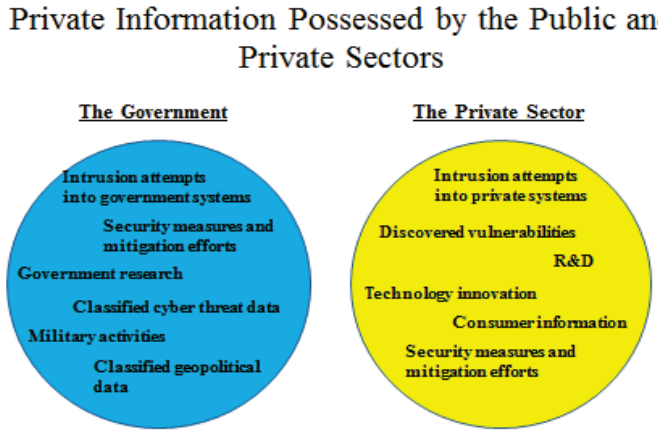
29. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

30. *See id.* at 195 (referring to the tension between the right to be let alone and the use of emerging technologies like "[i]nstantaneous photographs" to disseminate personal information).

In June 2013, former NSA contractor Edward Snowden leaked a large amount of information about previously undisclosed government surveillance activities undertaken for national security purposes.[31] The disclosures represent the unauthorized release of private information held by the government, and the surveillance activities themselves represent the collection of private information held by private citizens without their consent.

The conceptual framework that we encourage would consider the categories of private information held by both the government and the private sector, and the information-sharing program would be narrowly tailored to emphasize the categories of information that would be the most useful to the other side for improving cybersecurity, while excluding the categories of information that would put privacy or national security at risk. The following two figures are a visualization of the current status of open information sharing and the possible future of open information sharing under a regime like CISPA.[32]

FIGURE 1



31. Mirren Gidda, *Edward Snowden and the NSA Files–Timeline*, GUARDIAN (Aug. 21, 2013, 5:54 PM), http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline.

32. We use the term "open information sharing" here as a contrast to secretive government surveillance or the unauthorized release of sensitive data.

Figure 1 illustrates a few major examples of types of information that the different sectors might wish to keep secret.[33] By default, each side has exclusive access to their circle.[34] Some information in the left circle is accessible to the private sector, either because it is routinely shared or because it can be obtained under the Freedom of Information Act or similar statutory regimes. However, in the interest of national security, some types of information would routinely be withheld. For example, while an agency may be forthcoming about recent attempts to hack into its systems, it may be a bad idea to give too much information about the specific vulnerability that was exploited. A privately owned utility company might benefit from information about the vulnerability, but the current paradigm does not have an efficient mechanism for public-private cooperation in cyber threat information sharing.[35]

Information in the right circle could be accessible to the government through existing legal processes.[36] If the FBI were currently investigating a pattern of intrusions, it could likely meet the relevance standard to subpoena relevant information from several companies.[37] However, this is a very inefficient way of gathering the information because of informational asymmetry. The private companies know what information they have, while the government would have to ask. To remedy this informational asymmetry, one possibility is to encourage private firms to report intrusion attempts to law enforcement, but survey data from 2002 and 2004 indicate that only a minority of firms that experienced intrusions notified law enforcement.[38] The reluctance to share may be because revealing vulnerabilities could harm a company's reputation or make them into a more attractive target for hackers. This is a major reason why we

33. *See supra* Figure 1.

34. It should be noted that organizations within the circles may also keep their information secret from others within the same circle. Intrasectoral information transfer could be the subject of future analysis, but our primary focus with this Article is on intersectoral sharing.

35. The National Cybersecurity Communications and Integration Center of the Department of Homeland Security is authorized to facilitate information-sharing agreements for cybersecurity purposes under the National Cybersecurity Protection Act of 2014, but this authorization is too narrow to effectively support a circle of trust. P.L. 113-282 (2014); *see infra* text accompanying note 76.

36. *See supra* Figure 1.

37. To obtain a subpoena, the government must show that the information sought is relevant to an ongoing investigation. *See, e.g.*, Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored Email*, 2008 U. CHI. LEGAL F. 121, 128.

38. *See infra* notes 316-17 and accompanying text.

encourage an organized and largely anonymized system of disclosure for vulnerabilities and intrusions. Other information, like trade secrets, should be handled very carefully, with disclosure being strictly limited to government actors who could apply the information to improve the security of government systems.

Currently, the problem with cybersecurity information in the United States is that there are many information silos and little to no transparency between the holders of the information. To have a more effective approach to cyber defense, there should be a way to access the information held in the silos of the different institutional arenas. Information silos also exist for individual companies in the private sector on the topic of vulnerabilities and cybersecurity. While having segregated data collections may have advantages in some circumstances, we argue that it has too many disadvantages in the context of cybersecurity to permit this to continue as the status quo. Our "circle of trust" framework tries to address the disadvantages of siloed information.

When information flows from one silo to the other today, this may raise information-security concerns. This is particularly true when the information is flowing between the private and public sectors. Referring to Figure 1, when too much of the information goes from the right circle to the left circle, we might call it intrusive government surveillance.[39] When too much of the information goes from the left circle to the right circle, we might call it a security breach. Each side could benefit from some of the information in each circle. But how should we do that without overshare?

39. *See supra* Figure 1.

FIGURE 2

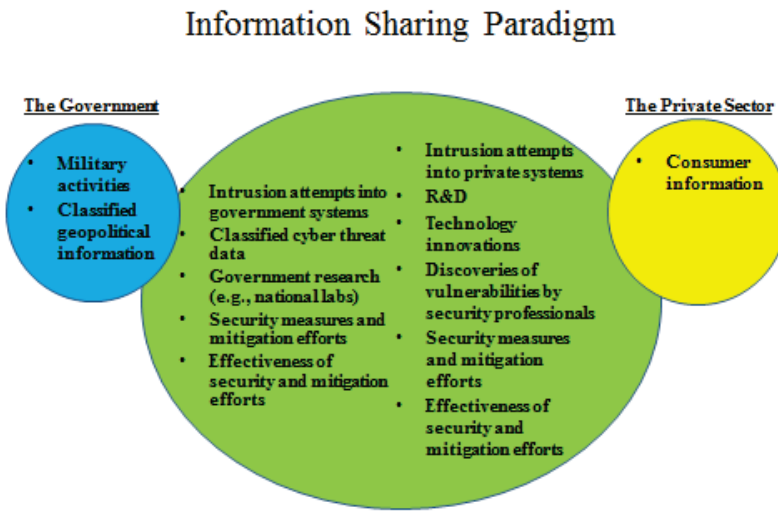


Figure 2 illustrates our conceptual framework for combining the right types of private information without overshare to create a circle of trust.[40] This is not an exhaustive list of categories for any of the circles, and the application of this framework should be analyzed very carefully. The shared information should be subject to stringent rules about secondary disclosures by the recipient, with stronger restrictions applying to more sensitive information. For example, private-sector recipients cannot disclose classified cyber threat data, and government recipients cannot disclose research information that is a trade secret.

Ultimately, our proposed framework is about cultivating trust between the private and public sectors, and in its current form, legislation will likely be necessary. The goal of this conceptual framework is to guide the creation of a legislative paradigm based on fostering trust between the private and public sectors. We characterize the middle circle of Figure 2 as representing a circle of trust.[41] We envision that the circle of trust will be managed by a trusted third party. When the public sector shares information with

40. *See supra* Figure 2.
41. *See supra* Figure 2.

the private sector, that encourages the private sector to trust the public sector and vice versa. Our proposed framework advances this notion of trust even further by keeping some information out of the central circle. Allowing both sides to preserve a degree of secrecy validates this circle of trust where public- and private-sector information intermingle, and assures participants that overreach by either side will be limited. This framework would capture the institutional advantages of the private and public sectors, provided that this legislative regime is crafted in such a way that the risks from developing the circle of trust are minimized.

As visualized in Figure 2, this conceptual framework would maintain government secrecy for classified military activities and geopolitical information, and would maintain private market secrecy for consumer information, including information about consumers' online activities.[42] In the middle oval, we have placed the types of information that we think could provide the clearest benefits to each sector when shared. Private cybersecurity researchers could benefit from information about intrusion attempts and details about vulnerabilities uncovered by government actors. Government agencies could benefit from up-to-date information about private cybersecurity innovations and the identification of vulnerabilities by private firms. Both sides could benefit from information about different security measures and their rate of success. Some existing laws would need to be revised to implement this proposal, such as the Electronic Communications Privacy Act, which currently may limit the ability of security researchers to share information between firms or with the government.[43]

This framework would not automatically give the general public access to lists of vulnerabilities in networks that were identified by government agencies. Instead, it would establish a circle of trust between the two sectors in order to support and improve the security of computers and networks, from Wall Street to 1600 Pennsylvania Avenue and everywhere in between. A vital part of this framework would be the vetting of information recipients. Both CISPA and the Order provide a mechanism for qualified members of the private sector to obtain security clearances so that

42. *See supra* Figure 2.

43. Burstein, *supra* note 13, at 170; Zhen Zhang, *Cybersecurity Policy for the Electricity Sector: The First Step to Protecting Our Critical Infrastructure from Cyber Threats*, 19 B.U. J. SCI. & TECH. L. 319, 335 (2013). Burstein states that "cybersecurity research currently faces a dearth of realistic, usable data to study modern-day threats." Burstein, *supra* note 13, at 172.

they can receive classified cybersecurity intelligence from the government.[44] Another essential part of our framework is that there must be limits on secondary disclosure and secondary use of shared information.

As trust grows between the public and private sectors, and as the limits on secondary use of cybersecurity information are established, adopting this framework could have a possible domino effect on the issue of surveillance. If an effective framework is accepted for balancing privacy and security, and there is adequate transparency in the program, warrantless surveillance programs could become unnecessary. With more structure and a lack of identifying data, any information that raises a red flag could be further investigated with search warrants and other manners of protective legal process. While the first step into an open information-sharing model may look like it could endanger privacy, the end result could be a system with increased transparency where warrantless "fishing expedition" surveillance is a thing of the past. The "place where there is no darkness" that is cryptically mentioned in Orwell's *1984* could be understood as a world without secrecy, where Big Brother sees all.[45] Our framework would support a "place where there is no darkness" in the sense of a segregated space of transparent relations between properly vetted representatives of government and the private sector. This place of transparency and light would promote the right balance between light within and shadow without to preserve both security and secrecy.

II. THE CYBER INTELLIGENCE SHARING AND PROTECTION ACT

The first part of our case study examines the proposed legislation known as CISPA, with our primary concern being whether the proposed regime lines up with our circle of trust framework for information sharing.

A. CISPA and Other Introduced Cybersecurity Legislation

CISPA was introduced by Rep. Mike Rogers in both the 112th Congress and the 113th Congress,[46] and by Rep. Dutch

44. *See supra* notes 23-24 and accompanying text.

45. ORWELL, *supra* note 1, at 25 (internal quotation marks omitted).

46. Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. (2013).

Ruppersberger in the 114th Congress.[47] In the 112th Congress, CISPA joined twenty other bills that focused on cybersecurity issues, none of which made it to the President's desk. Some of these bills touched on cybersecurity only tangentially, like the Broadband for First Responders Act of 2011, which would have required wireless public safety broadband networks to adopt appropriate cybersecurity measures.[48] Several focused on the need for research and development in cybersecurity areas,[49] on cybercrime,[50] or on the need for education and awareness.[51] Some would create a public-private partnership in the form of a formal organization to foster cooperation between the private sector and the government.[52] Many focused on the vulnerability of critical infrastructure.[53] Some of the bills also included amendments to the Federal Information Security Management Act of 2002,[54] which governs the information security practices of federal agencies. Several bills were of a fairly comprehensive nature, addressing many of the above issues.[55]

Two of the more comprehensive bills, the SECURE IT Act and the Cybersecurity Act of 2012, were each introduced at least twice during the 112th Congress. Compared to these bills, CISPA was relatively narrow, focusing on the information-gathering process. However, CISPA was a much hotter topic than any version of the Cybersecurity Act or the SECURE IT Act because CISPA would create a regime where private firms would be encouraged to voluntarily share cyber threat information with the government. Many people feared that information sharing under CISPA would

47. Cyber Intelligence Sharing and Protection Act, H.R. 234, 114th Cong. (2015).

48. Broadband for First Responders Act of 2011, H.R. 607, 112th Cong.; Broadband for First Responders Act of 2011, S. 1040, 112th Cong.

49. *E.g.*, PRECISE Act of 2011, H.R. 3674, 112th Cong.; SECURE IT Act, S. 2151, 112th Cong. (2012).

50. *E.g.*, Cyber Crime Protection Security Act, S. 2111, 112th Cong. (2012).

51. *E.g.*, Cyber Security Public Awareness Act of 2011, S. 813, 112th Cong.

52. *E.g.*, H.R. 3674 (proposing a "National Information Sharing Organization"); Cybersecurity Act of 2012, S. 3414, 112th Cong. (proposing the use of existing public-private partnerships, like the "Critical Infrastructure Partnership Advisory Council" and appropriate information sharing and analysis centers).

53. *E.g.*, Grid Cyber Security Act, S. 1342, 112th Cong. (2011); Homeland Security Cyber and Physical Infrastructure Protection Act of 2011, H.R. 174, 112th Cong.; Cybersecurity Act of 2012, S. 2105, 112th Cong.

54. *E.g.*, SECURE IT Act of 2012, H.R. 4263, 112th Cong.; S. 2105.

55. S. 2105; S. 3414.

include personal information and activity logs in a way that would "chill free speech" on the Internet.[56]

In the 113th Congress, CISPA again joined over twenty other bills that focused on cybersecurity. The SECURE IT Act appeared again, and the Cybersecurity Enhancement Act of 2014 was originally introduced, under a different name, in July 2013[57] and was placed on the Senate legislative calendar a year later, in July 2014. Cybersecurity bills introduced in the 113th Congress were somewhat narrower than the cybersecurity bills introduced in the 112th Congress. The Cyber Warrior Act of 2013 was an interesting bill, as it calls for the creation of "Cyber and Computer Network Incident Response Teams," to consist of National Guard members in each state and the District of Columbia.[58] Very similar versions of the Cyber Warrior Act were introduced in the House and Senate,[59] but neither bill was enacted.

In the 113th Congress, CISPA was joined by two other bills that focused on cyber threat information sharing[60] and two other bills that focused on critical infrastructure or particularly sensitive targets that are often under private control.[61] The Secure Chemical Facilities Act includes requirements concerning what the Secretary of Homeland Security must do with regard to security vulnerabilities uncovered at chemical facilities, including cybersecurity vulnerabilities.[62] Congress also introduced bills pertaining to data security and security breaches.[63] Some bills focused on cybersecurity funding and education, like the Cybersecurity Enhancement Act of 2013.[64] Several of the bills addressed the cybersecurity practices of

56. *Stop Online Spying Today*, SAVE THE INTERNET, http://act2.freepress.net/call/cispa_call/ (last visited Jan. 5, 2015).

57. Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 128 Stat. 2971.

58. Cyber Warrior Act of 2013, H.R. 1640, 113th Cong.

59. *Id.*; Cyber Warrior Act of 2013, S. 658, 113th Cong.

60. Cybersecurity Information Sharing Act of 2014, S. 2588, 113th Cong.; National Cybersecurity Protection Act of 2014, Pub. L. No. 113-282, 128 Stat. 3066.

61. National Cybersecurity and Critical Infrastructure Protection Act of 2013, H.R. 3696, 113th Cong.; Secure Chemical Facilities Act, S. 68, 113th Cong. (2013).

62. S. 68.

63. Cyber Privacy Fortification Act of 2013, H.R. 1121, 113th Cong.; Federal Agency Data Breach Notification Act of 2014, H.R. 4215, 113th Cong.

64. Cybersecurity Enhancement Act of 2013, H.R. 756, 113th Cong.

government agencies, but did not affect the private sector.[65] Cyber espionage from foreign actors was also the focus of several bills.[66]

As the above summary indicates, the 113th Congress introduced as many or more cybersecurity bills compared to the 112th Congress. However, by the midterm elections in 2014, only three of the cybersecurity-focused bills had been passed by the originating chamber: CISPA,[67] the Cybersecurity Enhancement Act of 2013,[68] and the National Cybersecurity and Critical Infrastructure Protection Act of 2014.[69] Two of the bills that passed in the House did so in April 2013, before the Snowden leak drew headlines. It was over a year after the Snowden leak before the House passed another cybersecurity bill, though several were introduced during that timeframe. The lack of progress on cybersecurity bills after the Snowden leak may have been due to a number of factors. Our theory is that because cybersecurity issues raise concerns about privacy, the Snowden leak and its ramifications for privacy made it less politically savvy to pursue cybersecurity.

After the midterm elections, however, the lame duck Congress had a few surprises up its sleeve.[70] For our purposes, three especially significant cybersecurity-related bills were passed in December of 2014 and signed by President Obama on December 18, 2014: 1) the Federal Information Security Modernization Act of 2014 (FISMA),[71]

---

65. Federal Information Security Modernization Act of 2014, Public L. No. 113-283, 128 Stat. 3078; H.R. 4500, 113th Cong. (2014) ("To improve the management of cyber and information technology ranges and facilities of the Department of Defense, and for other purposes."); DOD Cloud Security Act, H.R. 4505, 113th Cong. (2014); Veterans Information Security Improvement Act, H.R. 4370, 113th Cong. (2014); Executive Cyberspace Coordination Act of 2013, H.R. 3032, 113th Cong. FISMA was passed by Congress in December of 2014 and was signed into law by the President.

66. Deter Cyber Theft Act of 2014, S. 2384, 113th Cong.; Cyber Economic Espionage Accountability Act, H.R. 2281, 113th Cong. (2013); Deter Cyber Theft Act, S. 884, 113th Cong. (2013); Cyber Economic Espionage Accountability Act, S. 1111, 113th. Cong. (2013).

67. Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. (2013).

68. H.R. 756, 113th Cong. (2013) (as received in the Senate on April 17, 2013).

69. H.R. 3696, 113th Cong. (2014) (as received in the Senate on July 29, 2014).

70. For a review of recent congressional action on cybersecurity, see Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?* 38-45 (2015), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2548561.

71. Pub. L. No. 113-283, 128 Stat. 3073.

2) the National Cybersecurity Protection Act of 2014 (NCPA),[72] and 3) the Cybersecurity Enhancement Act of 2014 (CEA).[73] FISMA is an update to the older Federal Information Security Management Act, and focuses on the cybersecurity practices of federal agencies.[74] NCPA codifies the functions of the National Cybersecurity and Communications Integration Center (NCCIC) of the Department of Homeland Security (DHS).[75] Like CISPA, the NCPA approaches cybersecurity from an information-sharing perspective, though the NCPA takes a somewhat narrow approach, focusing on the newly formed National Cybersecurity and Communications Integration Center (NCCIC) of the Department of Homeland Security.[76] Finally, the CEA addresses a variety of topics like cybersecurity research and education, but for our purposes, its most significant contribution is Title I, which sets forth detailed guidance for the National Institute for Standards and Technology's activities relating to cybersecurity standards,[77] which we presume is intended as legislative oversight of the Cybersecurity Framework drafted pursuant to President Obama's Executive Order 13,636.

Meanwhile, the 114th Congress has been called into session, and CISPA is back, this time introduced by Rep. Dutch Ruppersberger (D-MD),[78] who supported the bill in the 112th and 113th sessions of Congress.[79] Devastating cyberattacks have landed in headlines more often over the last few years, and the clarion call for stronger cybersecurity has grown louder. The cybersecurity bills that were enacted into law in the eleventh hour of the 113th Congress were the first major legislative actions on cybersecurity in over a decade, but they leave many questions unanswered. Supporters of CISPA in the 114th Congress may be hoping that the third time is the charm for this legislation.

Joining CISPA in the 114th Congress is the Cyber Threat Sharing Act of 2015, a bill which is nearly identical to a legislative proposal offered by the White House in January.[80] This bill focuses

72. Pub. L. No. 113-282, 128 Stat. 3066.
73. Pub. L. No. 113-274, 128 Stat. 2971.
74. Pub. L. No. 113-283, 128 Stat. 3073; *see also* 44 U.S.C. § 3551 (2012).
75. Pub. L. No. 113-282, 128 Stat. 3066.
76. *Id.* at § 3.
77. Pub. L. No. 113-274, 128 Stat. 2971.
78. Cyber Intelligence Sharing and Protection Act, H.R. 234, 114th Cong (2015).
79. *See infra* note 182.
80. WHITE HOUSE, INFORMATION SHARING LEGISLATIVE PROPOSAL (2015), *available at*

on information sharing, and unlike most recent actions on cybersecurity, will allow for the private sector to voluntarily share "cyber threat indicators" with the federal government.[81] The term "cyber threat indicator" is given a fairly narrow definition, singling out methods and vulnerabilities and using language that emphasizes malice.[82] The White House explicitly states that the legislative proposal builds on important cybersecurity work in Congress, and the bill based on the proposal points to the CEA as a source of guidelines for developing mechanisms for the real-time sharing of cyber threat indicators.[83]

The NCPA and CEA have laid some of the legislative groundwork for strengthening cybersecurity and implementing Executive Order 13,636 and the Cybersecurity Framework, and the Cyber Threat Sharing Act of 2015 could potentially advance cybersecurity policy closer to our proposed circle of trust framework, though the latter bill would establish information-sharing within the NCCIC, rather than a trusted third party as we propose. But the legislative proposal enters a battlefield that is already filled with agendas and partisanship, and much can be learned by analyzing the progress of a similar information-sharing bill that has been raised in three separate congressional sessions. It is with this in mind that we present a case study of CISPA as an example of the politics and perceptions surrounding cybersecurity playing out on the national stage.

B. Text of CISPA

As written, CISPA would add § 1104 to the end of the National Security Act of 1947.[84] CISPA is described in the preamble as an act "[t]o provide for the sharing of certain cyber threat intelligence and

---

http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-information-sharing-legislative-proposal.pdf [hereinafter Information Sharing Legislative Proposal].

81. Cyber Threat Sharing Act of 2015, S. 456, 114th Cong.

82. *Id.* at § 2.

83. Press Release, Office of the Press Secretary, Securing Cyberspace—President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts (Jan. 13, 2015), [hereinafter Securing Cyberspace], *available at* http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace president-obama-announces-new-cybersecurity-legislat; Cyber Threat Sharing Act of 2015, S.456 § 2, 114th Cong.

84. H.R. 234, § 3. For the sake of clarity, textual references to § 3 of the bill will refer to the provision's placement in proposed § 1104.

cyber threat information between the intelligence community and cybersecurity entities, and for other purposes."[85] In the bill, "cyber threat intelligence" and "cyber threat information" have nearly identical definitions, except "cyber threat intelligence" is "intelligence in the possession of an element of the intelligence community" whereas "cyber threat information" does not contain a requirement for who is in possession.[86] Thus, it is "cyber threat intelligence" if it is held by a member of government intelligence operations, and "cyber threat information" if held by anyone else. In other words, the fundamental goal of CISPA is to put information from both sides into the center circle of trust that we depicted in Figure 2.[87]

The text of CISPA implies an awareness of the privacy-security balance. Proposed § 1104(c)(3) clarifies that there is no quid pro quo implied, in that if the government shares information with a private entity, the private entity does not thereby incur an obligation to share information with the government.[88] Proposed § 1104(f)(5) also includes language making it explicit that private entities will not be subject to any liability if they elect to not participate in voluntary actions pertaining to cyber threat information.[89] Using the terms of our theoretical framework, CISPA makes it explicit that the private sector is not required to move any information *into* the circle of trust.[90]

Under proposed § 1104(c)(1), once cyber threat information has been shared with the federal government, that information can be used "for cybersecurity purposes," to "investigat[e] and prosecut[e] . . . cybersecurity crimes" and "crimes involving . . . danger of death or serious bodily harm," to "protect[] . . . individuals from . . . danger of death or serious bodily harm," to protect national security, and to "protect[] . . . minors from . . . serious threats."[91] However, proposed § 1104(b)(2)(D)(iii) explicitly prohibits the government from using this information "for regulatory purposes."[92]

---

85. *Id.* pmbl.
86. *Id.* § 3.
87. *See supra* Figure 2.
88. H.R. 234, § 3.
89. *Id.*
90. The voluntary sharing of cyber threat information is also a focus of President Obama's legislative proposal that the White House announced in January 2015. Securing Cyberspace, *supra* note 80.
91. *Id.*
92. *Id.*

This places CISPA roughly in line with our proposal that there should be limits to secondary disclosure or secondary use of the information, though we would also encourage this sort of regime to place stricter limits on the secondary use and disclosure of more sensitive information.

There are a number of deficiencies in CISPA's current form that should be amended to make it more consistent with our circle of trust framework, and we make detailed suggestions to this effect in Section IV.B. The remainder of this Part places CISPA in context in a way that we hope will increase support for CISPA and similar legislation. First, we emphasize CISPA's place in the full global context of cybersecurity issues. Second, we examine how CISPA fits in the context of privacy law in the United States, with special emphasis on the voluntary disclosure provisions of the Stored Communications Act. Third, we place CISPA into its own context—that is, placing the controversial provisions of CISPA in the context of the more protective provisions of CISPA.

C. The Cybersecurity Context of CISPA

The threat that CISPA addresses goes far beyond hacker collectives like Anonymous and Lulzsec.[93] In the House Report, the legislators explicitly refer to the threats posed to domestic systems by cyber intrusions from foreign governments.[94] These concerns are not baseless paranoia, but are instead based on threats that have already been seen on the world stage. Hackers located in China have been blamed for cyberattacks on major U.S. news organizations like the *New York Times*, the *Washington Post*, and the *Wall Street Journal*.[95] In May 2014, the U.S. Department of Justice indicted five Chinese military hackers, making history as the first time that a state actor has been charged with hacking and related economic

93. *See* Carole Cadwalladr, *We Are Anonymous: Inside the Hacker World of Lulzsec, Anonymous and the Global Cyber Insurgency by Parmy Olson–Review*, GUARDIAN (Aug. 17, 2013), http://www.theguardian.com/technology/2013/aug/18/we-are-anonymous-parmy-olson-review.

94. H.R. REP. NO. 112-445, at 5 (2012) (noting that a review of a number of issues concluded that "a number of advanced nation-state actors are actively engaged in a series of wide-ranging, aggressive efforts to penetrate American computer systems and networks").

95. *See* Siobhan Gorman, Devlin Barrett & Danny Yadron, *Chinese Hackers Hit U.S. Media*, WALL ST. J. (Jan. 31, 2013, 8:28 PM), http://online.wsj.com/article/SB10001424127887323926104578276202952260718.html.

espionage.[96] The United States and Israel are alleged to have worked together to develop Stuxnet,[97] and it is fairly likely that more cyber weapons will emerge that can target industrial control systems. Some nations already have sections of their militaries devoted to cyber offense.[98]

Cyberattacks pose a danger to critical infrastructure like power grids and water treatment plants.[99] In 2007, researchers conducted a test at Idaho National Laboratories, commonly called the "Aurora Generator Test."[100] The Aurora Test revealed that it was possible for a hacker to use malicious commands to cause a power generator turbine to overheat and damage the equipment, showing the very real potential for a cyberattack to act like a physical attack.[101] Stuxnet demonstrated this in real space. One reason that Stuxnet was such an effective cyber weapon was because it caused the infected control system to make the centrifuges run at speeds well outside "their specified operating range," while also "disguis[ing] the disruption" so that it would not be noticed by system operators.[102] Before being discovered in the summer of 2010, Stuxnet had been operating for at least a year undetected, and during that time it is alleged to have destroyed hundreds of rotating centrifuges, in addition to causing severe damage to the rotating steam turbine at an Iranian nuclear power plant.[103]

---

96. Press Release, Dep't of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), *available at* http://www.justice.gov/opa/pr/2014/May/14-ag-528.html.

97. *The Meaning of Stuxnet*, ECONOMIST (Sept. 30, 2010), http://www.economist.com/node/17147862; *see also* Pam Benson, *Computer Virus Stuxnet a 'Game Changer,' DHS Official Tells Senate*, CNN (Nov. 18, 2010, 6:21 AM), http://www.cnn.com/2010/TECH/web/11/17/stuxnet.virus/index.html. Stuxnet is a sophisticated cyber weapon that was designed to exploit vulnerabilities in industrial control systems—specifically, systems used for processing uranium in Iranian nuclear facilities. *The Meaning of Stuxnet*, *supra*.

98. Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 457 (2012).

99. *See* Zhang, *supra* note 43, at 323.

100. CLAY WILSON, CONG. RESEARCH SERV., RL32114, BOTNETS, CYBERCRIME, AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 20 (2008).

101. *Id.*

102. Roland L. Trope & Stephen J. Humes, *Before Rolling Blackouts Begin: Briefing Boards on Cyber Attacks That Target and Degrade the Grid*, 40 WM. MITCHELL L. REV. 647, 675 (2014).

103. *Id.* at 675-76; *see also Iran Confirms Stuxnet Worm Halted Centrifuges*, CBSNEWS (Nov. 29, 2010, 3:19 PM), http://www.cbsnews.com/stories/

Cyber operations can take many forms and serve many purposes. Cyberattacks may be used to complement conventional war efforts. In 2008, cyberattacks against Georgian government websites coincided with armed conflict between Russia and Georgia, making it difficult for the Georgian government to communicate with the public about the conflict.[104] A second possible application of cyber threats is cyber espionage. Aggressive malware known as Snake has been found on computers in Ukraine and appears to have been targeting government agencies, stealing information, and allowing attackers to access the infected computer remotely.[105] Some cyber operations could be classified as weapons under international law because they cause physical damage to their targets. In 2010, the Stuxnet worm exploited four zero-day vulnerabilities to cause significant physical damage to centrifuges in Iran.[106] As many as one-fifth of Iran's centrifuges may have been destroyed,[107] though Iranian officials have previously stated that the damage was not as extensive as some have estimated.

While complementing conventional warfare sounds dangerous, and pervasive cyber espionage is alarming, the weaponization of cyber threats is the most disturbing development. After the news of Stuxnet's origin broke, experts in foreign policy and cyber conflict expressed unease about the beginning of a cyber "arms race."[108] This reference echoes the historical arms race of nuclear weapon development, but as a practical matter, cyber weapon research is likely to progress much faster than nuclear weapon research. Unlike a nuclear weapon, which leaves very few clues in the wake of its destruction, cyber weapons remain largely intact unless part of the

---

2010/11/29/world/main7100197.shtml; Nicole Perlroth, *Researchers Find Clues in Malware*, N.Y. TIMES (May 30, 2012), *available at* http://www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stuxnet-and-duqu.html?_r=0.

104. Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 4-5 (2009).

105. David E. Sanger & Steven Erlanger, *Suspicion Falls on Russia as 'Snake' Cyberattacks Target Ukraine's Government*, N.Y. TIMES (Mar. 8, 2014), http://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html?_r=1.

106. Jarred Shearer, *W32.Stuxnet*, SYMANTEC (Feb. 26, 2013, 7:15 PM), http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99. A zero-day vulnerability is a security flaw that was unknown to the vendor until it was exploited. *See id.*

107. Perlroth, *supra* note 103.

108. *E.g.*, Misha Glenny, *A Weapon We Can't Control*, N.Y. TIMES, June 25, 2012, at A19.

code is written to cause the program to self-destruct or stop working upon the fulfillment of a condition. For example, Stuxnet's expiration date was June 24, 2012, and no new infections could occur after that date.[109] However, there is still a good chance that the code can be analyzed. Even if the efforts in creating Stuxnet and similar cyber weapons were unique, by releasing Stuxnet and similar creations "into the wild," the creator makes these cyber weapons available for reverse engineering to allow third parties to recreate the effects.[110]

Stuxnet is publicly regarded as the first sophisticated cyber weapon that specifically targets industrial control systems.[111] These control systems are commonly referred to as Supervisory Control and Data Acquisition (SCADA) systems, and are typically used in the operation of critical infrastructure.[112] Stuxnet underscores the vulnerability of SCADA systems to cyberattacks and the importance of protecting these systems from attacks. It would not be an overstatement to say that threats against critical infrastructure are threats against national security. An attack that takes advantage of a vulnerability in the power grid could result in massive power outages.[113] If a water treatment facility is the target of a cyberattack, that attack could lead to untreated sewage being dumped in a public water supply.[114] Cyberattacks against transportation infrastructure could result in train collisions or even plane crashes.[115] These sorts of attacks could potentially be perpetrated from hundreds or thousands of miles away.

---

109. William Jackson, *Stuxnet Shut Down by Its Own Kill Switch*, GCN (June 26, 2012), http://gcn.com/Articles/2012/06/26/Stuxnet-demise-expiration-date.aspx.

110. *See* Ellen Nakashima, *U.S. Accelerating Cyberweapon Research*, WASH. POST (Mar. 18, 2012), *available at* http://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/2012/03/13/gIQAMRGVLS_story.html (noting the danger that a target could reverse engineer a cyber weapon).

111. Nicolas Falliere, *Stuxnet Introduces the First Known Rootkit for Industrial Control Systems*, SYMANTEC (Jan. 23, 2014, 6:25 PM), http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices.

112. Sklerov, *supra* note 104, at 19.

113. Brian Wingfield, *Power-Grid Cyber Attack Seen Leaving Millions in Dark for Months*, BLOOMBERG (Feb. 1, 2012), http://www.bloomberg.com/news/2012-02-01/cyber-attack-on-u-s-power-grid-seen-leaving-millions-in-dark-for-months.html.

114. Sklerov, *supra* note 104, at 20.

115. *Id.*

One can easily see why the government should be involved in protecting critical infrastructure, but a significant systemic issue stands in the way: Most critical infrastructure in the United States is owned and operated by members of the private sector.[116] This can make it difficult for government actors to share classified cyber threat information with the members of the private sector who would benefit the most. Addressing this difficulty by setting out procedures for the sharing of classified information with "utilities" is one of the most beneficial provisions of CISPA.[117]

We theorize that if the public were more informed about the threats posed by this new "cyber arms race" and legislation's potential role in protecting critical infrastructure, public opinion about legislation like CISPA might shift. We do not encourage the use of alarmist rhetoric to frighten citizens into supporting a bill that would restrict civil liberties, but at the same time, citizens should be informed about the possible threats so that an educated discourse can occur. In our view, it would facilitate this discourse to ensure that the public is informed about realistic threats in the cyber realm and about the current state of privacy law in the United States. Thus, it is to the privacy law context of CISPA that we now turn.

D. The Legal Context of CISPA

The most vocal criticisms of CISPA typically turned on the provisions that potentially allow private actors to share information about citizens with the government.[118] These provisions are what really set CISPA apart from recently enacted legislation like the NCPA.[119] CISPA would immunize these actors from legal liability if the actors had a good faith basis for identifying information as "cyber threat information" and sharing it with the government, as

116. Gus P. Coldebella & Brian M. White, *Foundational Questions Regarding the Federal Role in Cybersecurity*, 4 J. NAT'L SECURITY L. & POL'Y 233, 240 (2010) (estimating that 85% of CNI is owned by the private sector).

117. *See* Cyber Intelligence Sharing and Protection Act, H.R. 234, 114th Cong. § 3 (2015). Similar benefits are also provided by the newly enacted NCPA, though the NCPA's language uses the broader term "critical infrastructure." National Cybersecurity Protection Act of 2014, Pub. L. No. 113-282, § 7, 128 Stat. 3066, 3070.

118. McCullagh, *supra* note 18. President Obama's new legislative proposal also allows the private sector to share information about cyber threats with the government. Securing Cyberspace, *supra* note 80.

119. *See* text accompanying note 76.

permitted under that section.[120] In proposed § 1104(b), private entities are permitted to disclose information to the federal government "[n]otwithstanding any other provision of law."[121] The "notwithstanding" language is perhaps the most troubling provision of CISPA because it explicitly removes information shared under CISPA from the coverage of other laws aimed at protecting privacy. Critics of this voluntary sharing provision and the immunization from legal liability assert that it gives private companies a license to violate the privacy rights of consumers, free from any oversight of privacy law.[122]

The idea that CISPA explicitly removes this information from the purview of other privacy laws sounds worrisome on its face, but does it really make a substantial difference? If the "notwithstanding" language was not included in the final bill, what privacy laws would actually apply to the content covered by CISPA? There are two main potential sources: the Fourth Amendment to the Constitution, and statutes.

1. *The Fourth Amendment*

The Fourth Amendment protects persons from unreasonable government searches,[123] and compliance with the Fourth Amendment typically requires the government to get a warrant before obtaining evidence when there is a "reasonable expectation of privacy."[124] On June 25, 2014, the Supreme Court issued a decision in the case of *Riley v. California* concerning the "search incident" exception to the warrant requirement and its application to cell phone data.[125] In *Riley*, the Supreme Court made it very clear that data stored on a cell phone is protected by the Fourth Amendment, and that police cannot search an arrestee's cell phone as casually and informally as they might flip through a notepad found in an arrestee's pocket.[126] The Court essentially acknowledged in *Riley* that the expectation of privacy that necessitates a search warrant applies to cell phone data even when

120. H.R. 234, § 3.

121. *Id.*

122. *See* McCullagh, *supra* note 18 (quoting Rep. Jared Polis as saying that CISPA would "'waive every single privacy law ever enacted in the name of cybersecurity'").

123. U.S. CONST. amend. IV.

124. *See* Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

125. 134 S. Ct. 2473, 2480, 2482 (2014).

126. *Id.* at 2493.

the holder of the cell phone has been arrested. If police want to search through the potentially dozens of gigabytes of text, music, emails, and videos stored on an arrestee's cell phone, the *Riley* Court explicitly directs them to get a warrant.

Because it is limited to the search incident warrant exception and focuses on data stored on a device, the Fourth Amendment reasoning of *Riley* likely would not prevent legislation like CISPA from operating on the Internet where information is being transferred. Some may worry that CISPA allows the government to subvert the warrant requirement without relying on an established exception like search incident. However, there are two problems with applying the Fourth Amendment to information covered by CISPA: (1) the fact that sharing is voluntary, and (2) the potential application of the third-party doctrine. The first hurdle for Fourth Amendment protection is that voluntary sharing initiated by private companies, even when permitted by statute, is likely not considered a state action, and thus the information sharing would not implicate the Fourth Amendment.[127]

Even if information sharing under CISPA did potentially implicate the Fourth Amendment as state action, those protections only apply when a "reasonable expectation of privacy" exists. The Supreme Court has not yet conclusively addressed the issue of a reasonable expectation of privacy in data being moved across the Internet. *Riley* shows that when data is stored on a device like a cell phone, police cannot rely on the search incident warrant exception to search that device.[128] But does it violate your reasonable expectation of privacy if law enforcement obtains your information from a service provider? Under the third-party doctrine, there is no reasonable expectation of privacy in information disclosed to a third party if the government requests that information from the third-party recipient.[129] Many legal scholars worry that the third-party doctrine of Fourth Amendment jurisprudence may preclude any

127. *See* United States v. Richardson, 607 F.3d 357, 364 (4th Cir. 2010) (holding that an Internet Service Provider (ISP) was not a state actor with respect to the ISP's search that led to the discovery of child pornography that the ISP was then required by statute to disclose).

128. 134 S. Ct. at 2494-95.

129. Couch v. United States, 409 U.S. 322, 335-36 (1973) (finding no reasonable expectation of privacy in financial records turned over to an accountant for tax return purposes); United States v. Miller, 425 U.S. 435, 442-43 (1976) (finding no reasonable expectation of privacy in financial records disclosed to a financial institution in the ordinary course of business).

Fourth Amendment protection for information stored or transmitted online because third parties inherently must process information stored and transmitted over the Internet.[130]

Case law continues to develop on this point. In *United States v. Warshak*, the Sixth Circuit concluded that the third-party doctrine does not apply to an email service because that service is an intermediary of the communication instead of a recipient.[131] However, the content of terms-of-service agreements might eliminate a reasonable expectation of privacy if such agreement gives the service provider broad rights to monitor traffic.[132] Any protection that the Fourth Amendment provides to information covered by CISPA may therefore be reduced to the extent that service providers reserve the right to monitor traffic and activity on the service. Thus, even if CISPA's voluntary sharing provisions do not preclude the application of the Fourth Amendment, the third-party doctrine and the service provider's own privacy policy and terms of service may still reduce or eliminate a reasonable expectation of privacy in the information covered by CISPA.

The degree of protection offered to online communications under the Fourth Amendment is an open question, and it is unclear what the Supreme Court will conclude on this issue. In *United States v. Jones*, the Supreme Court considered whether actions by law enforcement in attaching a GPS device to a suspect's automobile violated the Fourth Amendment.[133] Because of the nature of GPS and the similarity of GPS technology to other Internet technologies, the *Jones* case could have had implications for the current debate about a reasonable expectation of privacy online. However, though the majority in *Jones* concluded that the placement of a GPS device on a car violated the Fourth Amendment, this conclusion was based on a

---

130. *E.g.*, Andrew William Bagley, *Don't Be Evil: The Fourth Amendment in the Age of Google, National Security, and Digital Papers and Effects*, 21 ALB. L.J. SCI. & TECH. 153, 173-74 (2011); David S. Barnhill, *Cloud Computing and Stored Communications: Another Look at* Quon v. Arch Wireless, 25 BERKELEY TECH. L.J. 621, 643 (2010). *But see* Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 634 (2011) (noting that some courts are moving away from a more aggressive third-party doctrine when interpreting the Fourth Amendment).

131. 631 F.3d 266, 288 (6th Cir. 2010).

132. *Id.* at 287; *see also In re* § 2703(d) Order, 787 F. Supp. 2d 430, 440 (E.D. Va. 2011) (finding no legitimate Fourth Amendment privacy interest in an IP address where Twitter's privacy policy states that Twitter will log users' IP addresses).

133. 132 S. Ct. 945, 948 (2012).

theory of trespass rather than on a reasonable expectation of privacy.[134] Similarly, in *City of Ontario v. Quon*, the Supreme Court *assumed*, but did not conclusively *determine*, that text messages obtained from a service provider would be protected by the Fourth Amendment.[135] During the oral arguments in *Quon*, Justice Roberts indicated confusion about how electronic messaging works, and expressed his initial thought that the Fourth Amendment would not apply if such messages were handled by a third party during transit.[136] The non-conclusory assumption of Fourth Amendment application to text messages held by a third party thus indicates that the Supreme Court recognizes the existence of a controversy, but is not yet willing to weigh in authoritatively on this point.

2. *Privacy Statutes and the Stored Communications Act*

If the Fourth Amendment does not apply, either because the information sharing is voluntary or because of the third-party doctrine, that would leave existing statutory regimes to fill in the gaps and protect online privacy when the Constitution cannot. This gap-filling purpose was one of the initial reasons for the enactment of the Stored Communications Act,[137] which we examine in more detail below.

Statutory privacy law in the United States is very sector-specific. The sharing of consumer credit information,[138] health information,[139] and video rental histories[140] are all regulated, but many other sectors are not restricted in how and when they can share consumer information. Proposed § 1104(c)(4) of CISPA identifies certain classes of "sensitive personal documents" that, if shared by the private sector under other provisions of CISPA, may not be used

134. *Id.* at 949.

135. City of Ontario, Cal. v. Quon, 560 U.S. 746, 760 (2010).

136. Transcript of Oral Argument at 48-50, *Quon*, 560 U.S. 746 (No. 08-1332), *available at* http://www.supremecourt.gov/oral_arguments/argument_transcripts/08-1332.pdf (exemplifying the confusion of Chief Justice Roberts and Justice Scalia as to how wireless communications are transmitted).

137. *See* Casey Perry, Recent Development, U.S. v. Warshak*: Will Fourth Amendment Protection Be Delivered to Your Inbox?*, 12 N.C. J.L. & TECH. 345, 349 (2011) (noting that the ECPA supplements the Fourth Amendment).

138. Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681t (2012).

139. 42 U.S.C. § 1320d-6 (2012) (addressing the "[w]rongful disclosure of individually identifiable health information").

140. 18 U.S.C. § 2710 (2012).

by the federal government.[141] This category includes information concerning library circulation, book sales, firearms sales, tax returns, education, and medical records.[142] This might mitigate some of the dangers inherent in circumventing sector-specific privacy laws, though arguably it does not go far enough since it only prohibits use by the federal government and does not address use by other private parties or by state or local governments. To improve this prohibition on use, the language should be amended to cover personally identifiable information and address use by parties other than the federal government. This is important in order to establish the circle of trust that we emphasize in our conceptual framework in Part I.

However, even as currently written, CISPA's effects on sector-specific privacy laws are likely to be fairly narrow because the laws themselves are narrow. The main statute of general applicability that applies to electronic communications is the Stored Communications Act of 1986 (SCA).[143] Thus, when CISPA opponents assert that CISPA allows companies to circumvent current privacy law, circumvention of the SCA is the broadest and most potentially problematic element.

The SCA was enacted as part of the Electronic Communications Privacy Act (ECPA). The SCA addresses the voluntary disclosure of electronic communications in § 2702 of Title 18 and the compelled disclosure of electronic communications in § 2703.[144] Because CISPA is explicit that the government cannot compel the production of cyber threat information from members of the private sector, § 2703 is not in issue.

a. Electronic Communication Services and Remote Computing Services

The SCA was enacted in 1986 and has not been substantially amended since then. The SCA still contains a fairly archaic distinction between electronic communication services (ECS) and remote computing services (RCS). Under the SCA, the definition for ECS is the same as under the Wiretap Act, where it is defined as "any service which provides to users thereof the ability to send or

141. Cyber Intelligence Sharing and Protection Act, H.R. 234, 114th Cong. § 3 (2015).
142. *Id.*
143. 18 U.S.C. §§ 2701-2712.
144. *Id.* §§ 2702-2703.

receive wire or electronic communications."[145] RCS is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."[146]

Both of these definitions have been unchanged since 1986, even though technology and business models have advanced significantly. The ECS provisions are generally viewed as applying to electronic messaging, especially email. In the mid-1980s, the transfer of email was fairly fragmented, with communications being transmitted from server to server, stored at various locations temporarily during the trip before being downloaded by the recipient.[147] Modern email is transmitted very differently, including through the use of the Internet Message Access Protocol (IMAP),[148] with many consumers accessing messages solely via webmail. The category of RCS was intended to address the business model where companies outsourced a lot of storage and processing functions due to the high cost of doing this in house.[149] More powerful, mobile, and accessible technologies have rendered this particular business model largely moot.

There is a lot of overlap between the concepts of ECS and RCS today because so many activities take place entirely online, including the sending and storage of email. This overlap is significant because the strength of protections under the SCA turns on the distinction between ECS and RCS. The difference between these two categories of services is especially important in the compelled disclosure provisions of § 2703 because the type of service determines the type of procedure required for the government to compel information. As noted above, however, CISPA's emphasis on voluntary disclosure prevents the provisions of § 2703 from applying. Thus, to the extent that opponents of CISPA warn that CISPA allows the government to obtain personal information without a warrant, a warrant would likely not be required under the SCA anyway because the disclosure is voluntary instead of compelled. In the absence of the "notwithstanding" language, therefore, the only provisions of the SCA that would apply would be the provisions of § 2702.

145. *Id.* § 2510(15).

146. *Id.* § 2711(2).

147. William Jeremy Robison, Note, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1205-06 (2010).

148. *See IMAP and POP*, U. MINN., http://it.umn.edu/imap-and-pop (last visited Jan. 5, 2015).

149. Robison, *supra* note 147, at 1206-07.

b. Disclosures and Exceptions Under § 2702

Under § 2702(a), communication contents held by an ECS provider cannot be disclosed to anyone unless an exception applies.[150] Communications carried or maintained by an RCS provider cannot be disclosed without an exception either, though the most common interpretation of § 2702(a)(2) is that the RCS provision requires carriage or maintenance to be "solely for the purpose of providing storage or computer processing services."[151] This qualification language for RCS providers was likely intended to address possible issues involving the third-party doctrine of the Fourth Amendment. This qualification has not aged well as technology has developed, given that it is a common practice for providers to reserve secondary use rights to customer data, such as for marketing purposes. Regardless of whether a service qualifies as ECS or RCS, non-content information, such as the identity of the sender or recipient of a message, cannot be shared with the government unless an exception applies.[152]

The requirement that RCS providers only have access to information for limited purposes will likely prove to be a thorny issue in the near future, especially for customers of companies that provide free services in exchange for permission to share customer information with third-party advertisers. If a service provider is not an ECS provider, but also cannot be an RCS provider because the provider has the authority to access customer information for other purposes, then 2702(a) would likely not prohibit that provider from voluntarily disclosing customer information to the government. In that situation, CISPA's "notwithstanding" provision would have no effect because the SCA would not apply anyway.

Whether a provider qualifies under the ECS or RCS terms is a very complicated issue that is the subject of disagreements between

150. 18 U.S.C. § 2702(a)(1).

151. *Id.* § 2702(a)(2)(B). An often overlooked part of § 2702(a)(2)(B) is the clause that follows the above quote, which reads "*if* the provider is not authorized the contents of any such communications for purposes of providing any services other than storage or computer process" (emphasis added). This implies that if the RCS provider is authorized to access communications for other purposes, § 2702(a)(2)(B) is inapplicable. However, for the purposes of this Section, we will accept the currently prevailing interpretation as expressed in *Flagg v. City of Detroit*, 252 F.R.D. 346, 358-59 (E.D. Mich. 2008).

152. *Id.* § 2710(a)(3), (b).

courts.[153] Although this is an open question, with eligibility as an RCS provider being especially thorny, we will assume for the sake of argument that any private company that shares information under CISPA would be bound by the terms of the SCA in the absence of the "notwithstanding" language of proposed § 1104(b). Thus, for these companies to share information on a voluntary basis, an exception under § 2702(b) would need to apply. The most relevant exceptions for voluntary disclosure are when lawful consent is obtained from qualified parties, when disclosure is made to law enforcement after the service provider "inadvertently obtained" communication contents pertaining to the commission of a crime, and when disclosure is required because of an emergency.[154]

The privacy policies of most services on the Internet reserve to the company a right to disclose information to the government. Depending on the wording of provisions like this, one might argue that the company has obtained the lawful consent to disclose information when the consumer consents to the privacy policy. However, this exception is largely inapplicable because most of these provisions include language about the disclosure being in response to lawful requests, and sharing under CISPA would be voluntary and not likely to be accompanied by a request that can compel disclosure. The exception for communications "inadvertently obtained" might permit CISPA disclosures by a service provider that discovered a system compromise while conducting maintenance, but this category of disclosures is likely to be fairly narrow in terms of its effects on privacy.[155]

The emergency exception, on the other hand, is much broader. Under the emergency exception of the SCA, a provider with a good faith belief that there is "an emergency involving danger of death or serious physical injury to any person" may disclose to a governmental entity communications relating to the emergency.[156] This emergency exception was added in 2001 as part of the USA

153. *Compare* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 902 (9th Cir. 2008) (holding that an archive of text messages was for backup protection purposes and thus the service was an ECS), *rev'd*, City of Ontario, Cal. v. Quon, 560 U.S. 746 (2010), *with* Flagg *ex rel.* Bond v. City of Detroit, 252 F.R.D. 346, 363 (E.D. Mich. 2008) (holding that an archive of text messages was for storage purposes and thus the service was an RCS).

154. 18 U.S.C. § 2702(b)(3), (7), (8).

155. *See id.* § 2702(b)(7).

156. *Id.* § 2702(b)(8).

PATRIOT Act[157] and was amended to its current form by the Homeland Security Act of 2002.[158] Congress likely recognized in passing this amendment to the SCA that emergency disclosure provisions can be exploited. This awareness is reflected in the inclusion of reporting requirements. In § 2702(d), Congress requires the Attorney General to submit an annual report to Congress listing the number of instances of emergency disclosures under that section and also requires this report to summarize the basis for disclosure in instances where investigations relating to the voluntary disclosure did not result in criminal charges being filed.[159]

The fact that the emergency exception was initially introduced with the USA PATRIOT Act should raise a few civil libertarian eyebrows, especially considering how broad it is in its current form. For instance, with the current language of the emergency exception of § 2702, a provider need only have a good faith belief that an emergency exists.[160] There is also no time-related language in this emergency exception, such as requirements that the threat of physical harm be "imminent." The emergency disclosure exception is an example of security being given more weight than privacy in the ongoing back-and-forth quest for a balance between privacy and security. Relying on an emergency exception would be undesirable in our circle of trust framework, which we believe should be established and practiced before an emergency so that it will work more efficiently and with stronger privacy guidelines when an emergency occurs.

---

157. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 212, 115 Stat. 272, 284.

158. Homeland Security Act of 2002, Pub. L. No. 107-296, § 225(d)(1)(D), 116 Stat. 2135, 2157 (codified as amended at 18 U.S.C. § 2702(b) (2012)). The language in the PATRIOT Act permitted a provider to disclose information in the event of an emergency if the provider "reasonably believes" that there is such an emergency, § 212, 115 Stat. at 285, whereas the language in the Homeland Security Act of 2002 required only a "good faith" belief that such an emergency exists, § 225(d)(1)(D), 116 Stat. at 2157.

159. 18 U.S.C. § 2702(d).

160. *Id.* § 2702(b)(8).

c. Applying the SCA to CISPA

CISPA's opponents generally cite concerns about civil liberties when opposing the voluntary disclosure language of CISPA,[161] but they do not acknowledge that there is statutory precedent for these provisions. We argue that those concerned with CISPA and civil liberties should focus on this underlying statute. There are at least three reasons to view CISPA as either an extension of or at least closely related to the emergency disclosures exception of the SCA: (1) the potential harms that could flow from cyberattacks, which both seek to address; (2) the similar "good faith" provisions in the two; and (3) the presence in both of annual reporting requirements. Taken together, these features suggest that analyzing CISPA separately from the SCA paints an incomplete picture of the dominant policy approach to cybersecurity.

First, we noted above that cybersecurity threats pose substantial dangers to *people*, not just their computers, especially if the attacks are on critical infrastructure. Thus, it would not be an unreasonable extension of the emergency-disclosures exception to view this exception in the SCA as covering cyber threats against critical infrastructure. CISPA itself contains explicit terms allowing the government to use cyber threat information to protect individuals from "the danger of death or serious bodily harm" in proposed § 1104(c)(1)(C).[162] This provision addressing proper use of cyber threat information thus echoes the emergency disclosure exception under the SCA.[163]

Second, in proposed § 1104(b)(3), entities that share information with the government under CISPA are exempted from liability if they act in good faith in identifying, obtaining, and disclosing cyber threat information.[164] This good faith liability exemption parallels the good faith belief language of the emergency exception in § 2702(b)(8) of the SCA.

Third, like the emergency disclosure reporting requirement under § 2702(d) of the SCA, CISPA also includes an annual

161. *See, e.g.*, Michelle Richardson, *CISPA Remains Fatally Flawed After Secret Committee Markup*, ACLU (Apr. 12, 2013, 12:20 PM), https://www.aclu.org/blog/technology-and-liberty-national-security-free-speech/cispa-remains-fatally-flawed-after-secret.

162. Cyber Intelligence Sharing and Protection Act, H.R. 234, 114th Cong. § 3 (2015).

163. *See* 18 U.S.C. § 2702(b)(8).

164. H.R. 234, § 3.

reporting requirement to keep Congress informed of the type and use of voluntary disclosures and control possible abuse of the system.[165] The reports must include, among other things, "appropriate metrics to determine the impact of the sharing of such information with the Federal Government on privacy and civil liberties."[166]

The strongest argument against CISPA, that is, the broad permission it gives for private entities to disclose consumer information notwithstanding other provisions of law, is thus overstated. This argument assumes that if modern privacy law *did* apply, it would limit CISPA's reach. This argument largely ignores two things: (1) the ambiguity of the application of the Fourth Amendment to information subject to disclosure under CISPA; and (2) the strong parallels between the voluntary disclosure provisions of CISPA and the emergency disclosure exception of the SCA.

The House Report of CISPA during the 112th Congress does not mention the SCA, indicating that the House members drafting it may have given inadequate consideration to CISPA's relationship with the SCA.[167] During the floor debate before the House, Rep. Jerrold Nadler (D-NY) expressed his concerns that CISPA's voluntary sharing provisions supersede "the Electronic Communications Privacy Act (ECPA) and the Wiretap Act."[168] However, this concern was not addressed in a rebuttal.

In our proposal, we suggest striking the "notwithstanding" language that precludes application of existing privacy law, but we also suggest amending CISPA to contain explicit references to § 2702 of the SCA if the voluntary sharing provisions are retained. Keeping CISPA isolated in the National Security Act of 1947 will continue to make it difficult to see the overlap between CISPA and the SCA at first glance. To clarify the relationship between cybersecurity laws and privacy laws, CISPA would ideally include a provision to amend the SCA and thus more clearly address the

---

165. *Id.* § 2(c)(1).

166. *Id.* § 2(c)(1)(D).

167. *See* H.R. REP. NO. 112-445 (2012). The April 17 report does not mention the SCA or the Electronic Communications Privacy Act by name, nor does it mention 18 U.S.C. § 2702. *See id.*

168. 158 CONG. REC. H2165 (daily ed. Apr. 26, 2012) (statement of Rep. Nadler). Congressman Nadler likely meant to refer to the Stored Communications Act, which was enacted along with the Wiretap Act as part of the Electronic Communications Privacy Act, because otherwise, referring to ECPA and the Wiretap Act separately would not make sense. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208 (2004).

relationship between voluntary "cyber threat information" disclosures under CISPA and emergency disclosures under the SCA. However, the new language that we propose in this Article is primarily limited to the text of CISPA. Amending the SCA should nonetheless be the subject of future study.

The civil libertarians who oppose CISPA because of perceived threats to individual privacy are not necessarily mistaken about the existence of these threats. The mistake is in asserting that CISPA "'waive[s] every single privacy law ever enacted in the name of cybersecurity.'"[169] This assertion relies on an incomplete narrative about the degree to which modern information privacy law protects online privacy. Essentially, it assumes that existing Internet privacy law is much more protective of individual privacy than it really is.

The efforts of civil libertarians would be better focused on reversing or limiting the underlying statutory precedent found in the emergency exception of the SCA. By pointing to a problem that is actually rooted elsewhere, and rejecting CISPA based on a misunderstanding of federal privacy law, opponents may succeed in preventing the enactment of a law with several valuable and novel elements. CISPA's valuable contributions include the creation of procedures for granting security clearances to private-sector actors for cybersecurity purposes and also the provisions aimed at protecting civil liberties.[170]

E. Protections for Civil Liberties Within CISPA

The fact that CISPA permits voluntary sharing "[n]otwithstanding any other provision of law"[171] rightly causes opponents to be concerned, but even without that provision, it is doubtful that current privacy law would make much difference in CISPA's execution. Above, we noted that cyber threats can pose physical dangers and argued that these physical dangers could put

169. McCullagh, *supra* note 18 (quoting 158 CONG. REC. H2148 (daily ed. Apr. 26, 2012) (statement of Rep. Polis)).

170. Other cybersecurity bills have also had some of these strengths, though we ultimately focused on CISPA because of the bill's surprising resilience in three separate congressional sessions. The recently enacted NCPA also includes procedures for security clearances in § 7, but the language only singles out members of public-private partnerships and owners and operators of critical infrastructure for eligibility. National Cybersecurity Protection Act of 2014, Pub. L. No. 113-282, § 7, 128 Stat. 3066, 3070. The deficiencies of the security clearance language in the NCPA are addressed in Subsection IV.B.1.

171. H.R. 234, § 3.

CISPA in line with the existing emergency disclosure exception of the SCA. Even if these positions are not accepted, CISPA still imposes a number of requirements on government actors to protect consumers from abuse of the voluntary sharing provisions. These protections, by addressing the need to protect against abuse of CISPA, help to mitigate some of the potential harm to civil liberties that the "notwithstanding" language might cause. These efforts to protect civil liberties help to bring CISPA closer to an implementation of our circle of trust framework.

CISPA includes three important types of provisions to protect privacy and civil liberties. First, CISPA imposes a number of restrictions on government use of cyber threat information in proposed § 1104(b) and 1104(c).[172] Second, CISPA includes an annual reporting requirement to keep Congress informed of the use of voluntarily disclosed information, so that there will be congressional oversight of related privacy issues.[173] Third, CISPA includes a sunset provision that will allow the law to expire five years after enactment.[174] Because the reporting requirement is discussed above, and the sunset provision is largely self-explanatory, the remainder of this section will examine the restrictions on government use in more detail.

Restrictions on government use of information are found in proposed § 1104(b)(2) and 1104(c). Proposed § 1104(b)(2) addresses the use and protection of information.[175] For example, information disclosed to the federal government under CISPA would be exempted from disclosure under Freedom of Information Act requests and other statutes that require government entities to publicly disclose information. The federal government is also prohibited from using that information for "regulatory purposes."[176] This section also requires the government to anonymize or minimize private-sector information, as appropriate, before the government may share this information further.

Proposed § 1104(c) contains additional restrictions on government use of cyber threat information. Affirmative government searches of shared information are limited by proposed §§ 1104(c)(1) and (2) to the purpose of investigating and prosecuting cybersecurity

172. *Id.*
173. *Id.* § 2(c).
174. *Id.* § 4.
175. *Id.* § 3.
176. *Id.*

crimes.[177] Proposed § 1104(c)(3) prohibits the government from requiring private entities to share information, or from conditioning cyber threat sharing by the government on reciprocal sharing by the private sector. The government is also required under proposed § 1104(c)(4) to refrain from using certain types of personal information. For example, the government cannot use information derived from library circulation records, book sale records, medical records, or records of firearms sales.[178]

If the government violates any of the restrictions on government use of cyber threat information, proposed § 1104(d) creates a private cause of action against the government, where the aggrieved parties can obtain damages, court costs, and reasonable attorney fees. This private cause of action ensures that government violations of the terms of CISPA can be redressed.

This is not to say that the protections are perfect. A number of aspects of the protections should be amended to more effectively protect citizens. For example, the civil liability provision applies only to intentional or willful violations by the government, not negligent violations.[179] In 2012, Rep. Jerrold Nadler (D-NY) also expressed concern during the floor debates that the two-year statute of limitations for bringing a suit is "unworkable, unfair, and unrealistic."[180]

We also take issue with the terms "regulatory purposes" and "[a]ffirmative search," neither of which are defined.[181] During the floor debates in the 112th Congress, Rep. Dutch Ruppersberger (D-MD) provides some context for "regulatory purposes," stating that the government would be prohibited from using disclosed information as part of a criminal proceeding if the information provides "evidence of tax evasion."[182] However, this does not set firm limits on what would be considered a prohibited "regulatory purpose." Future amendments to CISPA or future legislation that uses these terms should clarify what these terms mean.

The reporting requirement of CISPA should also be revised to better resemble the reporting requirement of the Order. In the Order,

177. *Id.*
178. *Id.*
179. *Id.*
180. 158 CONG. REC. H2165 (daily ed. Apr. 26, 2012) (statement of Rep. Nadler).
181. H.R. 234, § 3.
182. 158 CONG. REC. H2163 (daily ed. Apr. 26, 2012) (statement of Rep. Ruppersberger).

the report concerning privacy and civil liberties must recommend ways to "minimize or mitigate" risks to these interests.[183] In contrast, reports about information sharing under CISPA must include "appropriate metrics to determine the impact of the sharing . . . on privacy and civil liberties."[184] There is a significant difference between requiring a report to address actual minimization and mitigation of threats and requiring a report to provide metrics to determine the extent to which sharing harms privacy and civil liberties. Accordingly, we recommend the amendment of CISPA to bring its reporting requirement more in line with the reporting requirement of the Order.

As the above sections show, CISPA is a complicated piece of legislation that the public and legislators alike tend to either support or oppose vehemently. It is also a very important piece of legislation that addresses a serious threat. The threat that CISPA addresses is sometimes underestimated, even though cyber threats have the potential to do real world damage. The strength of privacy protections in the legislative context surrounding CISPA, on the other hand, is sometimes overestimated. CISPA's ambivalent approach to privacy, while seemingly worrisome on its face, is ultimately consistent with how online privacy is currently treated in the law. Moreover, CISPA is largely consistent with our circle of trust framework, in that it addresses the movement of information from the public and private sectors into a space of shared information, and also addresses secondary usage of that information. For an alternative model for balancing security and privacy, we now turn to the question of presidential authority and the Order.

III. CYBERSECURITY, THE ORDER, AND PRESIDENTIAL AUTHORITY

One major difference between CISPA and the Order is the direction of information flow. CISPA focuses on the movement of cyber threat information into the circle of trust from both the private and public sectors. As written, the Order would only permit the government to insert cyber threat information into the circle of trust. Government researchers might benefit from this arrangement insofar as it could result in agencies being more informed about what other agencies know, but the primary beneficiary would be the private

183. Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13,636, § 5(b), 78 Fed. Reg. 11,739, 11,740 (Feb. 12, 2013).

184. H.R. 234, § 2(c)(1)(D).

sector, and the government actors would still not have access to cyber threat information held by the private sector.

The Order also ensures that information about recommended security practices is readily available through the Cybersecurity Framework. By providing a voluntary cybersecurity standard, the Cybersecurity Framework thus facilitates the sharing of information about security measures between the government and the private sector.[185] Additionally, adopters of the Cybersecurity Framework must have their implementation evaluated for compliance with the standard. The Cybersecurity Framework thus also represents a different kind of information being shared within the circle of trust. Through the Cybersecurity Framework, the government will share recommendations for cybersecurity practices, and the adopters will share information about their implementation of the Cybersecurity Framework so that both the government and the private sector can evaluate the success of the program. Now that Congress has enacted the Cybersecurity Enhancement Act of 2014, the National Institute for Standards and Technology (NIST) has formal congressional authorization to establish voluntary cybersecurity standards. Some questions, however, still remain about the scope of the President's power and his authority to direct action on cybersecurity.

Under the Constitution of the United States, the judicial, legislative, and executive branches of the government are each empowered to address controversies in different ways. Article III courts address live controversies through *ex post* adjudication.[186] Congress enacts bills using the bicameral legislative process, but is explicitly prohibited from enacting ex post facto legislation.[187] The judiciary is thus inherently backward-looking, while the legislature is inherently forward-looking. Under Article II, the executive branch is imbued with the authority to execute existing laws, with the President having some additional limited authority as the Commander-in-Chief of the nation's military.[188]

Because of the inherently *ex post* nature of judicial resolution, the role of Article III courts in protecting the nation's cyber infrastructure is minimal. It is fairly clear that Congress has authority to regulate interstate cybersecurity matters. Congress has also

185. Exec. Order No. 13,636, § 7, 78 Fed. Reg. at 11,739-40.

186. *See* Erwin Chemerinsky, *A Unified Approach to Justiciability*, 22 CONN. L. REV. 677, 677-78 (1990) (providing an introduction to modern justiciability doctrines).

187. U.S. CONST. art. I, § 9, cl. 3.

188. U.S. CONST. art. II, § 2, cl. 1.

already addressed the idea of the federal government assisting private owners of critical infrastructure via the Homeland Security Act[189] and the recent enactment of the NCPA.[190] Notwithstanding the enactment of several cybersecurity bills in the waning hours of the 113th Congress, congressional action on cybersecurity has been slow, which has led some to ask about the extent to which the President might have authority to act on these issues. Because the Order emphasizes the creation of cybersecurity standards, a major focus of this Part is on presidential authority to require the adoption of technology. Although the Cybersecurity Framework is proposed as a voluntary cybersecurity standard, and the CEA focuses extensively on the voluntary nature of the standard, it is worthwhile to also consider the possible legality of a mandatory cybersecurity standard.

A. Presidential Authority

Article II of the United States Constitution vests the executive power in the President, who is also designated the Commander-in-Chief of the nation's armed forces.[191] Constitutional law scholars often discuss the idea of presidential power under Article II, the authorities granted by various clauses, and the possibility that the President might possess certain inherent presidential powers.[192] Aside from the clause in Article II making the President the Commander-in-Chief of the armed forces, another potential source of presidential power under the Constitution is the first sentence of Article II, which states that there is an "executive Power" that is "vested in a President."[193] Proponents of the Vesting Clause theory have argued that the Vesting Clause creates a category of actions that are within

189. Homeland Security Act of 2002, Pub. L. No. 107-296, § 223, 116 Stat. 2135, 2156 (codified as amended in 6 U.S.C. § 143 (2012)).

190. National Cybersecurity Protection Act of 2014, Pub. L. No. 113-282, 128 Stat. 3066.

191. U.S. CONST. art. II, § 2, cl. 1.

192. *See, e.g.*, Gary Lawson, *What Lurks Beneath: NSA Surveillance and Executive Power*, 88 B.U. L. REV. 375, 376 (2008). Lawson, for example, is a proponent of the Vesting Clause as a source of presidential authority. *Id.* ("'[T]he executive Power shall be vested in a President of the United States of America.'" (quoting U.S. CONST. art. II, § 1, cl. 1)).

193. U.S. CONST. art. II, § 1, cl. 1; *see also* Steven G. Calabresi & Kevin H. Rhodes, *The Structural Constitution: Unitary Executive, Plural Judiciary*, 105 HARV. L. REV. 1153, 1165-66 (1992) (setting forth an argument for interpreting the Vesting Clause as an independent grant of presidential authority).

the president's authority, but the scope of this "executive Power" is not clear.[194]

There are also instances where Congress explicitly sets out authorities of the President over certain sectors during times of crisis, such as in § 606 of the Communications Act. Section 606(a) provides for presidential authority to prioritize communications that are viewed as essential to national defense and security.[195] Section 606(d) provides for presidential authority to suspend rules applicable to wire communications, to close facilities, or to place the government in control of communications facilities and equipment (provided just compensation is provided to the facility owners) when there is a state or threat of war.[196] Sections 1701 and 1702 of Title 50 of the U.S. Code also address presidential authority to take control of activities involving transactions with foreign countries when a national emergency has been declared to address an "unusual and extraordinary threat" that in substantial part arises from outside the United States.[197] Commentators have discussed giving the President the authority to shut down networks in cases of emergency, but some have noted that this would be risky and would not necessarily address a demonstrable need.[198]

How might the executive branch step in and direct the behavior of private parties? On one hand, the executive branch possesses substantial regulatory power in the form of administrative agency regulations. The authorities of administrative agencies are delegated to them by Congress, and the required procedures are set forth in the Administrative Procedure Act (APA).[199] On the other end of the spectrum exists the authority that the President possesses as the Commander-in-Chief of the nation's military forces, which some commentators say was included in the Constitution to set forth the hierarchy and ensure that there remains some degree of civilian control over military activity.[200] The President's power as the Commander-in-Chief includes the concept of martial law, which may

194. *See* Calabresi & Rhodes, *supra* note 193, at 1175-78.

195. 47 U.S.C. § 606(a) (2012).

196. *Id.* § 606(d).

197. 50 U.S.C. §§ 1701, 1702(a) (2012).

198. Gregory T. Nojeim, *Cybersecurity and Freedom on the Internet*, 4 J. NAT'L SECURITY L. & POL'Y 119, 133-34 (2010).

199. *See* 5 U.S.C. § 500 (2012). Subchapters 1 through 3 of Chapter 5 of Title 5 contain procedural requirements for the type of formal agency action that is likely to be relevant to the current topic.

200. Lawson, *supra* note 192, at 381.

be declared when there has been a breakdown of civil law and the government has to step in to control the situation.[201]

Each of these options likely requires explicit authorizing action by Congress. Executive agencies derive their authority from statutes and cannot act contrary to statute, though courts generally defer to agency interpretation on matters where Congress was unclear or ambiguous.[202] There are also substantial questions about whether the President has the authority to unilaterally declare martial law or whether Congress must approve any such declarations.[203] Under certain circumstances, however, the President can utilize his authority as the Commander-in-Chief of the nation's military forces to order limited military action without congressional approval under the War Powers Resolution of 1973.[204] Short of formal administrative action, martial law, or military action, though, does the President have binding authority to order private parties to take specific action?

Recent commentary suggests that cyberspace will play a significant role in future wars,[205] and Congress stated in the National Defense Authorization Act of 2012 that the military should apply the laws of war to cyber conflicts.[206] Many recent conflicts between nations have involved cyber warfare elements, including the conflict between Russia and Ukraine.[207] Because of the danger that America's cyber infrastructure will be a target in future international conflicts and the inconsistent speed with which Congress has been making progress on cybersecurity legislation, it is essential to determine whether the President has the power to require, or even politely request, that private providers of critical infrastructure improve their cybersecurity practices or share cyber threat information.

---

201. *See* 53A AM. JUR. 2D *Military and Civil Defense* § 374 (2014).

202. Chevron, U.S.A., Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837, 842-43 (1984).

203. *See, e.g.*, Jason Collins Weida, Note, *A Republic of Emergencies: Martial Law in American Jurisprudence*, 36 CONN. L. REV. 1397, 1399-1400 (2004).

204. 50 U.S.C. §§ 1541-1548 (2012).

205. *See* Pragati Verma, *Future Wars Will Be Fought in Cyberspace*, FIN. EXPRESS (Aug. 24, 2009), http://www.financialexpress.com/news/future-wars-will-be-fought-in-cyberspace/505992.

206. National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 954, 125 Stat. 1298, 1551 (2011).

207. Sanger, *supra* note 12, at A18. The conflicts in Georgia and Syria also included cyberwar elements. *Id.*

In *Youngstown Sheet & Tube Co. v. Sawyer*,[208] the Supreme Court evaluated whether President Truman could seize steel mills to prevent interruption of manufacturing by a strike during a time of conflict absent a formal declaration of war. While a majority of Justices agreed that such a seizure went beyond the scope of the executive power under the Constitution,[209] the Justices viewed the case in many different ways, resulting in five solo concurrences. The seizure was viewed as being analogous to legislating, so it would fall within Congress's enumerated powers, not the President's.[210] Justice Black, a strict textualist, did not read the Constitution as allowing for any inherent presidential powers.[211] Justice Frankfurter, on the other hand, suggested that the President may have limited inherent powers,[212] while Justice Jackson's concurring opinion provided a more helpful test for evaluating whether a President has authority to act.[213] Under Justice Jackson's test, there are three zones of authority for the exercise of a President's powers. The President has the most authority when Congress approves the President's action, the least authority when his acts go against the express or implied will of Congress, and an intermediate amount of authority, which means that he can act as long as Congress remains indifferent about the subject, when Congress has said nothing for or against the President's actions.

B. Executive Action on Cybersecurity and Critical Infrastructure

Protecting critical infrastructure has been an increasingly important priority over the last decade. The Homeland Security Administration is statutorily entrusted with many federal cybersecurity issues[214] and may also assist private operators of critical infrastructure upon request by the private entities,[215] but so far, government involvement in private cybersecurity matters has been purely voluntary on the part of the private entities.

208. 343 U.S. 579 (1952).
209. *Id.* at 587.
210. *Id.* at 587-88.
211. *Id.* at 585.
212. *Id.* at 610-11 (Frankfurter, J., concurring).
213. *Id.* at 635-38 (Jackson, J., concurring).
214. *See* 6 U.S.C. § 131 (2012) (defining terms relevant to the Critical Infrastructure Information Act of 2002).
215. *Id.* § 143.

The Executive Order of February 2013 is just one of many actions by a sitting U.S. President acknowledging the importance of this topic.[216] The three most recent presidential administrations, including President Obama during his first term, have all publicly promoted the importance of securing critical infrastructure.[217] Several of these have been in the form of presidential directives. Presidential directives, sometimes called national security directives or presidential policy directives, are a specific category of executive orders relating to national security or defense.[218] The position of the Department of Justice (DOJ) is that such directives have the same legal effect as an executive order.[219]

In July 1996, President Clinton issued Executive Order 13,010, which established the President's Commission on Critical Infrastructure Protection (PCCIP).[220] President Clinton issued Presidential Decision Directive 63 (PDD-63) in May 1998 in an attempt to effect the changes recommended in the PCCIP's report.[221] The actions of the Bush administration on the topic include Executive Order 13,231,[222] Homeland Security Presidential Directive 7 (HSPD-7),[223] the National Strategy to Secure Cyberspace,[224] the

---

216. Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013).

217. Critical Infrastructure Protection, Presidential Decision Directive 63, (May 22, 1998), *available at* http://www.fas.org/irp/offdocs/pdd/pdd-63.htm; Critical Infrastructure Identification, Prioritization, and Protection, Homeland Security Presidential Directive 7 (Dec. 17, 2003) [hereinafter PD-7], *available at* http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1; THE WHITE HOUSE, CYBERSPACE POLICY REVIEW (2009), http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf; *see also* Eric A. Greenwald, *History Repeats Itself: The 60-Day Cyberspace Policy Review in Context*, 4 J. NAT'L SECURITY L. & POL'Y 41, 41 (2010).

218. *See* Jeffrey C. Fox, *What Is an Executive Order?*, THISNATION, http://www.thisnation.com/question/040.html (last visited Jan. 5, 2015).

219. Legal Effectiveness of a Presidential Directive, as Compared to an Executive Order, 24 Op. O.L.C. 29, 29 (2000), *available at* http://www.justice.gov/sites/default/files/olc/opinions/2000/01/31/op-olc-v024-p0029_0.pdf.

220. Greenwald, *supra* note 217, at 44.

221. *See id.* at 45-46.

222. Critical Infrastructure Protection in the Information Age, Exec. Order No. 13,231, 66 Fed. Reg. 53,063 (Oct. 16, 2001).

223. PD-7, *supra* note 217.

224. THE WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE (2003), *available at* http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf.

National Infrastructure Protection Plan,[225] and several directives that are still classified, such as National Security Presidential Directive 16 (NSPD-16)[226] and National Security Presidential Directive 54 (NSPD-54).[227] In 2009, President Obama issued the Cyberspace Policy Review.[228] The Cyberspace Policy Review recognizes the importance of establishing leadership within the federal government to improve cybersecurity issues and describes cybersecurity as a global issue that also requires international cooperation.[229] In 2010, President Obama declassified some aspects of NSPD-54,[230] and a number of details about the previously classified Comprehensive National Cybersecurity Initiative are now available on the White House website.[231] On February 12, 2013, President Obama issued Executive Order 13,636, titled Improving Critical Infrastructure Cybersecurity.[232] Two years later, President Obama issued another executive order about cybersecurity, and this one focused specifically on information sharing.[233]

PDD-63, HSPD-7, and the Cyberspace Policy Review all stress the importance of the government working closely with the private sector to ensure adequate protection and implementation. Executive Order 13,636 and Executive Order 13,691 both emphasize cooperation between the government and private sector. As is

225. DEP'T OF HOMELAND SEC., NATIONAL INFRASTRUCTURE PROTECTION PLAN: PARTNERING TO ENHANCE PROTECTION AND RESILIENCY (2009), *available at* http:// www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

226. CLAY WILSON, CONG. RESEARCH SERV., RL31787, INFORMATION WARFARE AND CYBERWAR: CAPABILITIES AND RELATED POLICY ISSUES 10 (2004), *available at* http://www.researchgate.net/publication/235012618_Information_Warfare_and_Cyberwar_Capabilities_and_Related_Policy_Issues.

227. *See* Ellen Nakashima, *Bush Order Expands Network Monitoring; Intelligence Agencies to Track Intrusions*, WASH. POST, Jan. 26, 2008, at A03 (discussing a classified directive authorizing federal intelligence agencies to monitor federal agencies' computer networks).

228. THE WHITE HOUSE, *supra* note 217.

229. *Id.* at 7-9, 20-21.

230. Jaikumar Vijayan, *Obama Administration Partially Lifts Secrecy on Classified Cybersecurity Project*, COMPUTERWORLD (Mar. 2, 2010, 6:40 PM), http://www.computerworld.com/article/2520273/cybercrime-hacking/obama-administration-partially-lifts-secrecy-on-classified-cybersecurity-project.html.

231. *The Comprehensive National Cybersecurity Initiative*, WHITE HOUSE, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (last visited Jan. 5, 2015).

232. Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013).

233. Promoting Private Sector Cybersecurity Information Sharing, Exec. Order No. 13,691, 80 Fed. Reg. 9,349 (Feb. 13, 2015).

evidenced by these documents, the President regularly makes recommendations that, if implemented, would alter many aspects of private businesses, but these recommendations are typically voluntary.

C. The Potential for Mandatory Cybersecurity Regulations

To what extent does the President have the authority, either inherent or otherwise, to require the private entities in control of critical infrastructure to take steps to protect their systems? Under § 606(d) of the Communications Act,[234] the President may have the authority to take control of communications providers and require additional security if there is a "threat of war," but there does not appear to be explicit correlating authority over other critical infrastructure, such as power and water companies.[235]

The wording of § 606(d), however, is potentially broad enough to permit the President substantial control over critical infrastructure access to the Internet because it authorizes government control over wire communications facilities *and equipment* when there exists a state or threat of war.[236] The full ramifications of this wording are not fully clear, but there may be an argument that in enacting § 606(d), Congress intended for the President to have control over critical communications infrastructure in times of crisis, and that this intent would also extend to an intent that the President have control over the elements of that communications infrastructure that are inseverable from other types of critical infrastructure. Insofar as modern power companies need to be connected to the Internet to render services, § 606(d) might permit the President to exert some level of control over the methods through which these power companies are connected by wired communications technology to the outside world.[237] Further analysis of the legislative history of § 606(d) may be beneficial. Such a reading of § 606(d) would stretch

234. 47 U.S.C. § 606(d) (2012).

235. *See id.*

236. *Id.*

237. Zhang notes that many of the SCADA systems used by power companies are connected to the Internet or to a wireless network, and 85% of the relays in the electric grid system are digital. Zhang, *supra* note 43, at 327-28. In the case of power companies, it is unclear how this possible presidential authority will interact with the existing cybersecurity standards set by the North American Electric Reliability Corporation (NERC). *See id.* at 324; *see also* Trope & Humes, *supra* note 102, at 670 (expressing skepticism that it would be feasible for boards to comply with the Cybersecurity Framework and the NERC standards).

the text of the statute and would likely only be appropriate as a remedy in extreme situations.

Because the reach of § 606(d) is unclear, the extent of presidential authority must also be analyzed in other ways. In evaluating whether the President has the authority to require private actors to implement stronger cybersecurity measures, we can turn to Justice Jackson's test in his concurring opinion in *Youngstown*.[238] Is this an area where Congress has expressly supported the use of presidential authority for this purpose? This is unclear, given the prior analysis of statutory authority, though there may be an argument that in authorizing presidential control of wired communications, Congress intended to give the President authority over the methods used to secure wired communications, since the language does allow government control to be exerted over equipment when there is a threat of war.

The more important question in determining the scope of any such power is whether exercise of presidential authority would be counter to the express or implied will of Congress. This is a very tricky question and requires analogizing. Looking at the context of various statutes, we can begin to shape an idea of the conditions when Congress might or might not approve of the use of presidential authority to unilaterally impose requirements on private operators of critical infrastructure. Under § 143 of Title 6, involvement of the Department of Homeland Security in cybersecurity issues of privately held critical infrastructure is limited to the voluntary election of the private entities.[239] This focus on voluntary election by private owners of critical infrastructure suggests that Congress would not approve of the executive branch interfering with the private entities and controlling critical infrastructure as a matter of everyday affairs. However, § 606(d) of the Communications Act suggests that Congress would approve of the exercise of presidential authority when the country was under a state of war *or* a threat of war, and §§ 1701 and 1702 of Title 50 state that Congress would approve of the exercise of presidential authority over transactions with foreign nations when the exercise relates to a presently declared national emergency.

---

238. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 635-38 (1952) (Jackson, J., concurring).

239. 6 U.S.C. § 143 (2012) (authorizing DHS to provide cybersecurity assistance to private operators of critical infrastructure "upon request"). The voluntary nature of this intervention is reiterated by the National Cybersecurity Protection Act of 2014. Pub. L. No. 113-282, § 3, 128 Stat. 3066, 3066.

Looking at other statutes, then, suggests that while there is not explicit support for the exercise of presidential authority in this precise context, it would not necessarily be counter to congressional will in all cases either, though presidential authority to impose cybersecurity requirements on private entities may be limited to when there exists a state of war, a threat of war, or a declared national emergency. In our view, declaring a national cybersecurity emergency and using § 606 to order critical infrastructure providers to implement stronger protections would be less deleterious of civil liberties than the "Internet kill switch" proposal which has been struck down in Congress repeatedly.[240]

Further analysis would be beneficial to evaluate whether Congress intended to give the President authority over measures taken to secure wired communications equipment in other critical infrastructure areas. Even if that intent is unclear, it is still apparent that it would not be in opposition to congressional will for the President to exercise authority in cases of conflict or declared national emergency. As long as Congress continued to remain neutral on the topic, then, the President could exercise some authority in the interest of protecting national security.

However, in post-9/11 America, we should be cautious about relying on emergency justifications. Liberal democracies rely on the rule of law for stability, and it can be difficult to ensure the rule of law when emergencies occur.[241] There is a fundamental debate between theorists about how and when to address potential emergency situations. This debate involves issues such as whether exceptions should be carved out in the law *ex ante* or whether the government should act outside the law in the event of an emergency.[242] This is a particularly relevant debate in the cybersecurity context, where there is currently very little regulatory guidance and the possible ramifications of a successful attack are quite severe. If an attack like a "cyber Pearl Harbor" occurs, as some

240. David W. Opderbeck, *Cybersecurity and Executive Power*, 89 WASH. U. L. REV. 795, 798-99, 811 (2012).

241. Victor V. Ramraj, *No Doctrine More Pernicious? Emergencies and the Limits of Legality*, *in* EMERGENCIES AND THE LIMITS OF LEGALITY 3, 4 (Victor V. Ramraj ed., 2008).

242. For example, in the Ramraj text, the contributors who wrote chapters took a variety of positions on this point. The debate between Dyzenhaus and Gross is particularly illustrative, with Dyzenhaus emphasizing *ex ante* handling of potential emergency situations and Gross suggesting that it may be a better idea for government agents to engage in extra-legal actions with the possibility of ratification of their illegal actions after the fact. *Id.* at 12.

commentators warn is possible,[243] rapid legislative or executive responses are likely.[244] If this happens without any sort of existing guidelines, the resulting government action could make CISPA look as innocuous as a lunch menu. Thus, while existing laws suggest that the President has the authority to take control of critical infrastructure in the event of a cybersecurity emergency, we strongly urge policy makers to push forward with CISPA or a similar legislative proposal, while continuing to seek a sustainable balance between security and privacy. Our circle of trust framework could be applied to this end.

D. Voluntary Cooperation

Requests for voluntary cooperation with the government are likely to be less intrusive upon civil liberties than mandatory regulations. Both CISPA and the Order emphasize this type of approach, and the NCPA and CEA bestow congressional approval on voluntary cybersecurity programs. The legislative proposal announced by the White House in January 2015 also focuses on voluntary information sharing.[245]

However, nominally voluntary executive action may still raise civil liberties concerns in practice. To demonstrate this, consider the wiretapping controversy that began under President George W. Bush. In evaluating the actions of the NSA, the Department of Justice concluded that the wiretapping was consistent with the authority of the President under the Constitution.[246] The DOJ reasoned that the President has the authority to conduct activities that are critical to national security.[247] In the wiretapping situation, where the Administration justified its activities by referring to the

243. *See, e.g.*, Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121, 172-73 (2009) (expressing the need to set out policies in advance of a "cyber Pearl Harbor-like attack").

244. *See* Oren Gross, *Extra-Legality and the Ethic of Political Responsibility*, *in* EMERGENCIES AND THE LIMITS OF LEGALITY, *supra* note 241, at 88 (discussing the rush after an emergency to pass new legislation).

245. Securing Cyberspace, *supra* note 83.

246. U.S. DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT 1 (2006), *available at* http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB178/surv39.pdf ("The President has the chief responsibility under the Constitution to protect America from attack, and the Constitution gives the President the authority necessary to fulfill that solemn responsibility.").

247. *Id.* at 5.

President's inherent authority under the Constitution, private entities were generally not subject to legal compulsion.[248] Telecommunications companies that cooperated with the NSA's wiretapping efforts often did so voluntarily, at least nominally so.[249] The wiretapping controversy illustrates that making the private-to-government information flow voluntary, as CISPA would do, does not guarantee the protection of civil liberties. The risks of voluntary programs are addressed in more detail in Section IV.A.

Information sharing is just one form that a voluntary program might take. A voluntary program could also focus on adoption of cybersecurity technology. This leads to a new question about what incentives might encourage voluntary participation in a technology adoption program, a question that is also addressed in the Order.[250] In Section IV.A, we address this issue and provide some recommendations about incentives for companies to adopt the cybersecurity standards suggested by the Cybersecurity Framework.

While emphasizing security standards instead of information sharing might lessen some of the civil-liberties issues, the issue of providing private companies with security standards may still raise concerns. As long as only passive defense standards are requested,[251] concerns about the company's legal liability likely would not outweigh the value of participating in the program. However, if the President requested that critical infrastructure providers implement active defense mechanisms, including software to enable counterstrikes against cyber attackers to mitigate harm to the systems, that might require more careful oversight because of the potential liability issues if a counterstrike harms an innocent party. This situation could also raise potential international law issues due to the possibility that a counterstrike would hit targets located in foreign countries.[252]

---

248. This is not to say the government did not pressure providers to comply with its requests. Qwest, a major telecommunications provider that refused the NSA's requests, was reportedly pressured by suggestions that Qwest might lose out on future classified contracts or that its failure to cooperate could endanger national security. *See* Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY (May 11, 2006, 10:38 AM), http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

249. *See id.*

250. Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13,636, § 8(d), 78 Fed. Reg. 11,739, 11,742 (Feb. 12, 2013).

251. *See* Sklerov, *supra* note 104, at 21. For more of our discussion of passive defense, see Kesan & Hayes, *supra* note 98, at 471.

252. *See* Kesan and Hayes, *supra* note 98, at 508.

In the terms of our circle of trust framework for information sharing, the President is authorized to permit government secrets about cybersecurity to move into the center circle, but is probably not authorized to encourage private actors to move their own cybersecurity secrets into the center circle. Accordingly, accompanying legislation would be necessary in order to fully implement the circle of trust framework for cyber threat information sharing. The legislative proposal that the White House announced in January 2015 would provide some of the authorization needed,[253] and therefore provides a promising path to operationalizing the circle of trust. The Cybersecurity Framework matches up with our circle of trust framework in a way different from the cyber threat information-sharing provisions of the Order. Government-to-private information sharing is present when the government shares information about optimal cybersecurity protection, and permitting the government to evaluate adoption of the Cybersecurity Framework is a form of private-to-government information sharing. Through the evaluation of the implementation, all parties can examine the success or failure of the program, and thus reap benefits. This form of information sharing by the private sector should not require congressional intervention, because it is merely evaluating the usefulness of information provided by the government and does not require the private sector to share its own secrets with the government.

E. Comparing Executive Order 13,636 with CISPA

In this Section, we will evaluate the Executive Order by comparing it with CISPA and other legislative proposals when appropriate. Executive Order 13,636, which is titled Improving Critical Infrastructure Cybersecurity, has many themes in common with CISPA. Many of the differences are not that different. Consider, for example, the language used to describe the sectors to be protected. CISPA generally eschewed the term "critical infrastructure" in favor of the narrower term "utilities."[254] On the other hand, the Order adopted the term "critical infrastructure" as defined by the Homeland Security Act,[255] but Presidential Policy Directive 21 (PPD-21) narrowed this term by specifically

253. Securing Cyberspace, *supra* note 83.

254. Cyber Intelligence Sharing and Protection Act, H.R. 234, 114th Cong. § 3 (2015).

255. Exec. Order No. 13,636, 78 Fed. Reg. at 11,739.

enumerating the sectors that would be covered.[256] Thus, even though the Order uses the broader term "critical infrastructure," it then narrows it by specifically enumerating covered sectors. The CEA and NCPA similarly use the term "critical infrastructure," and the CEA also includes the limiting "sector-specific agency" language of PPD-21.[257]

Both CISPA and the Order focus on information sharing, and both address the need to make security clearances available to certain personnel employed by critical infrastructure providers.[258] The biggest difference between the two is the direction of the flow of cyber threat information. CISPA allows threat information to flow from the private sector to the government, as well as from the government to the private sector.[259] The Order only provides for threat information sharing by the government with the private sector.[260] In other words, CISPA permits cybersecurity information to flow from both the public and private sectors into the central circle of trust. CISPA's information flow model is also found in the legislative proposal announced by the White House in January 2015.[261]

Both CISPA and the Order emphasize the voluntary nature of private-sector participation. However, while CISPA is focused only on the information-sharing aspect, §§ 7 and 8 of the Order focus on the possibility of setting cybersecurity standards through the Cybersecurity Framework and creating a voluntary program to encourage its adoption.[262] The NIST makes available information about the progress of the Cybersecurity Framework on its website, including links to the Order, public comments, and webcast recordings of workshop meetings.[263]

---

256. Press Release, The White House, Presidential Policy Directive—Critical Infrastructure Security and Resilience, Presidential Policy Directive/PPD-21 (Feb. 12, 2013) [hereinafter PPD-21], *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

257. Pub. L. No. 113-282, 128 Stat. 3066 (2014); Pub. L. No. 113-274, 128 Stat. 2971 (2014).

258. H.R. 234; Exec. Order No. 13,636, § 4, 78 Fed. Reg. at 11,740.

259. H.R. 234.

260. Exec. Order No. 13,636, § 4, 78 Fed. Reg. at 11,739-40.

261. Securing Cyberspace, *supra* note 83.

262. *Id.* §§ 7-8, 78 Fed. Reg. at 11,740-42.

263. *Cybersecurity Framework*, NIST, http://www.nist.gov/cyberframework/ (last visited Jan. 5, 2015).

The Order calls for DHS to propose possible incentives to promote participation in the voluntary cybersecurity program, though it notes the possibility that additional legislation might be required in order to implement some types of incentives.[264] It is not clear what type of incentives President Obama is envisioning in this Order. In terms of financial incentive, tax breaks when a company is found to be sufficiently adhering to the program *or* tax credits for the cost of implementing suggested controls may both be viable options. Another option is for the Cybersecurity Framework to exempt private entities from civil liability when the entity makes a good faith effort to comply with the Cybersecurity Framework.[265] Liability exemptions are the only incentive for participation in CISPA as of March 2015. For purposes of the Order and the Cybersecurity Framework, adopting any of these three incentive models would most likely require congressional legislation, and none of the new cybersecurity laws enacted by Congress in December of 2014 address incentives to adopt standards.

1. *Liability Exemptions and Voluntariness*

The Order does not contain any provisions addressing civil liability. CISPA contains two: proposed § 1104(b)(3), and proposed § 1104(f)(5). Under proposed § 1104(b)(3), entities are exempt from civil and criminal liability for actions relating to identifying, obtaining, or sharing cyber threat information pertaining to their systems.[266] This exemption itself does not cause CISPA to differ from the Order further than it already does because this exemption applies only to the private-to-government flow of information, which the Order does not permit. On the other hand, proposed § 1104(f)(5) is much broader and emphasizes that there will be no liability for entities that choose to not participate in activities that CISPA authorizes.[267] Clarification is needed concerning whether this exemption from liability refers to civil liability. The way that it is currently written, it could prevent civil liability from attaching based

264. Exec. Order No. 13,636, § 8(d), 78 Fed. Reg. at 11,742.

265. *See* Trope & Humes, *supra* note 102, at 722 (noting that a congressional enactment would be required in order to give companies some assurance of immunity, in case some of the measures adopted for mitigating harm and creating more resilient systems did not work or caused additional harm).

266. Cyber Intelligence Sharing and Protection Act, H.R. 234, 114th Cong. § 3 (2015).

267. *Id.*

on the company not following the voluntary program. Thus, cooperation with the program would be more easily considered voluntary because a private entity would not risk potential civil liability if they did not participate. The Cyber Threat Sharing Act of 2015, which is based on President Obama's January 2015 legislative proposal takes a similar approach to CISPA, focusing on voluntary information sharing enhanced by a broad liability exemption.[268] The Cyber Threat Sharing Act of 2015 is more specific than CISPA, explicitly exempting companies from civil and criminal liability for disclosure or receipt of lawfully obtained cyber threat indicators.[269]

Statutory liability exemptions are not uncommon. There is one such exemption in the Stored Communications Act excusing electronic communication service providers from liability for sharing customer information.[270] The FISA Amendments Act of 2008 also provides release from liability for electronic communication service providers who provided information to comply with a directive issued by the Director of National Intelligence and the Attorney General.[271] However, as we discuss in Subsection IV.B.2, the inclusion of a liability exemption for private entities that share information may also remove incentives for these entities to treat their customers' information with care.

In the case of a private entity that does not adopt a voluntary cybersecurity standard, an exemption from liability may reinforce the voluntary aspect of such a program. However, if the voluntary procedures are costly to implement, a free rider problem may develop, as those who do not make the investment in compliance nonetheless are still able to reap the benefits because the more protected firms will help to reduce the circulation of malware. Essentially, if a large enough percentage of firms adopt the standard, it could foster the cybersecurity version of herd immunity,[272] and the unprotected firms could still reap benefits. From a social welfare

268. S. 456, 114th Cong. (2015).

269. *Id.* at § 2.

270. 18 U.S.C. § 2703(e) (2012).

271. 50 U.S.C. § 1881a(h)(3) (2012).

272. "Herd immunity" is a term often heard in the context of vaccines. *Community Immunity ("Herd Immunity")*, VACCINES.GOV, http://www.vaccines.gov/basics/protection/ (last visited Jan. 5, 2015). The idea is that by having most people in a community vaccinated for a particular illness, those who are not able to be vaccinated still reap benefits because the illness is not likely to appear in their community. *Id.* In the cybersecurity context, herd immunity could theoretically exist if a majority of networked systems were secure, because there would be fewer potential "carriers" of malicious code.

perspective, it may also be desirable to allow consumers to point to noncompliance with federal standards as evidence of negligent cybersecurity practices. This would likely not be possible if DHS includes a liability exemption as an incentive for compliance with the Cybersecurity Framework.

2. *Civil Liberties*

As the Obama Administration's response to CISPA indicates, the perceived civil-liberties failings of CISPA are a major reason that the administration is opposed to this legislation. The Order thus represents President Obama's efforts to establish that security and civil liberties are not mutually exclusive, and to find that elusive balance between security and privacy. Section 1 of the Order underscores the Administration's policy to enhance the security and resilience of critical infrastructure systems without sacrificing "business confidentiality, privacy, [or] civil liberties."[273] Section 5 goes into more detail about protections for privacy and civil liberties, stressing that such protections will be based on the Fair Information Practice Principles (FIPPs), as well as other applicable policies, principles, and frameworks.[274] The eight FIPPs are (1) Transparency; (2) Individual participation; (3) Purpose specification; (4) Data minimization; (5) Use limitation; (6) Data quality and integrity; (7) Security; and (8) Accountability and auditing.[275]

However, the January 2015 legislative proposal may compromise the administration's civil liberties high ground in comparison with CISPA. In authorizing members of the private sector to share cyber threat indicators with the National Cybersecurity and Communications Integration Center of DHS, the legislative proposal and the bill modeled after it echo the most problematic phrase from CISPA: "Notwithstanding any other provision of law."[276] As our analysis above shows, this does not truly circumvent any meaningful privacy law protection, but leaving this

273. Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13,636, § 1, 78 Fed. Reg. 11,739, 11,739 (Feb. 12, 2013).

274. *Id.* § 5, 78 Fed. Reg. at 11,740.

275. Privacy Policy Guidance Memorandum No. 2008-01 from Hugo Teufel III, Chief Privacy Officer, U.S. Dep't of Homeland Sec., on The Fair Information Practice Principles: Framework for Privacy Policy at the Dep't of Homeland Security 1 (Dec. 29, 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

276. S. 456 § 2, 114th Cong. (2015); Information Sharing Legislative Proposal, *supra* note 80, at §106(a).

wording intact could limit the effectiveness of future revisions to privacy law.[277]

There also may be privacy implications from the direction of information flow. The Order refers to reducing risks to privacy in the context of a legal regime that would only allow for cyber threat intelligence to flow from the government to the private sector. CISPA, on the other hand, only discusses privacy and civil-liberties concerns in the private-to-government direction of information flow. Privacy concerns can be raised in the government-to-private context as well, as the government deals with a large amount of personally identifiable information. Why does CISPA not address privacy and civil-liberties concerns in the context of information flowing from the government to the private sector?

Our circle of trust framework visualizes the central circle as receiving many protections, whether the information came from the government or the private sector originally. The fact that the Order creates a way for classified data to be shared with the private sector is significant because that provides a more comprehensive data set concerning what the government knows,[278] even though cyber threat information from the private sector would not be placed in the circle under the Order. CISPA's failure to account for possible privacy and civil-liberties concerns when the government discloses information may be inconsistent with our circle of trust framework.

In terms of privacy protections, the biggest advantage of the Order over CISPA is that, without the power to enact new legislation, the Order does not have the option of directing agencies to ignore existing privacy law. In stark contrast, through CISPA's current "[n]otwithstanding any other provision of law" clause,[279] all existing privacy law is disregarded–though as we noted above, it is unclear if the application of modern privacy law would change the way that CISPA could be applied. Some have criticized the Order as lacking "teeth" because of this,[280] but that is primarily due to the very nature of an executive order. The administration's January 2015

277. *See supra* Section II.D.

278. *See* Zhang, *supra* note 43, at 339 ("Classified and unclassified data together create a comprehensive data set when either data group alone would present an incomplete picture.").

279. Cyber Intelligence Sharing and Protection Act, H.R. 234, 114th Cong. § 3 (2015).

280. *E.g.*, Dave Frymier, *The Cyber Security Executive Order Is Not Enough*, WIRED (Mar. 1, 2013, 12:19 PM), http://www.wired.com/insights/2013/03/the-cyber-security-executive-order-is-not-enough/.

legislative proposal introduces these CISPA-style teeth,[281] suggesting that notwithstanding the limited reach of the Executive Order, the White House's goals for cybersecurity policy are ultimately consistent with many aspects of CISPA.

3. *Presidential Policy Directive 21*

The Order is accompanied by PPD-21, which primarily focuses on the responsibilities of the agencies rather than the overall policy goals. The focus on the role of government agencies in PPD-21 is much more detailed than the references to government agencies in CISPA. PPD-21 focuses on three strategic imperatives. The first strategic imperative emphasizes the need to unify efforts across the federal government relating to the protection of critical infrastructure.[282] To further this goal, PPD-21 requires DHS to operate two critical infrastructure centers: one to focus on physical infrastructure, and one to focus on cyber infrastructure.[283] The second strategic imperative focuses on baseline data and systems requirements to ensure format uniformity, interoperability, and redundancy to ensure continued access if there is a disruption.[284] The third strategic imperative is to use data analysis to inform decisions regarding critical infrastructure, including ongoing analysis of incidents, threats, and emerging risks, to provide "a near real-time situational awareness capability."[285] This third imperative has the potential to create a very valuable resource for tracking cyber threats so that information can be shared with the private sector in a timely manner.

PPD-21 also emphasizes the importance of sector-specific agencies (SSAs). Under the directive, SSAs are defined as the department or agency that is designated to work with a specific critical infrastructure sector on their security and resilience programs.[286] PPD-21 identifies sixteen critical infrastructure sectors. Of the sixteen, DHS is listed as the sole SSA for eight sectors and is a co-SSA for two additional sectors. This emphasis on the participation of DHS is consistent with existing trends in academic commentary about the role of DHS in handling cybersecurity issues

281. Information Sharing Legislative Proposal, *supra* note 80, at §103(a)
282. PPD-21, *supra* note 256.
283. *Id.*
284. *Id.*
285. *Id.*
286. *Id.*

relating to critical infrastructure.[287] It also produces an additional similarity between the Order, PPD-21, and CISPA because each places significant focus on DHS and the Secretary of Homeland Security.[288] This emphasis in the Order indicates that DHS will be a key player in the Cybersecurity Framework and is also likely to be a key player in future legislation focusing on cybersecurity.[289] The National Cybersecurity Protection Act of 2014 is the first major example of such legislation.[290] The NCPA references the situational awareness and sector-specific agency language of PPD-21,[291] which suggests that in passing the NCPA, Congress intended to formalize a number of elements of PPD-21.

The Order and PPD-21 each require multiple annual reports. Section 5(b) of the Order requires an annual review of the report on privacy and civil-liberties risks associated with the program,[292] and §§ 8 and 9 each require an annual report pertaining to critical infrastructure found to be at greatest risk.[293] Under § 8(c), the SSAs are required to report annually to the President about the program participation by owners and operators of critical infrastructure at greatest risk, and under § 9(a), the list of critical infrastructure at greatest risk shall be reviewed and updated annually. PPD-21 also preserves the obligation of the Secretary of Homeland Security to submit annual reports "on the status of national critical infrastructure" and also requires SSAs to provide annual reports to support the Secretary in the preparation of his annual reports.[294] These reporting requirements are similar to the reporting requirements of CISPA, though CISPA's reporting requirements solely emphasize civil-liberties concerns relating to the sharing of cyber threat information by the private sector.

---

287. *See* Coldebella & White, *supra* note 116, at 240-41 (noting that DHS has established the Critical Infrastructure Protection Advisory Council and also has Sector Coordinating Committees to address similar issues).

288. Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13,636, § 9(a), 78 Fed. Reg. 11,739, 11,742 (Feb. 12, 2013); PPD-21, *supra* note 256; Cyber Intelligence Sharing and Protection Act, H.R. 234, 114th Cong. (2015).

289. In recent years, critics of the DHS have asserted that the DHS has not properly addressed threats to the nation's cyber infrastructure. *See, e.g.*, Rebecca C.E. McFadyen, *Protecting the Nation's Cyber Infrastructure: Is the Department of Homeland Security Our Nation's Savior or the Albatross Around Our Neck?*, 5 I/S: J.L. & POL'Y FOR INFO. SOC'Y 319, 323 (2009).

290. Pub. L. No. 113-282, 128 Stat. 3066.

291. *Id.* at § 3.

292. Exec. Order No. 13,636, § 5(b), 78 Fed. Reg. at 11,740.

293. *Id.* §§ 8(c), 9(a), 78 Fed. Reg. at 11,742.

294. PPD-21, *supra* note 256.

However, we worry that both CISPA and the Order miss the mark on a very important topic: voluntariness. In our view, at least some private owners of critical infrastructure should be subject to mandatory government regulation on this topic, where their action or inaction could have dire national security consequences. Thus, when enacting formal legislation like CISPA, the 2015 legislative proposal, the NCPA, or the CEA, Congress should consider diverging from the pure voluntariness model and requiring disclosure of some classes of information. A purely voluntary technology adoption program may also be undesirable. Voluntariness is addressed in more detail in Section IV.A.

IV. RECOMMENDATIONS

Ultimately, legislative changes are needed that reach an effective balance between privacy and security. In our circle of trust framework, information would be shared by both sides, and the legislative regime would ensure that disclosed information is used appropriately and civil liberties are protected. CISPA, the Order, and the NCPA all advance methods to allow the private-sector access to classified cyber threat intelligence. Information sharing by the private sector is addressed by CISPA and the Cyber Threat Sharing Act of 2015. In balancing cybersecurity and privacy, CISPA places greater value on security, while the Order places greater value on privacy, and the Cyber Threat Sharing Act of 2015 arguably comes close to placing equal emphasis on both. The Order stresses the need to balance privacy protections and the pursuit of more secure and resilient critical infrastructure systems, but the uncertain legal foundations for elements of the Cybersecurity Framework not addressed by the CEA will likely result in long delays. In this Part, we provide recommendations to address issues surrounding both of these government actions in order to support the creation of a proposal that is consistent with our circle of trust framework.

A. The Big Hole in CISPA and the Order: Voluntariness

Should a circle of trust be built based on purely voluntary participation, or would a mandatory element be consistent with this framework? Thus far, cybersecurity proposals have predominantly emphasized voluntary participation. In CISPA, the voluntariness is in the context of cyber threat information sharing. In the Order, the voluntariness is in the context of adopting the Cybersecurity

Framework and the protections that it requires. The CEA underscores the voluntary nature of cybersecurity standards adopted by NIST.[295] In our view, a purely voluntary approach to either cyber threat information sharing or technology adoption could hinder the effectiveness of the programs, interfere with the establishment of a circle of trust between the private and public sectors, and may even violate international law.

Article 58 of the Geneva Convention Additional Protocol I requires a party to the conflict to protect its own civilians and civilian objects against "dangers resulting from military operations."[296] Jensen argues that complying with this legal obligation requires a proactive instead of reactive approach, and that a purely voluntary regime for cybersecurity preparedness might actually violate Article 58.[297] However, a government-led cybersecurity preparedness program may involve the execution of some cyber operations on privately owned networks, which raises other issues. Butler warns that cyber operations could potentially affect private civilian networks in a way that violates the Third Amendment.[298] If both Jensen and Butler are correct, this means that there may be tension between the Geneva Convention and the Constitution of the United States on the topic of voluntary cybersecurity programs. Butler's legal analysis is novel and interesting, but ultimately, we disagree with his conclusions concerning the Third Amendment, and believe that it stretches the language of the Third Amendment too far.[299]

Beyond the question of whether voluntary cybersecurity programs would be legal or required, the relative strengths of mandatory and voluntary regulations have been widely debated,

---

295. Pub. L. No. 113-274, § 101, 128 Stat. 2971, 2972 (2014).

296. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 58(c), June 8, 1977, 1125 U.N.T.S. 3, 29.

297. Jensen, *supra* note 7, at 1561.

298. Alan Butler, *When Cyberweapons End Up on Private Networks: Third Amendment Implications for Cybersecurity Policy*, 62 AM. U. L. REV. 1203, 1209-10 (2013). The Third Amendment reads, in full, "No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law." U.S. CONST. amend. III.

299. Specifically, we feel that Butler's analysis stretches the meanings of "soldier," "house," and "quartered." While it is true that policymakers are often called upon to apply old language to new technology, the environment created by cyberwarfare is sufficiently different from the environment of kinetic warfare that the creation of new policies would be more beneficial.

especially among law and economics theorists. The debate arises in many contexts, from environmental regulations,[300] to the labeling of hazardous chemicals,[301] to regulations affecting the financial sector.[302] Much of the literature is especially focused on mandatory versus voluntary information disclosure. Some economic models conclude that if firms are required to publicly disclose certain types of information, this may give the firms an incentive to not actively seek out information about their own products, services, or operations.[303] If the sort of model referenced by Polinsky and Shavell holds true, economists would expect firms to have more information about their own operations under a voluntary disclosure regime and less information under a mandatory disclosure regime.[304] This model, however, relies on the assumption that the benefit of having that information is less than the cost that might be incurred by disclosing that information.

A regulation that requires information disclosure may be perceived as more market-friendly than a regulation that requires the adoption of specific practices.[305] But some disagree about whether a mandatory information-sharing approach would have a greater effect on the market than a voluntary information-sharing approach. Some economic analysis suggests that firms would be likely to disclose

---

300. *See, e.g.*, JunJie Wu & Bruce A. Babcock, *The Relative Efficiency of Voluntary vs Mandatory Environmental Regulations*, 38 J. ENVTL. ECON. & MGMT. 158, 159 (1999); Anne G. Short & Timothy P. Duane, *Regulatory Spillover: How Regulatory Programs Influence Voluntary Efforts to Adopt Best Management Practices to Manage Non-Point Source Pollution*, 35 ENVIRONS ENVTL. L. & POL'Y J. 37, 40 (2011).

301. *See, e.g.*, Goh Choo Ta et al., *A Comparison of Mandatory and Voluntary Approaches to the Implementation of Globally Harmonized System of Classification and Labelling of Chemicals (GHS) in the Management of Hazardous Chemicals*, 49 INDUS. HEALTH 765, 766 (2011).

302. *See, e.g.*, Kalyani Munshani, *Security Concern or Economic Motivations? The Regulation of Informal Value Transfer Systems*, 12 OR. REV. INT'L L. 77, 78-79 (2010) (examining the response of financial institutions after the PATRIOT Act placed new mandatory reporting requirements on banks as well as on money services businesses like MoneyGram); Navin Beekarry, *The International Anti-Money Laundering and Combating the Financing of Terrorism Regulatory Strategy: A Critical Analysis of Compliance Determinants in International Law*, 31 NW. J. INT'L L. & BUS. 137, 137 (2011).

303. A. Mitchell Polinsky & Steven Shavell, *Mandatory Versus Voluntary Disclosure of Product Risks*, 28 J.L. ECON. & ORG. 360, 361 (2012).

304. *Id.* at 361-62.

305. Cynthia Estlund, *Just the Facts: The Case for Workplace Transparency*, 63 STAN. L. REV. 351, 353-54 (2011) (referring to disclosure mandates as "a comparatively market-friendly form of state intervention").

information voluntarily anyway, making mandatory disclosure requirements superfluous.[306] In contrast, Fishman and Hagerty's model concludes that a mandatory disclosure regime would be more beneficial than a voluntary disclosure regime when the disclosed information is hard to understand.[307] Once disclosed, intermediaries that assist with processing the disclosed information can make the difficult material easier to consume and understand.[308]

Some of the literature focuses on mandatory versus voluntary substantive regulations instead of information disclosure. Depending on the situation, mandatory regulations may be more efficient than voluntary regulations.[309] Shapiro and Rabinowitz conclude that a voluntary compliance program for OSHA would be less successful than a voluntary compliance program administered by the EPA because of the differences between issues affecting the environment and issues affecting occupational safety.[310]

Because the efficiency of voluntary versus mandatory approaches may be context-dependent, some flexibility may be desirable. However, the flexibility should be handled very carefully so that the degree of regulation is optimal. If the regulations are easy to avoid, then firms will likely argue that they fall within an uncovered category. For this reason, broadly applicable regulations can be desirable. In the context of taxes, the Ramsey intuition emphasizes establishing a broad tax base that applies to everyone, rather than allowing too many exceptions to be carved out of the tax law.[311] But as long as a regulatory program is always mandatory for some firms, there will likely be positive effects, including spillovers. The work of Short and Duane suggests that there may be some spillover effects between mandatory and voluntary environmental

306. Michael J. Fishman & Kathleen M. Hagerty, *Mandatory Versus Voluntary Disclosure in Markets with Informed and Uninformed Customers*, 19 J.L. ECON. & ORG. 45, 47 (2003).

307. *Id.* at 45.

308. Estlund, *supra* note 305, at 355.

309. Wu & Babcock, *supra* note 300, at 158; Ta, *supra* note 301, at 765-66; Sidney A. Shapiro & Randy Rabinowitz, *Voluntary Regulatory Compliance in Theory and Practice: The Case of OSHA*, 52 ADMIN. L. REV. 97, 100 (2000) ("Analysts suggest that voluntary regulatory compliance may be more efficient than traditional command and control regulatory approaches because it can produce the same (or more) protection at lower cost.").

310. Shapiro & Rabinowitz, *supra* note 309, at 100-01.

311. Ian Ayres & Paul Klemperer, *Limiting Patentees' Market Power Without Reducing Innovation Incentives: The Perverse Benefits of Uncertainty and Non-Injunctive Remedies*, 97 MICH. L. REV. 985, 991 (1999).

programs, where firms that are not required to adopt certain "best practices" required of others may nonetheless adopt those practices for a variety of reasons.[312] In the following subsections, we will explore how these principles would apply in the context of cybersecurity.

1. *Voluntariness and Information Sharing*

Currently, voluntary programs are emphasized by the proposed solutions to the problems facing cybersecurity professionals. The CEA and NCPA both strongly emphasize the voluntariness of private sector participation.[313] As discussed in the case study above, the voluntary program of CISPA focuses on information disclosures instead of the adoption of best practices. Because CISPA permits but does not require private firms to disclose cybersecurity threat information to the government, some might argue that a voluntary disclosure program would be more protective of privacy than a mandatory disclosure program. However, in Section III.D, we referenced the illegal wiretapping controversy as an example of when a voluntary information-sharing program is not protective of privacy and civil liberties. The wiretapping example illustrates that voluntariness is not a sufficient condition for the protection of privacy.

Moreover, a voluntary program may have less structure imposed on disclosures, leading to a greater risk of overshare and thus a greater risk to privacy, as compared to a mandatory program that requests very specific types of information. There is a clear need for controls in the information-sharing context to prevent overshare, but CISPA currently lacks such controls. Under proposed § 1104(c)(5), CISPA would require the government to notify the sharer if some of the shared information was not "cyber threat information."[314] The destruction of this extraneous information is not addressed, nor does CISPA suggest how such oversharing might be deterred. For example, should oversharing firms be required to disclose the overshare to their customers?

312. Short & Duane, *supra* note 300, at 99.

313. National Cybersecurity Protection Act of 2014, Pub. L. No. 113-282 128 Stat. 3066; Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274 128 Stat. 2971.

314. Cyber Intelligence Sharing and Protection Act, H.R. 234, 114th Cong. § 3 (2015).

Polinsky and Shavell note that some economic models would expect firms to have less information when disclosures are mandatory because the firms have an incentive to not investigate matters that might have to be disclosed.[315] However, in the cybersecurity context, firms have a significant stake in the security of their systems and would therefore be likely to investigate possible vulnerabilities even if those vulnerabilities would then have to be disclosed. Accordingly, we do not believe that a mandatory disclosure regime for vulnerabilities would lead to firms having *less* knowledge of vulnerabilities.

The conclusions from Fishman and Hagerty's model suggest that mandatory disclosure regimes would be appropriate when information is difficult to understand.[316] Because of the complicated nature of cybersecurity matters, we believe that cybersecurity is a context where a mandatory disclosure regime would be more beneficial to the public than a voluntary disclosure regime. A mandatory disclosure regime could also expand the market for intermediaries who specialize in explaining the significance of vulnerabilities, exploits, and other cybersecurity issues.

Companies would rightfully be concerned about the possible harms to reputation from sharing information about specific vulnerabilities. The reality is that victims of cyber intrusions do not like to admit that their systems have been compromised. Statistics compiled by the Computer Security Institute of San Francisco in 2002 indicated that 90% of surveyed companies experienced computer security intrusions, but only 34% stated that they notified law enforcement about the intrusions.[317] In 2004, the Computer Security Institute and the FBI published a report concluding that only 20% of companies reported intrusions to law enforcement.[318] Vulnerability to cyberattacks may be viewed as a weakness that many companies do not want to reveal to their competitors.

For this reason, we suggest that most cybersecurity data intended for sharing within the circle of trust should be anonymized and aggregated, in addition to all of the information being carefully maintained by a trusted third party. This approach could be informed by the approaches taken with regard to employment compliance

315. Polinsky & Shavell, *supra* note 303, at 361.

316. Fishman & Hagerty, *supra* note 306, at 45.

317. Jason Krause, *Hack Attack*, 88 A.B.A. J. 51, 52 (2002).

318. LAWRENCE A. GORDON ET AL., CSI/FBI COMPUTER CRIME AND SECURITY SURVEY 13 fig.20 (2004), *available at* http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf.

practices. As Estlund notes, much of the information that employers are required to disclose about employment compliance practices is made available in aggregate form, making the details less identifiable while still preserving the usefulness of the information.[319] The public rarely, if ever, has access to firm-level data about employment compliance issues.[320] This sort of model could be applied in the cybersecurity context by anonymizing disclosure information and emphasizing aggregated information, such as how many vulnerabilities were reported by each sector and how often the same vulnerabilities were identified by different firms. Anonymizing and aggregating this information could also help to allay privacy concerns. Further, analysis of aggregated and anonymized cybersecurity information across several sectors could be useful for tracing patterns of vulnerabilities and exploits.

Under a regime that emphasizes voluntary disclosure of vulnerabilities, companies that experience intrusions or discover vulnerabilities will conduct a cost–benefit analysis. The firm is likely to disclose information when the benefits of disclosure outweigh the costs, but is likely to stop disclosing and exit the program as soon as the costs outweigh the benefits. On the cost side, the firm will be concerned about the negative publicity and possible reputational harm from disclosure. On the other hand, if there is a failure to disclose that later is discovered, this could cause even more harm to the company's reputation. On the benefits side of the equation, the company will consider possible benefits of disclosure, such as subsequent assistance by experts and the government resulting in a reduced chance of being attacked in the future. However, a survey revealed that one in four IT or security executives has a very low level of confidence in the government's ability to prevent or deter cyberattacks.[321] Thus, some companies may expect very few benefits to accrue from disclosing vulnerabilities, and the costs of disclosure will seem to outweigh the benefits.

The degree of possible reputational harm and legal liability is even greater in the case of the most egregious attacks, which could create a perverse incentive for lower rates of disclosure when a vulnerability could result in the most harm. Additionally, because not everyone has to disclose in a voluntary disclosure regime, those that

319. Estlund, *supra* note 305, at 396.

320. *Id.*

321. STEWART BAKER, SHAUN WATERMAN & GEORGE IVANOV, IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR 26 (2010), *available at* https://www.dsci.in/sites/default/files/NA_CIP_RPT_REG_2840.pdf.

do disclose vulnerabilities will stand out, thus exacerbating possible reputational harm and turning the company into an attractive target for future attacks.

A mandatory disclosure regime is likely to still result in some reputational harm, though the disclosures no longer stand out as much as they would in a voluntary regime. Because confidence in government may be low and providers may be unwilling to share information about security intrusions, a purely voluntary information-sharing program may be ineffective. Thus, a broad voluntary information-sharing program that includes personal information may be harmful to privacy and civil liberties, but even a narrow voluntary information-sharing program that is limited to vulnerability information may still be undesirable for entities that do not want to have that information released publicly. On the other hand, a compelled disclosure program is likely to still result in some reputational harm, and thus is likely to be opposed by the operators of critical infrastructure to whom it would apply. Giving control of this program to a trusted third party may mitigate some of these concerns, but it is not a panacea.

When discussing which type of regime would be optimal, we must first determine what the options are. The possibilities can be visualized as a matrix with voluntariness on one axis and identification on the other.

	Voluntariness	
Identification	Voluntary Open	Compelled Open
	Voluntary Anonymized	Compelled Anonymized

Policy makers who are calling for a model that emphasizes information sharing are currently focusing on voluntary open disclosure regimes. The clearest alternative to a voluntary disclosure regime is a compelled disclosure regime, but such a regime could still have negative effects on the reputations of private companies. A

third option is for anonymized compelled disclosures, as we suggest above. Under such a system, financial institutions could be identified by a prefix like FI and then assigned a number. Thus, required disclosures of cyber threat information would be associated with an anonymized identifier, potentially mitigating reputational harm to the provider, but while still ensuring that vulnerability information is made public. However, the reduction in reputational harm to companies from anonymized disclosures is offset by the harm to consumers who are denied information about specific companies and thus who are limited in their ability to seek redress if they are injured by the provider's substandard procedures. A voluntary anonymized disclosure regime would have benefits and risks similar to that of the compelled anonymized disclosure regime.

The importance of considering the needs of consumers leads us to a fifth option for an information-sharing regime: voluntary open, with disclosures resulting in mitigation of liability. CISPA uses this sort of modified voluntary approach. Under this approach, companies would disclose vulnerability information without compulsion, and the disclosure would result in a reduction of possible liability. This sort of mitigation approach is reflected in proposed § 1104(b)(4) of CISPA, which provides covered entities with exemption from liability for actions taken concerning cyber threat information.[322] However, we think that CISPA's provisions go too far by only requiring actions in "good faith" and not including an exception for gross negligence. If a company is grossly negligent with regard to either its cybersecurity program or the handling of customer information, providing an exemption from liability purely because this negligence was disclosed would run counter to the best interest of the consumer. Thus, while CISPA's model of "voluntary open disclosure plus liability exemption" may address some of the concerns of the service providers, its breadth would ultimately not be favorable to consumers.

We suggest that Congress should adopt more detailed regulations to remove loopholes that might allow for abuse of information-sharing procedures. This regulation should also emphasize two of the alternatives that we suggested above: anonymized compelled disclosure and open voluntary disclosure with mitigation. The model of open voluntary disclosure with mitigation would be more appropriate for industries that handle a

322. Cyber Intelligence Sharing and Protection Act, H.R. 234, 114th Cong. § 3 (2015).

large volume of low-sensitivity information. Anonymized mandatory disclosure may be more appropriate for industries that are at higher risk or that would be the most disrupted by cyberattacks. Regardless of whether the firm's identity is revealed or anonymized, all consumer information should be redacted or anonymized. If specific information about an individual is needed, as Chief Justice Roberts succinctly said in the recent case of *Riley v. California*, "get a warrant."[323]

2. *Voluntariness and the Adoption of Cybersecurity Standards*

The Cybersecurity Framework is a voluntary program for the adoption of best practices, but[324] a purely voluntary regime governing the adoption of cybersecurity protections is problematic because of the danger of inconsistent implementation. Shapiro and Rabinowitz warn that voluntary standards may be less protective or go after the lowest common denominator.[325] While all providers do not need to be using identical protections, the protections should be reasonable substitutes for each other. If one provider uses the technological equivalent of fishnet while another uses the technological equivalent of iron bars, the broadest benefits might not be realized.

Because a purely voluntary regulatory program may be less efficient than a mandatory program in some situations, we urge policy makers to consider adding a mandatory element to the Cybersecurity Framework. As we discuss in Section IV.C, this could be done by requiring adoption by the entities found to be at highest risk. Currently, the CEA prohibits the NIST from requiring any specific solutions or technologies as part of its voluntary cybersecurity standards,[326] and this prohibition preempts any mandatory element for the Cybersecurity Framework. We thus

---

323. 134 S. Ct. 2473, 2495 (2014).

324. *But see* Trope & Humes, *supra* note 102, at 725-27 (arguing that the Order is not truly voluntary because companies would be subject to pressure from the market to comply, and because a truly voluntary framework would not involve evaluations of those who adopt said framework). We disagree with this position. If the market wants companies to adopt the Framework, that does not mean that guidelines from the government are mandatory. Additionally, the process of evaluating the implementation of the Framework provides benefits to the company that adopts it, so we disagree with the assertion that there is no reason to evaluate compliance with a voluntary standard.

325. Shapiro & Rabinowitz, *supra* note 309, at 137.

326. Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, § 101, 128 Stat. 2971, 2972.

encourage the 114th Congress to reconsider this prohibition. The existence of a mandatory program could also contribute to spillover among the voluntary participants, who become better educated about risks through their association with adherents of the mandatory program, and who may also choose to adopt the best practices in case their firm is later found to be at highest risk. Thus, while we would not recommend making the entire Framework mandatory for all possible participants, we anticipate that there is a significant benefit to be gained from giving the Cybersecurity Framework some mandatory elements.

The danger of proceeding with cybersecurity standards on a purely voluntary basis is especially pronounced in critical infrastructure and SCADA systems. According to Symantec, there were fifteen publicly known SCADA vulnerabilities in 2010 and 129 publicly known SCADA vulnerabilities in 2011.[327] This is not counting undiscovered zero day vulnerabilities, like the four such vulnerabilities that were exploited by Stuxnet. This is not an area for a casual, "Do your best" type of approach. But instead of proposing that all critical infrastructure be legally obligated to adhere to the standard, we would limit the mandatory adoption requirement to critical infrastructure providers found to be at greatest risk of catastrophic damage, an analysis already required under the Order. We feel that this approach strikes a good balance between safety and permitting private companies to continue to make system decisions based on their individual needs. The possibility that the firm may eventually have to comply may also contribute to the spillover effect and increase the participation level even among firms that are not currently required to comply.

If the standards remain purely voluntary, compliance with voluntary cybersecurity standards could be buttressed with provisions aimed at mitigation, like the modified voluntary-open information-sharing proposal presented above. In such a situation, voluntarily adopting the approved standard could reduce civil liability. An analysis applying game theory to interactions between a private firm and a regulator concluded that penalties should be mitigated for firms that engage in good faith self-policing.[328] This model focused on penalties imposed by regulators, but the principle

327. SYMANTEC, INTERNET SECURITY THREAT REPORT: 2011 TRENDS 41 (2012), *available at* http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf.

328. Jay P. Kesan, *Encouraging Firms to Police Themselves: Strategic Prescriptions to Promote Corporate Self-Auditing*, 2000 U. ILL. L. REV. 155, 172.

could also apply to civil liability, which is really just a private governance method of imposing noncompliance penalties. The effect on liability could alternatively be framed in terms of noncompliance, where noncompliance with a standard could be admitted as evidence of negligence.[329] This approach is thematically similar to the doctrine of *negligence per se* in tort law. However, *negligence per se* typically only applies to laws that are mandatory, so the analogy is not perfect.

Even with a component aimed at reducing liability, a voluntary security program would still permit companies to externalize the costs of their noncompliance, and these costs are then borne by their competitors or by society at large.[330] A voluntary system also allows participants to exit the program if the benefits no longer exceed the costs. Thus, a voluntary program may result in higher costs and lower participation. We anticipate that a mandatory regulatory approach would eventually become accepted by firms as a cost of doing business, provided that the enforcement mechanisms are effective, the regulations apply equally to all firms in a specific sector, and the mandates are not excessively stringent.[331] Collaboration between the government and the private sector to shape these mandates could help ensure that these elements are present. Thus, it may be desirable to eventually transition to a mandatory protection system that is designed by giving substantial consideration to the perspectives of the firms that would be implementing it. But for now, it would be a good starting point to limit mandatory protection requirements to critical infrastructure operators at highest risk, while providing liability mitigation for voluntary adoption of the standard by all other covered entities.

B. Changes to CISPA

To strengthen CISPA's compatibility with our circle of trust framework, we now examine the possibility of amending some of CISPA's language. Even though we encourage a shift away from a

---

329. Shapiro & Rabinowitz, *supra* note 309, at 153 (noting that the danger of tort liability might provide incentives for voluntary compliance).

330. *Id.* at 104 ("A firm also is less likely to recoup its abatement costs if its competitors do not take similar safety or health precautions.").

331. *See* Munshani, *supra* note 302, at 97-98, 105-08 (discussing banks' support of financial regulations in the PATRIOT Act that they previously opposed when the regulations would only have applied to banks instead of other money services like Western Union and MoneyGram).

purely voluntary approach to information sharing, the changes to CISPA that we propose are limited to the current and purely voluntary version of CISPA. Because CISPA was introduced in much the same form in both the 112th Congress and 113th Congress,[332] and the version in the 114th Congress was introduced with no changes made from the version that passed the House in the 113th Congress,[333] this Section includes specific recommendations for CISPA's language because of its resilience throughout the three most recent sessions of Congress. Recommendations contained in this Section can also serve as a guide for other cybersecurity bills.

1. *Provisions of CISPA to Preserve with Few Changes*

There are a number of beneficial provisions of CISPA that make valuable contributions to the legal framework and that would provide valuable support for the establishment of a circle of trust. One of these is proposed § 1104(a), which would create a way for members of the private sector to obtain security clearances so that government agencies can share classified cyber threat intelligence with qualifying members of the private sector.[334] The limits on secondary disclosure of this information are addressed in proposed § 1104(a)(5). By keeping the information within the circle of trust, secrets held by the government and any private information of citizens that might be found within that information stay secure. The security clearance provision of CISPA is superior to the security clearance provision of the NCPA because the NCPA language only singles out members of public-private partnerships and owners and operators of critical infrastructure for eligibility.[335] Unlike the NCPA, CISPA's security clearance provisions are broader, allowing security clearances to be issued to employees, independent contractors, or officers of a covered entity.[336] By doing so, CISPA recognizes that making classified cybersecurity information available to those on the

332. *Compare* Cyber Intelligence Sharing and Protection Act, H.R. 3523, 112th Cong. (2012), *with* Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. (2013).

333. *Compare* Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. (2013), *with* Cyber Intelligence Sharing and Protection Act, H.R. 234, 114th Cong. (2015).

334. H.R. 234 § 3.

335. National Cybersecurity Protection Act of 2014, Pub. L. No. 113-282, § 7, 128 Stat. 3066, 3070.

336. H.R. 234 § 3.

ground is likely to be more valuable than granting clearances based on traditional bureaucratic structure.

Other important sections include proposed § 1104(d), which creates a civil cause of action against the government if voluntarily disclosed information is misused, and proposed § 1104(f)(5), which is a savings clause that explicitly prohibits the government from imposing liability on private entities that elect to not participate in the voluntary sharing program. Section 2 of the bill, which imposes reporting requirements on agencies concerning how the voluntarily shared information is used, is also vital because it keeps agencies accountable for use of information received from the private sector.

In the previous section, we urged that this should not be a purely voluntary regime. Our analysis of law and economics research has led us to conclude that mandatory disclosure regulations might actually be more protective of civil liberties than voluntary disclosure regulations in some contexts because the information collected would not depend on the whims of the information holders. However, we recognize the value of voluntary programs, especially in a context where public opinion is still uncertain. For this reason, we largely approve of CISPA's provisions that support the "open voluntary with mitigation" model that we proposed above.

2. *Amending CISPA to Address Privacy Concerns*

We analyzed all provisions of CISPA to identify the provisions that are the most and least consistent with our circle of trust framework, and in this Subsection, we will emphasize substantive provisions that should be deleted to make CISPA more compatible with our proposed legislative framework. First, we recommend striking the two instances of "Notwithstanding any other provision of law" within proposed § 1104(b)(1).[337] Above, we argued that the "notwithstanding" language, while troubling, ultimately does not significantly undermine current privacy law because current privacy law is itself inadequate.[338] However, if the underlying privacy laws are improved, especially the SCA, the "notwithstanding" provision of CISPA would limit the effectiveness of any such improvements. The "notwithstanding" language is also found in the Cyber Threat Sharing Act based on President Obama's legislative proposal

337. *Id.*
338. *See supra* Subsection II.D.2.b.

announced by the White House in January 2015, and should likewise be removed from that bill.[339]

Second, while we support the exemption from liability under an "open voluntary with mitigation" model, the exemption from liability in proposed § 1104(b)(3) should be limited. This section currently eliminates any means of redress that otherwise might be available to aggrieved parties against the private entities disclosing the customers' information, and the way it is written does not take the interests of consumers into account.[340] If the information that moves from the private sector into the central circle of trust is collected on a voluntary basis, the current broad exemption from liability removes any disincentive for careless overshare. For private consumers to reap the most benefits from the voluntary nature of CISPA's information-sharing provisions, companies should be encouraged to weigh the interests of their customers when deciding both *what* and *how much* information to disclose to the government. If companies receive a blanket immunization from liability, they have no incentive to be discerning about the disclosures. Our most modest proposal for amending this subsection is to eliminate the phrase "or for sharing such information in accordance with this section"[341] and adding a requirement that the entity act not only in good faith but with the use of the best available detection technology. The added requirement of best available detection technology overlaps with the Cybersecurity Framework and would help to mitigate the threat of false positives. This could reduce instances of customer information being disclosed "in good faith" when it did not actually implicate any cyber threat information. The exemption should also not cover negligent behavior. Thus, our amended version of proposed § 1104(b)(3) would read as follows:

(3) EXEMPTION FROM LIABILITY—

> No civil or criminal cause of action shall lie or be maintained in Federal or State court against a protected entity, self-protected entity, cybersecurity provider, or an officer, employee, or agent of a protected entity, self-protected entity, or cybersecurity provider, acting in

339. S. 456, 114th Cong. (2015); Information Sharing Legislative Proposal, *supra* note 80, at § 103(a).

340. H.R. 234, § 3.

341. *Id.*

good faith, non-negligently, and with the use of the best available cybersecurity and detection technology—
(A) for using cybersecurity systems to identify or obtain cyber threat information; or
(B) for decisions made based on cyber threat information identified, obtained, or shared under this section.

Additionally, having struck the "notwithstanding any other provisions of law" provisions of proposed § 1104(b), this section should be amended to recognize that information shared under CISPA comes within the scope of the protections of the Stored Communications Act and other privacy laws. Thus, we recommend amending proposed § 1104(b)(4) to read as follows:

(4) Relationship to other laws requiring the disclosure of information.
(A) The submission of information under this subsection to the Federal Government shall not satisfy or affect—
(i) any requirement under any other provision of law for a person or entity to provide information to the Federal Government; or
(ii) the applicability of other provisions of law, including section 552 of title 5, United States Code (commonly known as the 'Freedom of Information Act'), with respect to information required to be provided to the Federal Government under such other provision of law.
(B) Information sharing under this subsection is subject to the protections and exceptions of other laws that regulate and protect privacy, including but not limited to the Fourth Amendment to the United States Constitution, the Stored Communications Act of 1986 (18 U.S.C. §§ 2701–2712), the Wiretap Act (18 U.S.C. §§ 2510–2522), and the Health Insurance Portability and Accountability Act of 1996 (Pub. L. 104-191).

As we noted in our analysis above, the Stored Communications Act would likely permit voluntary information sharing under the

emergency exception of § 2702, and the application of the Fourth Amendment is currently unclear.[342] Thus, while bringing CISPA within the scope of sector-specific privacy statutes will contribute to the protection of certain categories of sensitive information, it should remain largely unaffected due to the lax approach that privacy laws of broader application take with respect to the Internet. Nevertheless, adding this provision leaves room for the Supreme Court or Congress to increase the protections for information transmitted online without leaving a large CISPA-sized gap in the protections. If the SCA as currently enacted does not protect this information adequately, as we suggest with our analysis of the emergency exception of § 2702, amendments to the SCA will be necessary. As written, the voluntary sharing provisions of CISPA are consistent with statutory precedent, and the civil liberties and personal privacy issues that this raises should be addressed by amending that statutory precedent and thus closing the door for future abuses. If the information-sharing regime becomes mandatory, then § 2703 of the Stored Communications Act will likely apply, and cybersecurity legislation that looks to create a mandatory information-sharing regime would also have to amend § 2703.

In the interests of protecting privacy and making the circle of trust more trustworthy, Congress should also amend paragraph 5 of subsection 1104(c). This section requires the government to notify a disclosing entity if the disclosed information does not fit the definition of "cyber threat information."[343] Putting the private party on notice that it is disclosing information outside the scope of the statute is very important because these disclosures could potentially lead to additional liability concerns for the disclosing party. However, this provision does not address what the government may then do with the "non-cyber threat information" so received and does not propose any method for deterring overshare. Because this interferes with the effectiveness of the circle of trust, we urge that this potential loophole be closed by requiring the destruction of such information and requiring the oversharing entity to notify customers that it disclosed more information than necessary. Thus, proposed § 1104(c)(5) should be amended to read as follows:

(5) NOTIFICATION AND DISPOSITION OF NON-CYBER THREAT INFORMATION— If a department

342. *See supra* Section II.D.
343. H.R. 234, § 3.

> or agency of the Federal Government receiving information pursuant to subsection (b)(1) determines that such information is not cyber threat information, such department or agency shall:
> (A) notify the entity or provider sharing such information pursuant to subsection (b)(1);
> (B) be prohibited from any use of this information;
> (C) promptly destroy any information that is voluntarily disclosed pursuant to subsection (b)(1) and fails to meet the definition of "cyber threat information" set forth in subsection (h)(4); and
> (D) require the entity or provider to give notice to the customers whose information may have been included in the extraneous disclosure.

In most cases, we expect that disclosure of personally identifiable information or other information included in proposed § 1104(c)(4) would also fall within § 1104(c)(5) as non-cyber threat information. Accordingly, not only could the federal government not use this type of information under (c)(4), but it would also have to notify the disclosing firm and destroy the disclosed copies of the sensitive personal information. The Cyber Threat Sharing Act of 2015 partially implements this recommendation by requiring the destruction of disclosed information that is not a cyber threat indicator, but it does not require the government to notify the discloser.[344]

We also recommend revising several of CISPA's definitions in the interest of narrowing the scope and protecting the privacy of citizens. To better address personal privacy concerns and increase intersectoral trust, "cyber threat information" should be redefined in a more limited fashion to limit the information that can be shared with the government, such as by explicitly stating that information so disclosed may not include any personally identifiable information and clarifying that malware and source code are the intended targets of this disclosure. We also recommend limiting the parts of the definition that refer to "efforts," which could encompass merely talking about something on social media, to explicitly refer to actions leading towards actual incidents. The definition for "cyber threat

344. S. 456, 114th Cong. (2015).

intelligence"[345] may be kept largely as it is, except with the addition of explicit references to malware and source code.

The voluntary sharing provision of CISPA permits private entities to share information for a "cybersecurity purpose[]."[346] The definition for this term is broad in much the same way as the definition for cyber threat information, and thus should be narrowed accordingly in the interest of protecting consumer privacy. This means including a prohibition on including personally identifiable information, limiting references to "efforts," and inserting a provision addressing malicious source code and malware.

C. Suggestions for the Cybersecurity Framework

Having examined possible changes to the language of CISPA, we turn now to our recommendations for the implementation of the Cybersecurity Framework. The Order permits the government to share cyber threat intelligence with qualified members of the private sector and also urges the creation of voluntary compliance standards for cybersecurity in the form of the Cybersecurity Framework. In this Section, we present recommendations for an approach to the Cybersecurity Framework and similar legislative efforts.

In setting out the policy of the Order, § 1 emphasizes the need to "collaboratively develop and implement risk-based standards."[347] This standard-setting approach is what we would classify as technology forcing, but it is also a technology-neutral approach to improving cybersecurity.[348] The Cybersecurity Framework currently has the potential to create mandatory demand for cybersecurity products. The Renewable Fuel Standards (RFS) program of the federal government is an example of an existing program that creates mandatory demand for relatively new energy products, and as the empirical work of Kesan, Slating, and Yang suggests, this mandatory demand appears to have a positive effect on the industry.[349] By generating mandatory demand, the RFS program appears to assist the

345. *See id.*

346. *Id.*

347. Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13,636, § 1, 78 Fed. Reg. 11,739, 11,739 (2013).

348. *See* Jay P. Kesan & Rajiv C. Shah, *Shaping Code*, 18 HARV. J.L. & TECH. 319, 333 (2005).

349. Jay P. Kesan, Timothy A. Slating & Hsiao-Shan Yang, *Mandatory Demand as a Policy Instrument: The Case of the Renewable Fuel Standard (RFS) Biofuel Program* (Ill. Pub. Law & Legal Theory, Research Paper No. 11-24, 2012), *available at* http://papers.ssrn.com/pape.tar?abstract_id=2083698.

development of the market, improving competition between the firms and contributing to the growth of economies of scale.[350]

In addition to alternative fuels, this sort of government intervention can also be observed in the information technology sector. Technology-forcing approaches in the information technology sector may often be more efficient than regulation that relies on purely market-based incentives.[351] Technology-forcing regulations may also be especially appropriate in areas where the focus is on concerns about safety.[352] However, technology-forcing regulations are sometimes uncertain because it is impossible to predict how a given area of technology will develop. Addressing this problem may require an ongoing dialogue between the public and private sectors concerning state-of-the-art technologies.[353] Our proposed circle of trust framework would provide a constructive environment for that ongoing dialogue.

The Order emphasizes that the Cybersecurity Framework will set cybersecurity standards. There are three main options for standards that regulations can adopt: (1) Performance standards, which do not specify required technology but instead describe how the technology should operate; (2) Design standards, which explicitly state how a technology must operate; and (3) Best available technology (BAT) standards, which require the adoption of the best technology available and thus provide flexibility for future technological developments.[354] Adoption of a BAT standard would generally require entities to upgrade their systems as better technologies become available. Performance standards allow the most deference to the market in terms of determining the final technology.[355] Thus, a BAT standard is desirable when the greatest emphasis is placed on technology, and a performance standard is desirable when the end goal is to let the market determine the best implementation. The Clean Air Act is an example of a regulatory regime that largely adopts BAT standards, with the focus of the CAA being on gradually removing a harm.[356]

The flexibility of a BAT standard would be consistent with the Order's stated focus of the Cybersecurity Framework as being risk-

350. *Id.*
351. Kesan & Shah, *supra* note 348, at 338.
352. *Id.*
353. *Id.* at 334.
354. *Id.* at 340-41.
355. *Id.* at 340.
356. *See id.* at 341.

based and technology neutral. A performance standard would also be consistent with the approach stated in the Order. A design standard would likely be inconsistent with this approach, as it would require more detail concerning technology implementations and would not be easily adaptable.[357] Either a performance standard or a BAT standard would also control for one of the major possible downsides of technology-forcing regulation by providing a more open-ended approach to technology that does not require the government to employ precognitive abilities to determine how future cybersecurity technologies will develop. The current version of the Cybersecurity Framework indicates that the standard will be performance-based, and the language emphasizes "best practices."[358] While this may raise questions about whether the Cybersecurity Framework is ultimately more of a BAT standard or a performance-based standard, this at least ensures that it will have more flexibility than a design standard.

Many more factors must be considered in addition to the basic approach that will be taken. There are two sides in any market: a supply side and a demand side. As some empirical work shows, mandating demand can aid in the development of a fledgling industry.[359] Discussions of regulatory approaches often invoke the familiar idiom of "carrots and sticks," where "carrots" are offered as positive consequences for compliance and "sticks" are offered as negative consequences for noncompliance.[360] Mandating demand in the cybersecurity context could involve a "stick" approach, such as a requirement that all operators of networks over a certain size implement cybersecurity protections or face sanctions. A "carrot" approach to mandating demand might instead provide tax breaks or tax credits for companies that adopt adequate cybersecurity technology. Greater demand means that the producers of cybersecurity technologies would sell more products. However, this alone may not encourage improvements in cybersecurity technology.

---

357. It may be possible to have a technology-forcing design approach in the cybersecurity context that is technology neutral. For example, such an approach might set a deadline by which time a service provider would have to show that they can successfully repel 98% of attacks.

358. *See* NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 1 (2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

359. Kesan, Slating & Yang, *supra* note 349.

360. Gerrit De Geest & Giuseppe Dari-Mattiacci, *The Rise of Carrots and the Decline of Sticks*, 80 U. CHI. L. REV. 341, 354-55 (2013).

Thus, we recommend also adopting regulations aiming at the supply side of the cybersecurity market.

Regulating the supply side can also either be done through a carrot or stick approach. A stick approach to the cybersecurity issue could be similar to the way that the National Highway Traffic Safety Administration (NHTSA) approached automobile safety in the 1960s. The NHTSA's performance-based requirement that manufacturers produce a "'passive occupant restraint system'" led to the development of air bags, which have since become a standard safety measure in all automobiles.[361] A carrot approach could utilize a competition where the winner's product is guaranteed to be purchased. This guaranteed purchaser option is an approach that has been examined in the context of vaccine development[362] and may also be applicable for spurring R&D in cybersecurity.

Either a carrot or stick approach could be effective at incentivizing the supply side. The NHTSA example shows that using a stick approach for the supply side may encourage the development of technologies for protecting consumers, so this method of approach might be effective for cybersecurity research. With such an approach, cybersecurity companies might be given a deadline for developing a passive cyber defense system that facilitates quick recovery from attacks. A carrot approach is likely to be attractive because it would require a lighter regulatory touch and thus involve less government interference with the market. A guaranteed purchaser approach to cybersecurity could include a contest where the prize is that the government will purchase a large number of copies of a winning cybersecurity solution that is able to detect, repel, and repair damage from the highest number of threat categories. In addition to incentivizing innovation, the large scale government purchase could then be repurposed to distribute the winning technologies to the sectors most in need of the strongest cybersecurity protection. Further research should be conducted to determine whether the supply side for cybersecurity products would be better encouraged by a carrot or stick approach to regulatory intervention.

Our initial expectation on this point is that a carrot approach may be more effective at incentivizing innovation on the supply side.

---

361. Kesan & Shah, *supra* note 348, at 337.

362. *See* MICHAEL KREMER & RACHEL GLENNERSTER, STRONG MEDICINE: CREATING INCENTIVES FOR PHARMACEUTICAL RESEARCH ON NEGLECTED DISEASES 42 (2004). *See generally* Kyle Wamstad, *Priority Review Vouchers—A Piece of the Incentive Puzzle*, 14 VA. J.L. & TECH. 126 (2009).

We thus propose that an effective model for the Framework would require the adoption of best practices, and simultaneously provide supply-side incentives in the form of contests and guaranteed government purchases. This best practices approach, combined with encouraging continual improvement in these technologies, will ensure that entities that adopt the Framework will be obligated to not allow their security systems to become outdated while ensuring that better technologies will be made available under a reliable timeline.

While recognizing that the Order has limited legal authority, we ultimately disagree with the Order's emphasis on purely voluntary adoption of the Framework. Telling our nation's critical infrastructure providers "Do the best you can" is not always going to be enough. In some situations, voluntary participation may be sufficient, and offering government support in exchange for participation may sometimes provide adequate incentive. But when a critical infrastructure provider is deemed to be at greatest risk for an intrusion that could cause catastrophic harm, this provider's participation in the Framework should be mandatory. The Order already requires the identification of critical infrastructure providers at greatest risk. In Section IV.A, we argued that it would be appropriate to take this identification a step further and require identified providers to adopt the Framework.

Ultimately, our recommendations for the Cybersecurity Framework would likely require concurrent congressional action to be effective. The NCPA and CEA represent initial steps in codifying congressional support for the Cybersecurity Framework and PPD-21, but the narrow language of both of these enacted statutes interferes with the creation of a circle of trust. Thus, policymakers should continue to evaluate cybersecurity standards and ways to promote public-private cooperation on this topic. The Order includes a number of good ideas, and in this Section, we have provided three suggestions for how to implement these good ideas in a meaningful way: (1) Adopt a flexible standard; (2) Offer supply-side and demand-side incentives; and (3) Make participation mandatory for providers at greatest risk. These recommendations emphasize security procedures that can be implemented with little to no deleterious effects on privacy and civil liberties, while also facilitating technological innovation.

CONCLUSION

Cybersecurity is a big deal. Protection of critical infrastructure is a matter of national security. The Obama Administration recognized this during President Obama's second term by issuing executive orders about cybersecurity in 2013 and 2015. Congress recognizes this as well, as indicated by the introduction of dozens of cybersecurity bills over the last several years and the enactment of several cybersecurity laws in the waning hours of the 113th Congress. Unfortunately, protecting cybersecurity has proven to be a much more partisan issue in Congress than it should be. Additionally, advocates for private enterprises discourage the imposition of meaningful cybersecurity requirements on privately owned critical infrastructure, while advocates for civil liberties and privacy react with alarm to regulation attempts that involve the collection of information about cyber threats. The resistance from both service providers and citizens indicates an alarming lack of intersectoral trust on the issue of cybersecurity.

Privacy and security are not mutually exclusive, but balancing the two interests may require cooperation and the occasional compromise. This Article focuses on CISPA and the Order to illustrate this quest for balance. Because such a quest will require tools, we propose a new conceptual information-sharing framework. We describe our framework as establishing a circle of trust, where information disclosed by the government and the private sector is ensured adequate protection and limitations on secondary use are well-established. A conceptual framework that balances privacy and security while permitting information sharing should emphasize intersectoral cooperation and the creation of this circle of trust.

Examining CISPA and the Order has permitted us to analyze the value of their respective voluntary regimes. We argue that a purely voluntary regime is undesirable in both contexts. Government intervention with the free market should be minimized, but when cybersecurity issues have implications for national security, some degree of mandatory regulation would be beneficial. Voluntary programs can be effective in some situations, but potential participants may interpret voluntary programs to be aspirational guidelines. In the sensitive context of cybersecurity, aspirational guidelines for security standards could lead to low levels of compliance and an ineffective regulatory regime, and aspirational guidelines for cyber threat information sharing could lead to the

withholding of valuable information by those who do not participate and a greater risk of overshare by those who do participate.

One advantage to having at least some mandatory element is that it is likely to have positive spillover effects that improve the status of actors covered by the voluntary program. A mandatory element may also enhance the circle of trust, insofar as it assures the voluntary participants that they will have ready access to the data that they need. A mandatory program also provides them with guaranteed peers who will be able to contribute new knowledge to partially mandatory standard adoption.

The Cybersecurity Framework and accompanying executive actions now have legislative support in the form of the NCPA and CEA, but these statutes do not embody our proposed circle of trust framework. CISPA could be easily revised to accompany the Cybersecurity Framework, operationalize the circle of trust framework, and fill in some of the gaps left by the new statutes without threatening privacy and civil liberties. A careful, deliberative process aimed at protecting cybersecurity and civil liberties must be implemented and tested within a reasonable timeframe, before the emergence of a cybersecurity crisis that causes us to suspend reason.