Loyola University Chicago Law Journal

Volume 47
Issue 2 *Winter 2015*

Article 4

2015

Sharing Shortcoming

Derek E. Bambauer

Sharing Shortcomings

*Derek E. Bambauer**

Current cybersecurity policy emphasizes increasing the sharing of threat and vulnerability information. Legal reform is seen as crucial to enabling this exchange, both within the public and private sectors and between them. Information sharing is due for some skepticism though, and this Essay (part of a symposium entitled Privacy in a Data Collection Society) attempts to provide it. Not only are there few real legal barriers to data exchange, but greater sharing will generate little benefit and will create significant privacy risks. This Essay creates a typography of vertical and horizontal information sharing, and argues that while top-down communication could be useful, it faces important practical impediments. The present focus on sharing increases the scope of the surveillance state unnecessarily and displaces more effective cybersecurity policy measures.

INTRODUCTION

Information sharing is trendy in American cybersecurity policy.[1]

* Professor of Law, James E. Rogers College of Law, University of Arizona. Thanks for helpful suggestions and discussion are owed to Jane Bambauer, Jennifer Granick, Dan Hunter, Thinh Nguyen, Sasha Romanosky, Peter Swire, Alexander Tsesis, Tal Zarsky, and the participants in Privacy in a Data Collection Society at Loyola University Chicago School of Law. The author welcomes comments at derekbambauer@email.arizona.edu.

Like all fads, however, the information-sharing trend would benefit from skeptical analysis to determine whether it is sustainable or evanescent.[2] This Essay argues that information sharing is overrated. As a method of improving cybersecurity, sharing is unlikely to produce meaningful benefits, and, indeed, generates potentially significant privacy harms.[3] Policymakers ought to treat it like the pet rock[4] rather than craft beer[5] as fads go, and shift their attention to more effective interventions.[6]

Information sharing is a major component both of recently enacted cybersecurity legislation and of bills pending in the current Congress. For example, in December 2014, President Barack Obama signed a series of bills intended to bolster security.[7] The National Cybersecurity Protection Act charges the Department of Homeland Security's (the "DHS") National Cybersecurity and Communications Integration Center with "Federal civilian interface for the multi-directional and cross-sector sharing of information related to cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities."[8]

---

1. *Cyber Security Bills Focus on Info Sharing*, BANKING EXCH. (May 19, 2015), http://www.bankingexchange.com/news-feed/item/5489-cyber-security-bills-focus-on-info-sharing; Denise E. Zheng & James A. Lewis, *Cyber Threat Information Sharing*, CTR. FOR STRATEGIC & INT'L STUD. (2015), http://csis.org/files/publication/150310_cyberthreatinfosharing.pdf. It has been popular in other contexts, such as national security, as well. *See, e.g.*, Peter P. Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 VILL. L. REV. 951 (2006).

2. *See* Amitai Aviram & Avishalom Tor, *Overcoming Impediments to Information Sharing*, 55 ALA. L. REV. 231 (2004) (assessing barriers to information sharing and evaluating when it is suboptimal); Sara Sorcher, *Obama's Info-Sharing Plan Won't Significantly Reduce Security Breaches*, CHRISTIAN SCI. MONITOR, http://passcode.csmonitor.com/influencers-infosharing.

3. *See* Joe Uchill, *Cybersecurity Pros Slam Threat Information-Sharing Bills*, CHRISTIAN SCI. MONITOR (Apr. 16, 2015), http://www.csmonitor.com/World/Passcode/2015/0416/Cybersecurity-pros-slam-threat-information-sharing-bills.

4. *See* Lindsay Bever, *Pet Rock Inventor Gary Dahl Dies at 78. He Put a Rock in a Box and Sold Millions*, WASH. POST (Apr. 1, 2015), http://www.washingtonpost.com/news/morning-mix/wp/2015/04/01/pet-rock-inventor-gary-dahl-dies-at-78/ (describing the pet rock as a "short-lived fad").

5. *See* Daniel Fromson, *Idea of the Week: Mapping the Rise of Craft Beer*, NEW YORKER (June 6, 2013), http://www.newyorker.com/news/news-desk/idea-of-the-week-mapping-the-rise-of-craft-beer.

6. *See* Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011 (2014) [hereinafter Bambauer, *Ghost in the Network*]; Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584 (2011) [hereinafter Bambauer, *Conundrum*]; Nathan A. Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503 (2013).

7. Eric Chabrow, *Obama Signs 5 Cybersecurity Bills*, BANK INFO SECURITY (Dec. 18, 2014), http://www.bankinfosecurity.com/obama-signs-5-cybersecurity-bills-a-7697/op-1.

8. National Cybersecurity Protection Act of 2014, Pub. L. No. 113-282, § 3, 128 Stat. 3066, 3067.

The bill also requires the DHS to submit, within six months, recommendations to Congress on how to speed up information-sharing agreements between the government and private sector.[9] Similarly, the Cybersecurity Enhancement Act of 2014 requires the National Institute of Standards and Technology to coordinate its cybersecurity efforts with Information Sharing and Analysis Centers, which are sector-specific entities that coordinate sharing of threats and vulnerabilities.[10] And the Federal Information Security Modernization Act of 2014 sets up an information-security incident center to coordinate information sharing among federal government agencies.[11]

Moreover, increasing threat-sharing remains a priority for both the Obama administration and Congress. In February 2015, the President issued an executive order designed to increase sharing by private entities with one another and, on a voluntary basis, with the federal government.[12] CISPA—the proposed Cyber Intelligence Sharing and Protection Act[13]—would greatly expand public-private exchange of cyber threat and vulnerability information,[14] and appears to stand a strong chance of passage[15] after both the Sony Pictures attack[16] and the data breach at the Office of Personnel Management ("OPM").[17] In a

9. *Id.* § 4.

10. Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, § 101(b), 128 Stat. 2971, 2972. *See generally Information Sharing: A Vital Resource for Critical Infrastructure Security,* U.S. DEP'T OF HOMELAND SECURITY, http://www.dhs.gov/information-sharing-vital-resource (last updated Sept. 17, 2015); *About FS-ISAC*, FIN. SERVS. INFO. SHARING & ANALYSIS CTR., https://www.fsisac.com/about (describing the Financial Services Information Sharing and Analysis Center ("FS-ISAC") as "the global financial industry's go to resource for cyber and physical threat intelligence analysis and sharing" that "was created by and for members and operates as a member-owned non profit entity").

11. Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, § 2, 128 Stat. 3073, 3084.

12. Exec. Order No. 13,691, 80 Fed. Reg. 9349 (Feb. 13, 2015).

13. H.R. 234, 114th Cong. (2015).

14. Russell Brandom, *CISPA, the Infamous Cybersecurity Bill, Is Headed Back to Congress*, VERGE (Jan. 8, 2015, 3:40 PM), http://www.theverge.com/2015/1/8/7517045/cispa-the-infamous-cybersecurity-bill-is-headed-back-to-congress.

15. *But see* Jennifer Steinhauer, *Senate Rejects Measure to Strengthen Cybersecurity*, N.Y. TIMES (June 11, 2015), http://www.nytimes.com/2015/06/12/us/politics/senate-rejects-measure-to-strengthen-cybersecurity.html.

16. Cory Bennett, *House Dem Revives Major Cyber Bill*, HILL (Jan. 8, 2015, 3:15 PM), http://thehill.com/policy/cybersecurity/228945-top-house-dem-to-reintroduce-major-cyber-bill.

17. *Cf.* Ellen Nakashima, *Chinese Hack of Federal Personnel Files Included Security-Clearance Database*, WASH. POST (June 12, 2015), http://www.washingtonpost.com/world/national-security/chinese-hack-of-government-network-compromises-security-clearance-files/2015/06/12/9f91f146-1135-11e5-9726-49d6fa26a8c6_story.html; Kim Zetter & Andy Greenberg, *Why*

publication touting its cybersecurity successes in 2015, the Obama administration cited a variety of statistics to back its claim that it had "[s]purred information sharing."[18] While the two major political parties differ on the specifics of proposed legislation,[19] there is a bipartisan consensus in favor of information sharing as a cybersecurity palliative.[20] The more information, the better. That consensus is largely wrong.

This Essay continues with three more Parts. Part I critiques the favorable perception of information sharing as a cybersecurity intervention. Part II organizes information sharing conceptually along horizontal and vertical axes, and argues that while top-down exchange may make sense theoretically, it suffers from intractable practical problems. Finally, Part III discusses the risks, particularly to privacy, from enhanced information sharing.

I. CRITIQUE

There are at least three significant problems with the current policy focus on information sharing as a palliative—shortcomings that have not received adequate attention. First, it is not clear that sharing currently faces meaningful legal barriers that impede efficient dissemination of data. Proposed reform measures may be solutions in search of an (evanescent) problem. Second, it is not plain that enhanced sharing will generate any significant benefits. Finally, it is not certain that greater sharing is good at all; the practice poses real risks to privacy. This Part explores these issues.

A. Illusory Barriers

Legislative proposals that bolster information flow depend critically upon the assumptions that current sharing is suboptimal and that legal reform can increase dissemination.[21] In short, law must be getting in

---

the OPM Breach Is Such a Security and Privacy Debacle, WIRED (June 11, 2015), http://www.wired.com/2015/06/opm-breach-security-privacy-debacle/.

18. Press Release, The White House, Office of the Press Sec'y, Fact Sheet: Administration Cybersecurity Efforts 2015 (July 9, 2015), https://www.whitehouse.gov/the-press-office/2015/07/09/fact-sheet-administration-cybersecurity-efforts-2015.

19. *See* Steinhauer, *supra* note 15.

20. *See* Bambauer, *Ghost in the Network*, *supra* note 6, at 1045–47.

21. *See* Jay P. Kesan & Carol M. Hayes, *Creating a "Circle of Trust" to Further Digital Privacy and Cybersecurity Goals*, 2014 MICH. ST. L. REV. 1475 (2014). Kesan and Hayes propose managed information flow between the government and vetted firms using a trusted third party. *Id.* Jennifer Granick has written about the legal barriers to the revelation of vulnerability data more generally. Jennifer Stisa Granick, *The Price of Restricting Vulnerability Publications*,

the way of better information.[22] This assumption is particularly strong for proposals such as liability shields for firms that distribute data.[23] On this account, companies would share more, but fear being sued for violating privacy laws, wiretapping unlawfully, committing torts and the like.[24] Immunity enables sharing, either directly by removing liability, or indirectly by relieving firms of the threat of plaintiff's attorneys motivated by strategic behavior.[25] The major source of claims that legal reform is needed, however, is the regulated entities.[26] Indeed, a Congressional Research Service ("CRS") study cites, as its principal evidence of the need for legal reform to produce more sharing, a survey of information technology security practitioners.[27] (Note that the survey is of information technology staff, who are rarely experts in questions regarding legal liability.) As scholars such as Jennifer Granick have noted, every target of government regulation would love immunity from suit by its consumers, even at the price of aiding the state.[28]

---

9 INT'L J. COMM. L. & POL'Y 1 (2005); *see also* ANDREW NOLAN, CONG. RESEARCH SERV., R43941, CYBERSECURITY AND INFORMATION SHARING: LEGAL CHALLENGES AND SOLUTIONS (2015).

22. There is a considerable literature on the economics of information disclosure and the incentives firms face to divulge data. *See, e.g.*, Ross Anderson & Tyler Moore, *The Economics of Information Security*, 314 SCI. 610 (2006); Howard Beales, Richard Craswell & Steven C. Salop, *The Efficient Regulation of Consumer Information*, 24 J.L. & ECON. 491 (1981); Mark A. Cohen & V. Santhakumar, *Information Disclosure as Environmental Regulation: A Theoretical Analysis*, 37 ENVTL. & RESOURCE ECON. 599 (2007); Michal J. Fishman & Kathleen M. Hagerty, *Mandatory Versus Voluntary Disclosure in Markets with Informed and Uninformed Customers*, 19 J.L. ECON. & ORG. 45 (2003). For legal sources, see Derek E. Bambauer & Oliver Day, *The Hacker's Aegis*, 60 EMORY L.J. 1051 (2011); and Peter P. Swire, *A Theory of Disclosure for Security and Competitive Reasons: Open Source, Proprietary Software, and Government Systems*, 42 HOUS. L. REV. 1333, 1345–79 (2006). I thank Sasha Romanosky for helpful discussion of this point.

23. *See* Ellen Nakashima & Katie Zezima, *Obama to Propose Legislation to Protect Firms That Share Cyberthreat Data*, WASH. POST (Jan. 12, 2015), https://www.washingtonpost.com/politics/obama-proposes-legislation-to-protect-consumer-data-student-privacy/2015/01/12/539c4a06-9a8f-11e4-bcfb-059ec7a93ddc_story.html.

24. NOLAN, *supra* note 21.

24. NOLAN, *supra* note 21.

25. *Id.* at 48–49.

26. Jennifer Granick, *The Right Way to Share Information and Improve Cybersecurity*, JUST SECURITY (Mar. 26, 2015), http://justsecurity.org/21498/share-information-improve-cybersecurity/; Nakashima & Zezima, *supra* note 23.

27. NOLAN, *supra* note 21, at 5 ("[I]n a recent survey of over 700 information technology security practitioners, half of the respondents listed worries about 'potential liability [from] sharing' as the main reason for not participating in an initiative for exchanging threat information.").

28. Granick, *supra* note 26.

However, the assumption that law is part of the problem does not hold up well to scrutiny. As the CRS study admits, there are few impediments to intergovernmental exchange of threat information,[29] and there are already myriad mechanisms by which private-sector firms communicate information about threats and vulnerabilities.[30] Vendors issue bug reports and patches. Independent researchers test software and report on new exploits.[31] Listservs distribute updates. Computer emergency response teams, such as US-CERT, put out advisories.[32] Information sharing and analysis centers coordinate industry-specific risks.[33] Systems administrators talk. Even Facebook has entered the threat-sharing game.[34] The list goes on. The information ecosystem for cybersecurity appears to be diverse and thriving.[35] Policymakers have not elucidated concrete examples of threats where further information could have prevented harm, or where there are structural weaknesses in existing flows.

The purported greatest concern for law as impediment—that private sector entities fail to reveal useful data to government agencies due to liability fears—also proves illusory when analyzed. The CRS study carefully lists the set of regulations that might deter private-public sharing: federal wiretapping law, industry-specific privacy rules, antitrust law, tort and contract law, and baroque causes of action, such

29. S*ee* Daphna Renan, *Pooling Powers*, 115 COLUM. L. REV. 211, 223–26 (2015) (describing how the executive branch used multiple sources of authority and agencies to address cybersecurity concerns). *But see* Keir X. Bancroft, *Regulating Information Security in the Government Contracting Industry: Will the Rising Tide Lift All Boats?*, 62 AM. U. L. REV. 1145, 1199–1200 (2013) (suggesting greater sharing of information about security compliance across agencies to reduce contractors' costs).

30. Patrick Eddington, *OPM, CISA, and the Cybersecurity Oxymoron*, JUST SECURITY (July 2, 2015), http://justsecurity.org/24360/opm-cisa-cybersecurity-oxymoron/.

31. *See, e.g.*, *Why Veracode?*, VERACODE, http://www.veracode.com/about/why-veracode (last visited Nov. 18, 2015).

32. *Id.*; *see 2015 Alerts*, US-CERT, https://www.us-cert.gov/ncas/alerts (last visited Nov. 18, 2015). *But see* Terrence K. Kelly & Jeffrey Hunker, *Cyber Policy: Institutional Struggle in a Transformed World*, 8 I/S 211, 229–33 (2012) (criticizing the U.S. Computer Emergency Ready Team for its failure to provide more tailored information sharing).

33. *See, e.g.*, *About Us*, NH-ISAC, http://www.nhisac.org/about-us/ (last visited Nov. 18, 2015) ("National Health Information Sharing and Analysis Center").

34. Ron Miller, *New Facebook Threat-Sharing Project Sees Safety in Herd*, TECHCRUNCH (Feb. 11, 2015), http://techcrunch.com/2015/02/11/new-facebook-threat-sharing-project-sees-safety-in-herd/.

35. *See* L. Jean Camp, *The State of Economics of Information Security*, 2 I/S 189, 195 (2006) ("[R]esearch has verified that information sharing is both economically valuable and a complement to security investment.").

as shareholder derivative suits.[36] These legal regimes may cause angst for information technology staff, and perhaps for the lawyers in their general counsel's office. But the concerns are quickly dispelled.

The three sections of the federal wiretapping statute—the Wiretap Act,[37] the Stored Communications Act,[38] and the Pen Register Act[39]—have exceptions that protect most, if not all, relevant sharing. The Wiretap Act and Stored Communications Act cover only the content of communications (not routing data),[40] and relieve liability where one party consents to the disclosure.[41] Firms such as Internet Service Providers ("ISPs") can protect themselves via contract with customers, generating consent, and via analyzing only non-content data. As a practical matter, even if firms unlawfully divulge content data to one another or to the government, affected consumers will have scant opportunity to detect the disclosure. And, the exception that enables providers to disclose contents to protect their rights or property seems amenable to gaming—providers could potentially enter into reciprocal security data-sharing agreements, and then disclose threat information as a necessary incident to protecting their rights under those agreements.[42] The Pen Register Act has similar exceptions,[43] and applies only to non-content data.[44]

The various bespoke privacy regimes, such as the Video Privacy Protection Act[45] and Children's Online Privacy Protection Act,[46] govern sensitive data like personally identifiable information ("PII"), but are unlikely to come into play. Information about one's video rental habits or age is not particularly helpful as cyber threat data. For antitrust, the Department of Justice has issued a policy statement clarifying that antitrust law is not an impediment to sharing.[47] Tort and contract law

36. NOLAN, *supra* note 21, at 13–33.
37. 18 U.S.C. §§ 2510–22 (2012).
38. *Id.* §§ 2701–12.
39. *Id.* §§ 3121–27.
40. *Id.* §§ 2511(1)(c), 2701(a).
41. *Id.* §§ 2511(2)(c), 2701(c)(2).
42. *Cf. Id.* §§ 2511(2)(a)(i), 2702(b)(5).
43. *Id.* § 3121(b)(1)–(2).
44. *Id.* § 3127(3)–(4) (defining both pen register and trap and trace device).
45. *Id.* § 2710.
46. 15 U.S.C. §§ 6501–06 (2012).
47. Press Release, U.S. Dep't of Justice, Department of Justice, Federal Trade Commission Issue Antitrust Policy Statement on Sharing of Cybersecurity Information (Apr. 10, 2014), http://www.justice.gov/atr/public/guidelines/305027.pdf.

have been almost a complete failure as a cause of action regarding both data breaches and deliberate disclosures;[48] its weakness is much bemoaned by legal scholars.[49] Finally, causes of action such as shareholder suits are founded not on disclosure, but rather on a failure of a duty of care on the part of directors and officers.[50] Thus, liability stems not from sharing information, but from a lack of care on the part of the corporation, such as a data breach where the disclosed data serves as evidence of the alleged lack of care.[51] That is a remote risk from sharing.

Moreover, risks of liability have hardly impaired private sector sharing—transactions of private information are routine,[52] causing considerable outrage among privacy advocates.[53] Private organizations may purport to be reluctant to share data with the government, but they do not hesitate to share it with one another, particularly for profit.

In short, law is not a meaningful impediment to increased exchange of threat and vulnerability information, either across the public and private sectors or between entities within one of them.

---

48. *See* Sasha Romanosky, David Hoffman, & Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation*, 11 J. EMP. LEGIS. STUD. 74 (2014) (finding that while 50% of breach suits settle, the awards are usually only nominal damages and only to named plaintiffs); *see also* Derek E. Bambauer, *Rules, Standards, and Geeks*, 5 BROOK. J. CORP. FIN. & COM. L. 49, 58 (2011); L. Jean Camp & Catherine Wolfram, *Pricing Security: A Market in Vulnerabilities*, *in* ECONOMICS OF INFORMATION SECURITY 18–22 (L. Jean Camp & Stephen Lewis eds., 2004); Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241 (2007); Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425 (2008).

49. *See, e.g.*, Citron, *supra* note 48, at 262–68; Vincent R. Johnson, *Credit-Monitoring Damages in Cybersecurity Tort Litigation*, 19 GEO. MASON L. REV. 113 (2011); Felix T. Wu, *Defining Privacy and Utility in Data Sets*, 84 U. COLO. L. REV. 1117, 1161–62 (2013).

50. *See* Smith v. Van Gorkom, 488 A.2d 858 (Del. 1985) (discussing duty of care to shareholders).

51. NOLAN, *supra* note 21, at 30.

52. *See* Natasha Singer, *You For Sale*, N.Y. TIMES, June 17, 2012, at BU1; s*ee* Megan Geuss, *FTC Proposes a Compromise So RadioShack Can Sell Consumer Data*, ARS TECHNICA (May 18, 2015, 1:10 PM), http://arstechnica.com/tech-policy/2015/05/ftc-proposes-a-compromise-so-radio shack-can-sell-consumer-data/; Emma Thomasson, *Mastercard: Real-Time Consumer Trend Data Is a Huge Growth Area for Us*, BUS. INSIDER (Jun. 11, 2014, 10:25 AM), http://www.bus inessinsider.com/r-mastercard-expects-big-growth-from-big-data-insights-2014-11.

53. *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998); Neil M. Richards & Jonathan H. King, *Three Paradoxes of Big Data*, 66 STAN. L. REV. ONLINE 41 (2013), http://www.stanfordlawreview.org/online/privacy-and-big-data/three-paradox es-big-data; Electronic Privacy Information Center, *Judge Approves Laughably Bad, Collusive Class Action Settlement*, EPIC (Apr. 3, 2015), https://epic.org/2015/04/judge-approves-laughably-bad-c.html.

B. Uncertain Benefits

Increased information sharing probably will not help cybersecurity much.[54] The pro-sharing argument rests on at least three key assumptions. First, the entity receiving cyberthreat information can and will act upon it. Second, the shared data is reliable. Finally, the volume of threat information is manageable for recipients. Each of these assumptions is uncertain at best.

First, organizations may not be able to make use of updates. It is difficult to reliably quantify cyberattack patterns.[55] But, at least some meaningful number of them—including the high-profile hack of sensitive data at the federal OPM[56]—occurred when attackers exploited known vulnerabilities.[57] If an exploit targets a known, patched bug, then more information likely makes little to no difference. Perhaps firms might use data about the prevalence of exploits to prioritize the order in which to apply patches, but studies show that many bugs remain unpatched for at least a year.[58] Firms delay implementation due to the need to test patches, to ensure interoperability with other code, and to manage resource constraints with their information technology

54. *See* Josephine Wolff, *Cybersecurity Legislation Is Too Short-Sighted*, SLATE (Apr. 29, 2015, 11:05 AM), http://www.slate.com/blogs/future_tense/2015/04/29/pcna_cisa_information_sharing_cybersecurity_legislation_is_too_short_sighted.html.

55. Attack statistics are notoriously unreliable. For example, some reported data show that the state of Utah is subject to more attacks per day than the Department of Defense, which seems unlikely. Brian Fung, *How Many Cyberattacks Hit the United States Last Year?*, NEXTGOV (Mar. 8, 2013), http://www.nextgov.com/cybersecurity/2013/03/how-many-cyberattacks-hit-united-states-last-year/61775/. There are services that attempt to track attacks in real time. Brian Krebs, *Who's Attacking Whom? Realtime Attack Trackers*, KREBS ON SECURITY (Jan. 5, 2015), http://krebsonsecurity.com/2015/01/whos-attacking-whom-realtime-attack-trackers/. And PricewaterhouseCoopers, which issues a widely used cyberattack report, bases its data on surveys. PWC, US CYBERCRIME: RISING RISKS, REDUCED READINESS (2014), http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/pwc-2014-us-state-of-cybercrime.pdf; *see* Cory Bennett, *Study: Cyberattacks Up 48 Percent in 2014*, HILL (Oct. 27, 2014), http://thehill.com/policy/cybersecurity/221936-study-cyber-attacks-up-48-percent-in-2014.

56. *See* Sean Gallagher, *Why the "Biggest Government Hack Ever" Got Past the Feds*, ARS TECHNICA (June 8, 2015, 10:00 AM), http://arstechnica.com/security/2015/06/why-the-biggest-government-hack-ever-got-past-opm-dhs-and-nsa/.

57. *See, e.g.*, Brian Krebs, *The Long Tail of ColdFusion Fail*, KREBS ON SECURITY (Mar. 17, 2014, 12:15 PM), http://krebsonsecurity.com/2014/03/the-long-tail-of-coldfusion-fail/#more-25158; *Snapchat Warned Before Hack About Vulnerability*, HERE & NOW (Jan. 3, 2014), http://hereandnow.wbur.org/2014/01/03/snapchat-security-breach. *See generally* Bambauer, *Ghost in the Network*, *supra* note 6, at 1050–52 (describing why organizations remain vulnerable to the "known unknowns" of vulnerabilities with patches).

58. *See, e.g.*, Arik Hesseldahl, *Why the Federal Government Sucks at Cyber Security*, RE/CODE (June 23, 2015), http://recode.net/2015/06/23/why-the-federal-government-sucks-at-cybersecurity/; *see also* Sales, *supra* note 6, at 1517.

staff.[59] Even if the shared information is useful, it still has to be used to make a difference.

The situation is worse for attacks against unknown weaknesses (zero-day exploits). Here, information is useless by definition: defenders simply do not know about the vulnerability, nor do they have the capability to protect themselves even if they learn about it.[60] Once the data are analyzed, hopefully a weakness (in the zero-day) can be found, along with a signature added to targets' intrusion-detection systems.[61] Until then, however, information sharing is irrelevant for zero-days.

Thus, sharing becomes useful only in a subset of circumstances: those where some targets (such as firms or government agencies) know about vulnerabilities, but others do not, and where the uninformed could engage in remediation if they knew more.[62] Reliable data on how often this occurs are lacking. However, this seems like a narrow range of cases:, where the exploit is imperfectly known, the remedy is ready at hand, and targets are capable of applying the fix without meaningful delay.

Next, there are reasons to be skeptical about the quality of the information that gets shared. There are risks from unreliability: irrelevant data clogs the system, and inaccurate data damages it. If the threat information is not cogent for the recipient, it consumes time and attention that should be devoted to relevant threats. And patches for nonexistent vulnerabilities can introduce their own flaws and impair functionality.

National security threat sharing provides a cautionary tale about information quality. After the attacks of September 11, 2001, governments at all levels were determined to reduce purported barriers to sharing of intelligence.[63] With the passage of the Homeland Security Act of 2002, the federal government established a set of nationwide fusion centers to share threat data with state and local governments.[64]

---

59. Sales, *supra* note 6, at 1508.

60. *See* Leyla Bilge & Tudor Dumitras, *Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World*, 19 PROC. 2012 ACM CONF. ON COMPUTER & COMM. SECURITY 833 (2012), http://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf.

61. *See Kaspersky Lab Discovered and Blocked Zero-Day Vulnerability in Adobe Flash Player*, KASPERSKY LAB (May 5, 2014), http://www.kaspersky.com/about/news/virus/2014/kaspersky-lab-discovered-and-blocked-zero-day-vulnerability-in-adobe-flash-player.

62. *See* Bambauer, *Ghost in the Network*, *supra* note 6, at 1041, 1050–52.

63. *See* Torin Monaghan & Priscilla M. Regan, *Zones of Opacity: Data Fusion in Post-9/11 Security Organizations*, 27 CANADIAN J.L. & SOC'Y 301 (2012).

64. Homeland Security Act of 2002, Pub. L. No. 107-296, §§ 891–99, 116 Stat. 2135, 2252–

DHS Secretary Janet Napolitano described the fusion centers as "one of the centerpieces of our counterterrorism strategy."[65] The centers have reportedly processed over 22,000 suspicious activity reports, at an estimated cost of at least $289 million.[66] However, a bipartisan report by an investigatory subcommittee of the Senate Homeland Security and Governmental Affairs Committee found no evidence that fusion centers identified a single terrorist threat or contributed in any way to disrupting an active terrorist plot.[67] The centers generally produced "irrelevant, useless, or inappropriate intelligence reporting . . . and many produced no intelligence reporting whatsoever."[68] Frequently, however, the centers shared information that "endanger[ed] citizens' civil liberties."[69] The centers not only failed to improve national security, but they consumed resources that could have been devoted to efforts that actually produced value.[70] Even if information on threats to cybersecurity proves to be more reliable than data on threats to national security, there will inevitably be problems of quality. And while some information technology personnel are sufficiently expert to sift the useful from the useless, not all of them can do so reliably. Those problems may be greater than the value that sharing provides—as with the fusion centers.

Lastly, a system for processing vulnerability and threat notifications must contend with significant challenges related to volume.[71] The sheer daily number of cyberattacks, even just on government networks, is staggering.[72] Administrators will have to determine what information

---

58.

65. U.S. SENATE COMM. ON HOMELAND SEC. & GOVERNMENTAL AFFAIRS, PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, FEDERAL SUPPORT FOR AND INVOLVEMENT IN STATE AND LOCAL FUSION CENTERS 2 (2012) [hereinafter SUBCOMMITTEE ON INVESTIGATIONS].

66. *Id.* at 3; Robert O'Harrow Jr., *DHS 'Fusion Centers' Portrayed as Pools of Ineptitude and Civil Liberties Intrusions*, WASH. POST (Oct. 2, 2012), http://www.washingtonpost.com/investigations/dhs-fusion-centers-portrayed-as-pools-of-ineptitude-and-civil-liberties-intrusions/2012/10/02/10014440-0cb1-11e2-bd1a-b868e65d57eb_story.html.

67. SUBCOMMITTEE ON INVESTIGATIONS, *supra* note 65, at 2.

68. *Id.*

69. *Id.* at 1.

70. *See generally* Priscilla M. Regan & Torin Monahan, *Beyond Counterterrorism: Data Sharing, Privacy, and Organizational Histories of DHS Fusion Centers*, 5 INT'L J. E-POL. 1 (2013); O'Harrow, *supra* note 66.

71. *See* Andrea Castillo, *Cybersecurity Bill More Likely to Promote Information Overload than Prevent Cyberattacks*, Congress Blog, HILL (May 7, 2015, 1:00 PM), http://thehill.com/blogs/congress-blog/homeland-security/241242-cybersecurity-bill-more-likely-to-promote-information.

72. *See, e.g.*, Bob Orr, *Pentagon Expands Cyber Defense Against Daily Attacks*, CBS NEWS

about these attacks to share, and with whom. That requires difficult judgments about which attacks are noteworthy or new, but in the absence of those judgments, the volume of information would be overwhelming for recipients. Threat information is most valuable when it is not yet known to the recipient, although warnings about existing threats might help entities prioritize dealing with them. Analytics software, such as that produced by Palantir, can aid in the task, but it is limited by the quality of its algorithms and the patterns identified as meaningful by its users.[73] The sheer quantity of attack data is a potentially insuperable problem. As security expert Bruce Schneier has written, the answer to the problem of finding a needle in a haystack is not to add more hay.[74]

Importantly, the government may not pass on some vulnerability information that is useful to targets, because that data is useful for offensive purposes as well as defensive ones.[75] Firms such as Microsoft have begun revealing details on vulnerabilities with the government before either releasing them to customers or patching them.[76] If the government learns of a new zero-day attack against the Microsoft Windows operating system, the state can alert firms and agencies to the vulnerability—or weaponize it for espionage or surveillance purposes.[77] The recent attack on the security firm Hacking Team demonstrated that agencies such as the FBI and Drug Enforcement Agency purchased the company's software, which exploits vulnerabilities in mobile phone operating systems and Microsoft's BitLocker encryption technology.[78] They bought it not to make those programs more secure, but to break

---

(Feb. 6, 2013, 7:34 PM), http://www.cbsnews.com/news/pentagon-expands-cyber-defense-amid-daily-attacks/; Ed Sperling, *Ten Million Cyberattacks a Day*, FORBES (Aug. 9, 2010, 6:00 AM), http://www.forbes.com/2010/08/06/internet-government-security-technology-cio-network-cyber-attacks.html.

73. *See Cyber Security*, PALANTIR, https://www.palantir.com/solutions/cyber/ (last visited Nov. 18, 2015).

74. Bruce Schneier, *Why Data Mining Won't Stop Terror*, SCHNEIER ON SECURITY (Mar. 9, 2005), https://www.schneier.com/essays/archives/2005/03/why_data_mining_wont.html.

75. *See* Eddington, *supra* note 30; Mailyn Fidler, *Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis*, I/S (forthcoming 2015–16), http://moritzlaw.osu.edu/students/groups/is/files/2015/06/Fidler-Second-Review-Changes-Made.pdf.

76. Michael Riley, *U.S. Agencies Said to Swap Data with Thousands of Firms*, BLOOMBERG (June 14, 2013, 11:01 PM), http://www.bloomberg.com/news/articles/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms.

77. Fidler, *supra* note 75 (manuscript at 6–7).

78. Thomas Fox-Brewster, *Leaked Emails: How Hacking Team and US Government Want to Break Web Encryption Together*, FORBES (July 6, 2015, 2:29 PM), http://www.forbes.com/sites/thomasbrewster/2015/07/06/us-gov-likes-hacking-team/.

into them. The FBI issued a statement in response to the revelation about its relationship with Hacking Team that reads, "the FBI routinely identifies, evaluates, and tests potential exploits in the interest of cyber security."[79] Put simply, the government already deliberately fails to share information about known vulnerabilities, because those weaknesses are useful for purposes other than cybersecurity. Enhanced sharing may simply improve the state's ability to monitor communications.

This divided loyalty is most evident in the mission of the government's most expert cybersecurity entity, the National Security Agency ("NSA"). The NSA has two missions. One is to secure the country's communications systems, and the second is to monitor those systems (and those of foreign nations).[80] Those goals are fundamentally in tension. Vulnerability information can be used to advance only one of them. There is no practical way to limit patches to U.S. systems alone; eliminating a vulnerability for one user inevitably makes it available to all of them. The NSA has to decide whether to improve America's cybersecurity or to engage in better surveillance. Thus, it will not share all of the vulnerability information it receives.

Conventional wisdom among policymakers is that information sharing is critical to improving cybersecurity. However, the benefits are likely overstated, perhaps significantly so.[81] Even if this approach does offer value, it may not be advisable to adopt it. Cybersecurity efforts are a zero sum game: resources spent sharing information cannot be used for education, prevention, or resilience.[82] Supporters of enhanced exchange have yet to make a rigorous case for adopting it instead of other measures.

C. Real Risks

Enhanced sharing of information with government entities creates real risks. Threat and vulnerability information will at times contain PII, such as IP addresses, e-mail addresses, or URLs for sites such as Facebook.[83] There are at least two risks from the accumulation of data

79. *Id.* (quoting statement from FBI's Quantico office).

80. *Mission*, NAT'L SECURITY AGENCY, https://www.nsa.gov/about/mission/index.shtml (last visted Nov. 18, 2015).

81. *See* Bambauer, *Ghost in the Network*, *supra* note 6, at 1045–47.

82. *See* Bambauer, *Conundrum*, *supra* note 6, at 635–67.

83. *See* Stewart Baker, *Why the House Information-Sharing Bill Could Actually Deter Information Sharing*, WASH. POST (Mar. 30, 2015), https://www.washingtonpost.com/news/

that includes PII. The government may misuse the information. For example, the fusion centers run by the DHS reported on activities by people that were expressly protected by the First Amendment, such as a motivational talk to a Muslim organization about good parenting techniques and a lecture at a mosque.[84] And, even if state agencies only employ data for legitimate purposes, merely retaining the information creates risks for subjects, because the government can also be hacked. The recent OPM breach revealed sensitive information of 20 million people[85], and this sort of hack is increasingly the norm rather than the exception.[86] A vulnerability database with PII would make an attractive target for attackers.[87]

This risk is compounded by private firms, who are likely to overshare under an immunity regime. A number of legislative proposals would shield firms from liability based on information shared with the government.[88] If that information contains PII for the firms' customers, or especially third parties, liability sets up worrisome incentives. Any privacy harms from that sharing would fall solely on the subjects of the PII: the firms would be protected.[89] Thus, if firms gain any benefit from sharing data, they will do so without balancing those advantages against harms. This also affects the level of precautions firms are likely to take in scrubbing data of PII before disclosing it. Firms with no downside from revealing PII are unlikely to invest in removing it from

---

volokh-conspiracy/wp/2015/03/30/why-the-house-information-sharing-bill-could-actually-deter-information-sharing/; Andy Greenberg, *CISA Cybersecurity Bill Advances Despite Privacy Concerns*, WIRED (Mar. 12, 2015, 7:18 PM), http://www.wired.com/2015/03/cisa-cybersecurity-bill-advances-despite-privacy-critiques/.

84. SUBCOMMITTEE ON INVESTIGATIONS, *supra* note 65, at 38.

85. Cory Bennett, *Lawmakers Look to Strip OPM Powers After Hack*, HILL (July 12, 2015, 6:00 AM), http://thehill.com/policy/cybersecurity/247593-lawmakers-look-to-strip-opm-powers-after-hack.

86. *See* Chris Frates & Curt Devine, *Government Hacks and Security Breaches Skyrocket*, CNN (Dec. 19, 2014), http://www.cnn.com/2014/12/19/politics/government-hacks-and-security-breaches-skyrocket/.

87. *See* Nuala O'Connor, *Why the OPM Data Breach Is Unlike Any Other*, CDT (June 22, 2015), https://cdt.org/blog/why-the-opm-data-breach-is-unlike-any-other/ ("[E]xpanded sharing is especially worrisome for data security because the bill permits unprepared agencies to receive data (rather than direct all sharing at a secure entity such as the DHS National Cybersecurity and Communications Integration Center), and contains only a weak requirement to strip personal information prior to sharing.").

88. *See* Andy Greenberg, *House Passes Cybersecurity Bill Despite Privacy Protests*, WIRED (Apr. 22, 2015, 5:38 PM), http://www.wired.com/2015/04/house-passes-cybersecurity-bill-despite-privacy-protests/.

89. *See* Nakashima & Zezima, *supra* note 23.

data.

Collecting information with PII has little offsetting security value. This data does not help determine the magnitude, novelty, or even origin of threats. Information about the source of threats, for example, is often contested, uncertain, or flatly wrong.[90] Experts are still uncertain about the source of the cyberattacks on Estonia in May 2007 and South Korea in 2009[91]—not to mention the entity responsible for the Sony Pictures hack.[92] Even if an attack originates from the computer or account of a single individual, it is likely that that person's credentials were compromised, as opposed to his being the true source of the threat.[93] Thus, sharing data with PII creates risks to privacy with little to no offsetting benefit for security.

This Part's critique undermines three key arguments in favor of bolstering information sharing. It shows that there are few, if any, legal barriers that impede exchange, that greater sharing will likely produce little benefit, and that more data flow creates significant risks to privacy.

II. CONTROL THE HORIZONTAL. CONTROL THE VERTICAL.[94]

It can be helpful conceptually to organize information-sharing regimes along two dimensions: the horizontal and the vertical. Horizontal sharing occurs among similarly situated entities—firms or federal agencies of roughly the same size in the same industry. Vertical sharing occurs among entities at different levels or with significantly different capabilities, such as between federal and local government agencies, or large corporations and small businesses in a sector. While

90. *See* Bambauer, *Conundrum*, *supra* note 6, at 589–90, 596–98; Benjamin Brake, *Strategic Risks of Ambiguity in Cyberspace*, COUNCIL ON FOREIGN REL. (Oct. 22, 2015), http://www.cfr.org/cybersecurity/strategic-risks-ambiguity-cyberspace/p36541.

91. *See* Bambauer, *Ghost in the Network*, *supra* note 6, at 1050.

92. *See* Timothy B. Lee, *The Sony Hack: How it Happened, Who Is Responsible, and What We've Learned*, VOX (Dec. 17, 2014, 9:00 PM), http://www.vox.com/2014/12/14/7387945/sony-hack-explained; Dana Tamir, *Who Hacked Sony? New Report Raises More Questions About Scandalous Breach*, SECURITY INTELLIGENCE (Feb. 5, 2015), https://securityintelligence.com/who-hacked-sony-new-report-raises-more-questions-about-scandalous-breach/; Jane Wakefield, *Whodunnit? The Mystery of the Sony Pictures Hack*, BBC (Dec. 18, 2014), http://www.bbc.com/news/technology-30530361.

93. Increasingly, targeted spear phishing attacks trick employees into revealing their credentials. *See* Kim Zetter, *Hacker Lexicon: What Are Phishing and Spear Phishing?*, WIRED (Apr. 7, 2015, 6:09 PM), http://www.wired.com/2015/04/hacker-lexicon-spear-phishing/ (relating the details of the successful spear phishing attack against RSA in 2011).

94. With apologies to the television series *The Outer Limits*, which opened with a voice-over that included the lines, "We will control the horizontal. We will control the vertical."

the mapping is rough, it is likely useful.[95] In particular, it suggests that while horizontal sharing may be useful, vertical sharing—the focus of much of cybersecurity policy and proposed legislation—is not likely to be of value.

The horizontal exchange of security data among peer firms in an industry, or government actors at a given level, probably makes sense.[96] These entities likely face similar threats and operational constraints, and probably have roughly equivalent resources to deploy for prevention and countermeasures.[97] And, they are likely to understand what data will be pertinent for their counterparts, and what steps their peers can reasonably take.[98] For example, a large firm that reveals a new signature for an intrusion detection system ("IDS") generates measurable benefit for peers using the IDS, but no benefit for small firms that do not.[99] In particular, firms in industries that use customized software, such as Supervisory Control and Data Acquisition ("SCADA") packages in utility companies, may be able to provide highly relevant vulnerability data to one another.[100] Similarly, advice that is applicable to a Fortune 500 company with a specialized information security team will not be useful to smaller organizations that do not have dedicated security resources.[101] Put simply, peers are

95. There are of course some tricky definitional questions in this simple matrix: are small firms in different industries more or less similar than a small firm and a large one in a given sector? Like any model, this one sacrifices some precision to offer some generalizable insights.

96. *See* Miller, *supra* note 34.

97. *See generally* J.D. Harrison, *Small Business Leaders Urge Congress to Rethink Cybersecurity Measures*, WASH. POST (Apr. 23, 2015), http://www.washingtonpost.com/news/on-small-business/wp/2015/04/23/small-business-leaders-urge-congress-to-rethink-cybersecurity-measures/.

98. *See* S. Kumar, *Why Small Firms Mean Big Business for Cybersecurity*, FORTUNE (May 20, 2015, 11:25 AM), http://fortune.com/2015/05/20/cybersecurity-small-business/.

99. There are excellent intrusion detection systems that are open source and thus available at no cost. *See, e.g.*, SNORT, https://www.snort.org/ (last visited Nov. 18, 2015). However, even free software requires information technology personnel to install, configure, and maintain it. Security expert John Viega argues that IDS "is only a good investment for the largest 5% of companies." John Viega, *Why Most Companies Shouldn't Run Intrusion Detection*, O'REILLY: COMMUNITY (Dec. 4, 2008), http://broadcast.oreilly.com/2008/12/why-most-companies-shouldnt-ru.html.

100. *See* U.S. DEP'T OF ENERGY, 21 STEPS TO IMPROVE CYBER SECURITY OF SCADA NETWORKS 3 (2007), http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf (describing use of SCADA software in utilities' networks).

101. *See* Kelly Jackson Higgins, *Stuxnet Expert Proposes New Framework for ICS/SCADA Security*, DARK READING (Sept. 4, 2013, 6:02 PM), http://www.darkreading.com/stuxnet-expert-proposes-new-framework-for-ics-scada-security/d/d-id/1140411? (citing security expert Ralph Langner, who estimates that very few critical infrastructure operators have even one information

more likely to share information that is relevant to their counterparts' cybersecurity environments, and that they can act upon once informed.

Upwards vertical sharing makes less sense, at least theoretically. Entities could share upwards—from smaller to larger firms, from local to state to federal government, and from the private sector to the public. This sharing, though, suffers from the problem of the information flood.[102] Organizations higher in the hierarchy will receive redundant information, and probably some that is irrelevant. Attention economics apply to this problem with full force.[103] Lower-level entities will generally not be able to determine what data is relevant to higher-level ones, and thus cannot be depended upon to do some of the necessary filtering. Vulnerabilities in bespoke software probably are not useful to anyone other than the owner.[104] And it is not clear that round-trip dissemination of vulnerability information—for example, from a firm in one industry to the federal government to a firm in a second industry—is more likely or more efficient than either horizontal sharing or notifying the relevant vendor.

Downwards sharing, such as from federal agencies like the NSA or DHS to private organizations, makes more sense conceptually.[105] Within an industry, larger firms may be better positioned to analyze data and detect trends.[106] Expert government agencies could potentially play the same role.[107] However, important information asymmetries plague this possibility as well. Larger companies or expert agencies likely know little about a given recipient's particular needs or capabilities. Information sharing risks being too specific, by providing

---

security person on their staff); Kumar, *supra* note 98.

102. *See* Castillo, *supra* note 71.

103. *See* Christine Jolls, Cass R. Sunstein & Richard Thaler, *A Behavioral Approach to Law and Economics*, 50 STAN. L. REV. 1471 (1998); Michael H. Goldhaber, *Attention Shoppers!*, WIRED (Dec. 1, 1997, 12:00 PM), http://archive.wired.com/wired/archive/5.12/es_attention.html.

104. *See generally* Scott, *supra* note 48; Microsoft Security Intelligence Report, *Vulnerability Subprocess*, http://www.microsoft.com/security/sir/story/default.aspx#!0day_subprocess.

105. *But see* Steven M. Bellovin et al., *Can It Really Work? Problems with Extending EINSTEIN 3 to Critical Infrastructure*, 3 HARV. NAT'L SECURITY J. 1 (2011) (explaining why the EINSTEIN threat detection system in use on government networks will not function adequately on private networks).

106. *See* Miller, *supra* note 34; Fahmida Y. Rashid, *Microsoft Releases Threat Information Sharing Framework*, SECURITY WEEK (Jan. 30, 2015), http://www.securityweek.com/microsoft-releases-threat-information-sharing-framework.

107. *See, e.g.*, Michael Rogers, Dir., Nat'l Sec. Agency, Remarks at the NSA Event: Sharing Cyber Threat Information to Protect Business and America (Oct. 28, 2014) (transcript available at https://www.nsa.gov/public_info/speeches_testimonies/28oct14_dirnsa.shtml) (discussing role of the NSA in information sharing).

detailed yet irrelevant information; too general, by providing broad advice or vulnerability data on platforms such as Microsoft Windows that are already covered by the vendor; or both. Descriptively, there appears to be relatively little downward sharing between government and the private sector at present, even though fewer privacy concerns arise when information flows in the opposite direction.[108] And, it is unclear why government agencies would be better or faster sources of cybersecurity information than vendors, peers, security firms, or independent researchers.

Information-sharing approaches can be usefully organized along horizontal and vertical dimensions. Horizontal sharing among similarly sized or situated entities makes sense, but appears to be taking place already. Vertical sharing risks flooding recipients with inapposite information. In both cases, it is not clear why government intervention is currently necessary.

III. THE RISKS

Current vertical information-sharing proposals create risks that are not balanced by the minimal security benefits they would offer. First, to borrow Paul Ohm's term, these initiatives would help the government construct the Database of Ruin, and use it for purposes far beyond securing U.S. networks.[109] For example, the Cybersecurity Information Sharing Act ("CISA") of 2015 has several features that create risk.[110] First, private entities that share information with the government receive immunity from civil actions based on that disclosure, even if the data contains PII.[111] Second, if the government archives the information, it can use it for a wide range of law enforcement purposes—including prosecution of trade secret misappropriation, identity theft, and the sexual exploitation of minors—in addition to employing it to enhance cybersecurity.[112] In theory, PII must be purged from information that is shared, but the combination of immunity and law enforcement usage

108. Steven Norton, *CIOs Say Cybersecurity Information Sharing Has a Long Way to Go*, WALL ST. J. (Apr. 6, 2015, 4:23 PM), http://blogs.wsj.com/cio/2015/04/06/cios-say-cybersecurity-information-sharing-has-a-long-way-to-go/.

109. *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1746 (2010) (defining the "database of ruin" as "the worldwide collection of all of the facts held by third parties that can be used to cause privacy-related harm to almost every member of society").

110. S. 754, 114th Cong. (2015).

111. *Id.* § 6(b); *see* Castillo, *supra* note 71.

112. S. 754 § 5(d)(5)(A)(vi).

raises questions about how effective such purging is likely to be.[113] And, of course, the information can be shared without the consent of the data subject. Scholars raise the concern that measures like CISA, rather than being effective measures in the surge towards cybersecurity, are instead intended as a component of the national security state's surveillance regime.[114] And the myriad recent data breaches at federal agencies demonstrates that the risks from governmental storage of information are not limited to official action—cybersecurity threat data will be attractive to attackers as well.[115] In short, current policy encourages the government to accumulate data profligately, where it may be subject to misuse by state actors or to misappropriation by crackers.

Second, a more subtle threat is that the fetish for information sharing may politically displace more effective cybersecurity measures.[116] Data-sharing policy initiatives are attractive because they are relatively uncontroversial; while civil liberties groups object to CISA and its kin, information technology firms have little to lose and potentially much to gain from such legislation.[117] The proposals do not require any substantive security steps by private entities, and while they may create some information management burden for federal agencies such as the

---

113. *Id*. § 4(d)(2); *see* Eddington, *supra* note 30.

114. *See, e.g*., Jennifer Granick, *Sloppy Cyber Threat Sharing Is Surveillance by Another Name*, JUST SECURITY (June 29, 2015, 9:23 AM), http://justsecurity.org/24261/sloppy-cyber-threat-sharing-surveillance/. *See generally* Omer Tene, *A New Harm Matrix for Cybersecurity Surveillance*, 12 COLO. TECH. L.J. 391 (2014).

115. Julie Hirschfeld Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. TIMES (July 9, 2015), http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html; Jack Moore, *The Year of the Breach: 10 Federal Agency Data Breaches in 2014*, NEXTGOV (Dec. 30, 2014), http://www.nextgov.com/cybersecurity/2014/12/year-breach-10-federal-agency-data-breaches-2014/102066/; Jai Vijayan, *4 Worst Government Data Breaches of 2014*, INFO. WEEK (Dec. 11, 2014, 9:06 AM), http://www.informationweek.com/government/cybersecurity/4-worst-government-data-breaches-of-2014/d/d-id/1318061.

116. Political scientist John Kingdon uses the model of a "policy window," in which there is a limited period of political salience for reform on an issue to be completed before the window closes. JOHN W. KINGDON, AGENDAS, ALTERNATIVES, AND PUBLIC POLICIES (2d ed. 2010); *cf*. Peter Sloan, *The Reasonable Information Security Program*, 21 RICH. J.L. & TECH. 2 (2014) (describing model information security plan that meets reasonableness requirements under various statutory regimes).

117. *See* O'Connor, *supra* note 87; Chris O'Brien, *Cyber Security Bill Pits Tech Giants Against Privacy Activists*, L.A. TIMES (Apr. 12, 2013), http://articles.latimes.com/2013/apr/12/business/la-fi-cybersecurity-bill-20130413; *Stop the Cybersecurity Information Sharing Bills*, EFF, https://act.eff.org/action/stop-the-cybersecurity-information-sharing-bills (last visited Nov. 18, 2015).

DHS, they do not require those organizations to do much beyond storing and sharing the information at their discretion. Information sharing is politically popular because it is relatively undemanding and appears to respond to a salient problem. The risk, though, is that passage of CISA or a similar bill will cause Congress and policymakers to turn their attention to other issues, even though significant cybersecurity problems remain.

Current information-sharing approaches thus create risks to privacy, by accumulating a storehouse of sensitive personal information, and to cybersecurity itself, by crowding out more controversial yet more effective measures.

CONCLUSION

Information sharing is a relatively easy answer to the difficult problems of cybersecurity. The challenge is that it is the wrong answer. While augmenting the exchange of threat and vulnerability data is cheap and intuitively appealing, it is also flawed at both theoretical and practical levels. The current focus on sharing is understandable, since it responds to a felt need to do something about cybersecurity in the wake of numerous high-profile breaches and attacks, and because it faces little opposition from stakeholders. But, like most worthwhile reforms, policy changes that make real progress in cybersecurity will come at a meaningful political cost. Measures that increase information flow create the appearance of useful change.[118] But that is a dangerous illusion: it abates the pressure to improve the security of systems and networks without producing any real benefit.[119]

The sharing obsession not only crowds out more effective interventions, it places potentially sensitive information at risk for little benefit. Several of the proposed legislative measures, such as CISA, expand the use of shared information beyond cybersecurity to standard law enforcement. While firms and government entities are supposed to expunge PII before release, there are no standards for so doing, and little practical likelihood of liability for a failure to comply. And, these risks come with scant countervailing benefit: there are no meaningful legal barriers to enhanced exchange at present, and more data may not help recipients who are flooded with information and limited in their

118. *See* Amitai Aviram, *The Placebo Effect of Law: Law's Role in Manipulating Perceptions*, 75 GEO. WASH. L. REV. 54 (2006).

119. *Cf.* Kesan & Hayes, *supra* note 21, at 1545–47.

cybersecurity resources.

The exchange of threat information works reasonably well at present, and the government should concentrate on more effective responses to cybersecurity weaknesses. In short, the only winning move for information-sharing legislation is not to play.[120]

120. WAR GAMES (United Artists June 3, 1983) (quoting the War Operation Plan Response, or Joshua, computer system: "The only winning move is not to play").