

BYU Law Review

Volume 2017 | Issue 5


Article 6

July 2017

CYBER!

Andrea M. Matwyshyn

Follow this and additional works at: <https://digitalcommons.law.byu.edu/lawreview>

 Part of the [Computer Law Commons](#), and the [National Security Law Commons](#)

Recommended Citation

Andrea M. Matwyshyn, *CYBER!*, 2017 BYU L. Rev. 1109 (2018).

Available at: <https://digitalcommons.law.byu.edu/lawreview/vol2017/iss5/6>

This Article is brought to you for free and open access by the Brigham Young University Law Review at BYU Law Digital Commons. It has been accepted for inclusion in BYU Law Review by an authorized editor of BYU Law Digital Commons. For more information, please contact hunterlawlibrary@byu.edu.

CYBER!

Andrea M. Matwysbyn*

This Article challenges the basic assumptions of the emerging legal area of “cyber” or “cybersecurity.” It argues that the two dominant “cybersecurity” paradigms—information sharing and deterrence—fail to recognize that corporate information security and national “cybersecurity” concerns are inextricable. This problem of “reciprocal security vulnerability” means that in practice our current legal paradigms channel us in suboptimal directions. Drawing insights from the work of philosopher of science Michael Polanyi, this Article identifies three flaws that pervade the academic and policy analysis of security, exacerbating the problem of reciprocal security vulnerability—privacy conflation, incommensurability, and internet exceptionalism. It then offers a new paradigm—reciprocal security. Reciprocal security reframes information security law and policy as part of broader security policy, focusing on two key elements: security vigilance infrastructure and defense primacy. The Article concludes by briefly introducing five sets of concrete legal and policy proposals embodying the new reciprocal security paradigm.

CONTENTS

I. INTRODUCTION.....	1111
II. CYBER ALL THE THINGS: WHAT COULD POSSIBLY GO WRONG?	1115

* Professor of law/professor of computer science (by courtesy) at Northeastern University, an affiliate scholar of the Center for Internet and Society at Stanford Law School, and a Senior Fellow of the Cyber Statecraft Initiative of the Atlantic Council. She thanks the US-UK Fulbright Commission and the Princeton Center for Information Technology Policy in the Woodrow Wilson School of Public and International Affairs, where she was the Microsoft Visiting Professor of Technology Policy in 2014–2015 during the writing of this Article. She also wishes to thank Steve Bellovin, Matt Blaze, Ian Brown, Christina J. DeVries, Jen Ellis, Ed Felten, Mark Geistfeld, Rebecca Green, Seda Guerses, Elizabeth Jex, Jake Kouns, Chris Hoofnagle, Yvette Liebesman, Christopher Marsden, Brian Martin, Bronwen Matthews, Terrell McSweeney, Nora Melley, Jennifer Mueller, Helen Nissenbaum, Stephanie Pell, Judith Rauhofer, Martin Redish, Hope Rosen, Lindsey Wegrzyn Rush, Abigail Slater, Mara Tam, Alka Tandan, and Marcia Tiersky for their helpful comments and critiques of this work.

A. Cybers, Cybers Everywhere: New Policy, Same as the Old Policy	1116
1. Cyber is sad: The problem of reciprocal security vulnerability	1121
2. Cybering so hard: Information sharing and deterrence	1126
B. CyberFacepalm: The Three CyberFlaws	1134
1. Ermahgerd, cybers: Privacy conflation	1135
2. Seems cyberlegit: Incommensurability	1145
3. Honeybadger don't cyber: Internet exceptionalism	1154
III. I SEE WHAT YOU CYBERED THERE: KLUDGING TOGETHER A ROBUST SECURITY PARADIGM.....	1161
A. Cybers, How Do They Work?: Lessons from Polanyi...	1162
1. Forever cyberalone: The pain of polycentric problems.....	1164
2. Y U NO cyber?: Transmission of tacit knowledge.	1165
3. Wow! Such cyber: Subsidiary awareness	1167
B. You Had One Cyberjob: The Monty Hall Problem	1169
C. Are You a Cyberwizard?: The Principle of Epistemological Humility.....	1172
IV. CYBERFRIENDSHIP IS MAGIC: RECIPROCAL SECURITY ...	1176
A. Keep Calm and Cyber On: Shifting to Reciprocal Security.....	1177
1. The cyberbox is bigger on the inside: Building a security vigilance infrastructure.....	1178
2. More cybercowbell: Defense primacy.....	1181
B. Cyberchallenge Accepted: Applying Reciprocal Security.....	1184
1. That cyberescalated quickly: Creating security vigilance infrastructure	1185
2. All Your Cyber Are Belong to Us: Defense primacy	1192
V. CONCLUSION: NO CYBERS WERE HURT IN THE WRITING OF THIS ARTICLE.....	1194

I. INTRODUCTION

I have a really bad feeling about this.

—Han Solo (as Ewoks prepare to cook him)¹

Once upon a time, in a galaxy not far away,² there lived the citizens of the Republic of Gadgetopia. For many years, a golden age of technological prosperity reigned over the land—an age of the beauty and the baud.³ Gadgetopia’s gadgets became progressively more magical⁴ and interconnected, even talking to each other through a global network that almost seamlessly connected citizens with each other and their government. But, as Gadgetopia’s citizens reveled in their shiny new world and began to rely on connected gadgets in their daily lives, they failed to notice that their social structures were straining under the weight of these new technologies.

Then, one day, a darker age arrived—an age of the bug and the brick.⁵ Gadgetopia’s magical technologies began to cause harm, malfunctioning because of coding errors and human failures of care. Criminals began to steal information that citizens shared freely through their devices and began to demand ransom.⁶ Government agencies began to lose control of their national security secrets.⁷

1. STAR WARS: EPISODE VI – RETURN OF THE JEDI (Lucasfilm 1983).

2. See generally STAR WARS: EPISODE IV – A NEW HOPE (Lucasfilm 1977) (“A long time ago, in a galaxy far, far away . . .”).

3. See generally The Mentor, *The Conscience of a Hacker*, PHRACK MAGAZINE, Sept. 25, 1986, <http://phrack.org/issues/7/3.html> (“This is our world now. . . the world of the electron and the switch, the beauty of the baud.”).

4. Arthur C. Clarke famously asserted in what is known as Clarke’s third law that “[a]ny sufficiently advanced technology is indistinguishable from magic.” See Esther Inglis-Arkell, *Technology Isn’t Magic: Why Clarke’s Third Law Always Bugged Me*, 109 (Apr. 28, 2013, 11:00 AM), <http://io9.gizmodo.com/technology-isnt-magic-why-clarkes-third-law-always-bug-479194151> (“Arthur C Clarke was a brilliant futurist and writer, but he is probably most widely known for the third of his famous three laws, ‘Any sufficiently advanced technology is indistinguishable from magic.’”).

5. A bricked device is one that has become nonfunctional, meaning that it has basically become an expensive brick. See Chris Hoffman, *What Does “Bricking” a Device Mean?*, HOW-TO GEEK (Sep. 26, 2016), <https://www.howtogeek.com/126665/htg-explains-what-does-bricking-a-device-mean/> (“‘Bricking’ essentially means a device has turned into a brick.”).

6. For a discussion of recent ransomware attacks, see, e.g., Brian Heater, *The Growing Threat of Ransomware*, PC (Apr. 13, 2016, 7:00 AM), <http://www.pcmag.com/news/343547/the-growing-threat-of-ransomware>.

7. For a discussion of technology compromise of national security secrets, see, for example, Mohit Kumar, *After Failed Auction, Shadow Brokers Opens NSA Hacking Tools for*

Gadgetopia's stock markets⁸ and elections⁹ began to demonstrate technological irregularities. Cars began to kill people because of coding errors in brakes¹⁰ and engines¹¹ that car manufacturers had missed or chosen not to fix.¹² Medical devices and hospital machines began to harm patients due to code "glitches" in ways that were impossible for average citizens to monitor and avoid.¹³ Imprudently-connected infrastructure,¹⁴ power grids,¹⁵ and public safety systems¹⁶ began to fail, and Gadgetopia's enemies began to attack it remotely through the very same technologies that had previously brought social prosperity.¹⁷ Eventually, Gadgetopia's citizens stopped trusting their

Direct Sales, THE HACKER NEWS (Dec. 14, 2016), <http://thehackernews.com/2016/12/nsa-hack-shadow-brokers.html>.

8. For a discussion of security vulnerabilities in stock markets, see, for example, Priya Anand, *How Vulnerable Are the U.S. Stock Markets to Hackers?*, MARKETWATCH (July 31, 2015, 11:17 AM), <http://www.marketwatch.com/story/how-vulnerable-are-the-us-stock-markets-to-hackers-2015-07-31>.

9. For a discussion of election system vulnerabilities, see BRENNAN CTR. FOR JUSTICE, VOTING SYSTEM SECURITY AND RELIABILITY RISKS (2016), https://www.brennancenter.org/sites/default/files/analysis/Fact_Sheet_Voting_System_Security.pdf.

10. For a discussion of one vulnerable vehicle, see Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway – With Me in It*, WIRED (July 21, 2015, 6:00 AM), <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/> ("Their code is an automaker's nightmare: software that lets hackers send commands through the Jeep's entertainment system to its dashboard functions, steering, brakes, and transmission, all from a laptop that may be across the country.").

11. *Id.*

12. *Id.*

13. See, e.g., Anne Marie Porrello, *Death and Denial: The Failure of the THERAC-25, A Medical Linear Accelerator* (unpublished Computer Science paper, California Polytechnic State University), <http://users.csc.calpoly.edu/~jdalbey/SWE/Papers/THERAC25.html> (chronicling death or severe radiation injury to patients due to software malfunction in the Therac-25 machine).

14. See, e.g., Erik Larson, Patricia Hurtado & Chris Strohm, *Iranians Hacked from Wall Street to New York Dam, U.S. Says*, BLOOMBERG TECH. (Mar. 24, 2016, 7:20 AM), <https://www.bloomberg.com/news/articles/2016-03-24/u-s-charges-iranian-hackers-in-wall-street-cyberattacks-im6b43tt>.

15. See, e.g., Jamie Condliffe, *Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks*, MIT TECH. REV. (Dec. 22, 2016), <https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/>.

16. See, e.g., Kristen Lee, *It's Scarily Easy to Hack a Traffic Light*, JALOPNIK (Aug. 16, 2016, 8:50 AM), <http://jalopnik.com/its-scarily-easy-to-hack-a-traffic-light-1785313010>.

17. See, e.g., PAUL RUGGIERO & JON FOOTE, U.S. DEP'T OF HOMELAND SEC., CYBER THREATS TO MOBILE PHONES (2011), https://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf.

gadgets, their markets, and their government, and the economy faltered. Things ended badly in Gadgetopia.

Gadgetopia may strike you as a scary place to live. Sadly, however, the story of Gadgetopia is a dystopic but entirely plausible version of the United States' future. We have entered our age of the bug and the brick. Whether our story ends more happily than Gadgetopia's is now up to us. This Article attempts to offer a concrete legal path away from Gadgetopia's fate and toward meaningful security. Despite 105 "cybersecurity" bills introduced in Congress in 2015¹⁸ and the successful passage of federal information sharing legislation, the Cybersecurity Act of 2015,¹⁹ the "emerging national crisis"²⁰ in both public and private sector information security continues to escalate unabated. Why?

Perhaps we are missing the bigger picture. This Article offers that bigger picture and a radically different paradigm for information security regulation. Two ill-suited regulatory models from the last century currently dominate the legal and policy discussions of "cybersecurity" law and policy—information sharing²¹ and deterrence.²² This Article does not attempt to "cyberize" last century's regulatory paradigms for "the cyberspace domain."²³ Instead, this Article highlights the underappreciated reality that corporate information security and national "cybersecurity" are reciprocal and inextricably interwoven. Consequently, it advocates a

18. See, e.g., David J. Bender, *Congress Passes the Cybersecurity Act of 2015*, NAT'L L. REV. (Dec. 20, 2015), <http://www.natlawreview.com/article/congress-passes-cybersecurity-act-2015>; Nick Leiserson & Jen Ellis, *Political Pwnage: The Hacker's Guide to Cybersecurity Policy*, Address at ShmooCon Hacker Convention (Jan. 2016), https://archive.org/details/Political_Pwnage_The_Hackers_Guide_to_Cybersecurity.

19. Bender, *supra* note 18.

20. For testimony of Professor Matt Blaze at Congressional hearing, see Patrick Howell O'Neill, *FBI Slammed on Capitol Hill for 'Stupid' Ideas About Encryption*, DAILY DOT (Apr. 29, 2015), <http://www.dailydot.com/politics/second-crypto-war-hearing-washington/>.

21. See *infra* Section II.A.2.

22. "I think clearly the concepts of deterrence in the cyber domain are still relatively immature. We clearly are not I think where we need to be. . . . This is still the early stages of cyber in many ways." Interview by Jim Sciutto with Mike Rogers, Dir., Nat'l Sec. Agency, https://www.youtube.com/watch?time_continue=32&v=EDZSoCCZU_s (statements at 4:00).

23. The "cyber domain" or "cyberspace domain" is a term used by military officials to refer to internet-enabled information transfers. It is predicated on the notion that the internet is a separate "battlefield," divorced from kinetic space. DEP'T OF THE ARMY, FM 3-38: CYBER ELECTROMAGNETIC ACTIVITIES 1-5, (2014), <http://fas.org/irp/doddir/army/fm3-38.pdf>.

different legal approach—a decentralized, technically-robust regulatory paradigm called “reciprocal security.”

Part II introduces the problem of “reciprocal security vulnerability”—the practical reality that the information security of the private and public sector are inextricably interwoven. It also introduces the emerging legal field that is often called—for better or worse²⁴—“cyber” or “cybersecurity law” and challenges the field’s two dominant regulatory models, information sharing and deterrence. Commenting on the analytical shortcomings of current “cybersecurity” legal scholarship, Part II then dissects three analytical flaws plaguing this “cyberized” legal scholarship and policy on security: privacy conflation, incommensurability, and internet exceptionalism. Next, using the security-related provisions of the Digital Millennium Copyright Act (DMCA) as a security case study, Part II explains how these three flaws have led to unnecessarily adversarial and confused “cybersecurity” rhetoric in both the public and private sector. In fact, current rhetoric is so muddled that it threatens to pit different federal agencies’ missions squarely against each other, simultaneously damaging both innovation and national security.

With the goal of addressing the flaws identified in Part II, Part III introduces the work of seminal philosopher of science Michael Polanyi and highlights his insights on comprehending complicated, “polycentric”²⁵ problems through harnessing “tacit knowledge” with “subsidiary awareness.”²⁶ Borrowing lessons from Polanyi’s work, Part III next uses the cognitive exercise of the Monty Hall problem to advocate reframing legal and policy efforts through introducing an attacker mindset. Finally, Part III applies a healthy dose of what First Amendment scholars have called “epistemological humility.”²⁷ Part IV then introduces a new paradigm known as reciprocal security. Reciprocal security is an innovation-sensitive approach to jointly improve both public and private sector security. Two concrete goals animate the reciprocal security paradigm: creation of a security

24. See *infra* Section II.B.

25. See *infra* Section III.A.1.

26. See *infra* text accompanying notes 394–97.

27. See discussion *infra* Section III.C.

vigilance infrastructure and defense primacy.²⁸ Part IV then briefly introduces five specific light-touch legal and policy proposals embodying the reciprocal security paradigm. These proposals will be explored in greater depth in a subsequent companion essay.²⁹ Part V concludes.

II. CYBER ALL THE THINGS:³⁰
WHAT COULD POSSIBLY GO WRONG?³¹

The world is a dangerous place, Elliott, not because of those who do evil, but because of those who look on and do nothing.

—Mr. Robot³²

The stakes of our national information security debate could not be higher. In December 2016, the White House issued a statement about the ejection of a group of Russian diplomats and levied sanctions against Russia,³³ stating that these diplomatic measures arose as a consequence of Russia’s “significant malicious cyber-enabled activities”³⁴ that “were intended to influence the election, erode faith in US democratic institutions, sow doubt about the integrity of our electoral process, and undermine confidence in the institutions of the US government.”³⁵ Accompanied by a report from the FBI and the Department of Homeland Security,³⁶ the announcement of sanctions

28. See discussion *infra* Section IV.A.

29. Andrea Matwyshyn, *Cyber Harder* (Nov. 17, 2017) (unpublished manuscript) (on file with author).

30. *All the Things*, KNOW YOUR MEME, <http://knowyourmeme.com/memes/all-the-things> (last visited Jan. 12, 2018).

31. *What Could Possibly Go Wrong*, KNOW YOUR MEME, <http://knowyourmeme.com/photos/732258> (last visited Jan. 12, 2018).

32. *Mr. Robot: Ones and Zeroes* (USA television broadcast Jul. 1, 2015).

33. Evan Perez & Daniella Diaz, *White House Announces Retaliation Against Russia: Sanctions, Ejecting Diplomats*, CNN (Jan. 2, 2017, 10:14 PM), <http://www.cnn.com/2016/12/29/politics/russia-sanctions-announced-by-white-house/index.html>.

34. *Id.*

35. *Id.*

36. Sam Thielman, *FBI and Homeland Security Detail Russian Hacking Campaign in New Report*, GUARDIAN, (Dec. 29, 2016, 5:19 PM), <https://www.theguardian.com/technology/2016/dec/29/fbi-dhs-russian-hacking-report>.

followed earlier reports of a CIA assessment that concluded “Russia intervened in the 2016 election.”³⁷ But where do we go from here?

Two regulatory paradigms from last century have dominated our national information security debate—information sharing and deterrence—and, yet, they are both imperfectly suited for the task. Both paradigms fail to address an underlying problem in security: the problem of reciprocal security vulnerability across the public and private sector. Similarly, current legal scholarship on “cybersecurity” also falls short, suffering from three prevalent analytical flaws: privacy conflation, incommensurability, and internet exceptionalism.

*A. Cybers, Cybers Everywhere:*³⁸ *New Policy, Same as the Old Policy*

There’s a zero percent chance of this working.

—Agent Lacy, *The Interview*³⁹

Security engineers sometimes colorfully refer to the unfortunate condition of “rearranging deck chairs on the Titanic”—the situation in which a looming and obvious problem is “addressed” by moving around existing (ineffectual) pieces until disaster inevitably strikes.⁴⁰ In “cybersecurity” law and policy, the “deck chairs” are the various sector-specific⁴¹ paradigms⁴² that comprise our current regulatory

37. Adam Entous, Ellen Nakashima & Greg Miller, *Secret CIA Assessment Says Russia Was Trying to Help Trump Win White House*, WASH. POST (Dec. 9, 2016), https://www.washingtonpost.com/world/national-security/obama-orders-review-of-russian-hacking-during-presidential-campaign/2016/12/09/31d6b300-be2a-11e6-94ac-3d324840106c_story.html?utm_term=.4b50dc226882.

38. *X, X Everywhere*, KNOW YOUR MEME, <http://knowyourmeme.com/memes/x-x-everywhere> (last visited Jan. 12, 2018).

39. THE INTERVIEW (Point Grey Pictures 2014).

40. Doyle Rice, *Titanic Deck Chairs’ Sad Symbolism Lives On*, USA TODAY, <http://usatoday30.usatoday.com/news/nation/story/2012-04-07/titanic-rearrange-deck-chairs/54084648/1> (last updated Apr. 7, 2012, 10:35 AM).

41. *See, e.g.*, 16 C.F.R. § 312 (2017). For HIPAA security rule, see 45 C.F.R. §§ 160, 162, 164 (2017). For GLBA security rules, see 16 C.F.R. § 314 (2017).

42. A common information sharing approach is the creation of sector-specific affinity groups—information sharing and analysis centers (ISACs). *See, e.g.*, AUTO-ISAC, <https://www.automotiveisac.com/> (last visited Jan. 12, 2018); FIN. SERVICES: INFO. SHARING & ANALYSIS CTR., <https://www.fsisac.com/> (last visited Jan. 12, 2018); R-CISC, <https://r-cisc.org/isac/> (last visited Jan. 12, 2018).

approach.⁴³ This segmented approach may seem superficially intuitive in light of traditional legal regulatory approaches and the practical realities of governmental inter-agency politics. It might seem expedient to treat various public and private sector security deficits as discrete and disconnected failures and to simply replace organizational management after each large compromise.⁴⁴ This approach, however, falls victim to the condition of rearranging deck chairs described above: we risk losing sight of the bigger picture as we tinker with small pieces of it.

Two recent large-scale security compromises—those of Sony Pictures Entertainment and the Office of Personnel Management—demonstrate that the problems of security vulnerability are never isolated and discrete. Instead, they plague both the private and public sector reciprocally.⁴⁵ In December 2014, Sony Pictures Entertainment, Inc.,⁴⁶ suffered a significant and far-reaching information security compromise,⁴⁷ allegedly in retaliation for the planned release of the movie, *The Interview*.⁴⁸ Because of Sony's

43. For a discussion of the sector-specific approach to security, see Andrea M. Matwyshyn, *Data Devolution: Corporate Information Security, Consumers, and the Future of Regulation*, 84 CHI.-KENT L. REV. 713 (2010) (explaining dominant, sector-specific federal information security laws).

44. We might also be inclined toward an endless cycle of simply naming, shaming, and replacing organizational leadership for security failures. See, e.g., Evan Perez & Wesley Bruer, *OPM Director Katherine Archuleta Steps Down*, CNN, (July 11, 2015, 10:06 AM), <http://www.cnn.com/2015/07/10/politics/opm-director-resigns-katherine-archuleta/>.

45. For example, Professor Kristin Eichensehr argues that the United States operates under a “de facto system of ‘public-private cybersecurity’ . . . characterized by the surprisingly important, quasi-governmental role of the private sector on many important cybersecurity issues, and correspondingly, by instances in which the federal government acts more like a market participant than a traditional regulator.” See Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467, 470–71 (2017).

46. Kim Zetter, *Sony Got Hacked Hard: What We Know and Don't Know So Far*, WIRED (Dec. 3, 2014, 4:02 PM), <http://www.wired.com/2014/12/sony-hack-what-we-know>.

47. Aly Weisman, *A Timeline of the Crazy Events in the Sony Hacking Scandal*, BUS. INSIDER (Dec. 9, 2014, 4:15 PM), <http://www.businessinsider.com/sony-cyber-hack-timeline-2014-12>.

48. *Id.*

infamously checkered history⁴⁹ of security management,⁵⁰ information security experts immediately asked to what extent Sony's public relations nightmare⁵¹ resulted from the company's own failure to implement reasonable security.⁵² Meanwhile, despite some forensic data possibly to the contrary,⁵³ the FBI and other government sources surprised the security community with a public announcement that the attack was orchestrated by a nation-state actor—North Korea.⁵⁴ But perhaps more troubling than the potentially hasty⁵⁵ attribution⁵⁶

49. Sony was the subject of an FTC consent decree and several state attorney general investigations due to its use of code that resembled a rootkit—a security-compromising code tool used by malicious attackers—in its consumer products. This security invasive code was found in both government and corporate systems, placing them at risk for compromise. For a discussion of the Sony DRM rootkit, see Nate Anderson, *FTC Finally Settles with Sony BMG Over Rootkit*, ARS TECHNICA (Jan. 30, 2007, 4:34 PM), <http://arstechnica.com/business/2007/01/8738/>. For a legal discussion of the problematic nature of security-invasive DRM such as that used by Sony, see Andrea M. Matwysyn, *Technoconsensus*, 85 WASH. U. L. REV. 529 (2007).

50. For example, Sony's PlayStation network was down for an extended period of time due to a previous security compromise. See Samuel Gibbs, *Sony Offers Discounts After Christmas PlayStation Network Hack*, GUARDIAN (Jan. 2, 2015, 6:06 AM), <http://www.theguardian.com/technology/2015/jan/02/sony-christmas-playstation-network-hack-discounts-psn-lizard-squad>; Laura Northrup, *PlayStation Network Users Report Hacked Accounts, Terrible Options from Sony*, CONSUMERIST (Mar. 12, 2015, 12:59 PM), <http://consumerist.com/2015/03/12/playstation-network-users-report-hacked-accounts-terrible-options-from-sony/>; Jose Pagliery, *Why Should We Trust the Sony PlayStation Network Ever Again?*, CNN (Feb. 2, 2015, 12:47 PM), <http://money.cnn.com/2015/02/02/technology/security/sony-playstation-hack/>.

51. See Dave Lewis, *Sony Pictures Data Breach and the PR Nightmare*, FORBES (Dec. 16, 2014, 3:00 AM), <http://www.forbes.com/sites/davelewis/2014/12/16/sony-pictures-data-breach-and-the-pr-nightmare>.

52. Infosec professionals highlight Sony's history of "ongoing problems" of suboptimal security. See Security Curmudgeon, *Absolute Sownage: A Concise History of Recent Sony Hacks*, ATTRITION.ORG (June 4, 2011, 4:17 AM), http://attrition.org/security/rants/sony_aka_sownage.html.

53. Skeptical security experts pointed to alternate theories of the attack based on known facts, including the possibility of an insider attack. See *infra* note 56; Aarti Shahani, *Doubts Persist on U.S. Claims of North Korean Role in Sony Hack*, NPR (Dec. 26, 2014, 4:26 PM), <http://www.npr.org/sections/alltechconsidered/2014/12/26/373303733/doubts-persist-on-u-s-claims-on-north-korean-role-in-sony-hack> (discussing the technical difficulty of correctly attributing attacks when attackers use obfuscatory or "opsec" measures to cover their tracks).

54. See Michael S. Schmidt, Nicole Perlroth & Matthew Goldstein, *F.B.I. Says Little Doubt North Korea Hit Sony*, N.Y. TIMES (Jan. 7, 2015), <https://www.nytimes.com/2015/01/08/business/chief-says-fbi-has-no-doubt-that-north-korea-attacked-sony.html>.

55. However, open questions remain among computer security experts regarding the appropriate attribution of the attack. See Bruce Schneier, *Sony's DRM Rootkit: The Real Story*, SCHNEIER ON SECURITY (Nov. 17, 2005, 9:08 AM), https://www.schneier.com/blog/archives/2005/11/sonys_drm_rootk.html.

56. See Marcus J. Ranum, *Attribution is Hard, Part 1*, TENABLE (Jan. 13, 2015), <https://www.tenable.com/blog/attribution-is-hard-part-1>; Marcus J. Ranum, *Attribution is*

was the impression created by some senior government and military officials that perhaps they⁵⁷ may not have fully anticipated⁵⁸ this particular attack⁵⁹ scenario⁶⁰—the attack of a nation-state actor on a multinational commercial entity.⁶¹ In short, the complicated policy and forensic aftermath of the Sony compromise highlighted a long-standing,⁶² uneasy, and reciprocal relationship⁶³ of corporate information security conduct⁶⁴ and national security matters.⁶⁵

Hard, Part 2, TENABLE (Jan. 20, 2015), <https://www.tenable.com/blog/attribution-is-hard-part-2>.

57. See Phillip Swarts, *NSA Chief Says U.S. Cyber Infrastructure Lags Behind Adversaries, Expects Major Attack*, WASH. TIMES (Feb. 23, 2015), <http://www.washingtontimes.com/news/2015/feb/23/adm-mike-rogers-nsa-director-says-us-infrastructure/>. Mike Rogers, NSA Director Admiral, explained he was surprised by the hack and stated, “I didn’t think it’d go against the motion picture company, to be quite honest . . .” *Id.*; see also Rogers, *supra* note 22.

58. See Swarts, *supra* note 57.

59. The attackers remain at large. See Kim Zetter, *The Sony Hackers Were Causing Mayhem Years Before They Hit the Company*, WIRED (Feb. 24, 2016, 7:00 AM), http://www.wired.com/2016/02/sony-hackers-causing-mayhem-years-hit-company/?mbid=social_twitter.

60. Yet, this threat scenario had been recognized in the private sector for over five years. See Ellen Nakashima, *Chinese Hackers Who Breached Google Gained Access to Sensitive Data, U.S. Officials Say*, WASH. POST (May 20, 2013), https://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html; Kim Zetter, *Google Hack Attack Was Ultra Sophisticated, New Details Show*, WIRED (Jan. 14, 2010, 8:01 PM), <http://www.wired.com/2010/01/operation-aurora>.

61. Some reports indicated, however, that attribution was facilitated by information obtained from the National Security Agency. See David E. Sanger & Martin Fackler, *N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say*, N.Y. TIMES (Jan. 18, 2015), http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?_r=0 (“The evidence gathered by the ‘early warning radar’ of software painstakingly hidden [by the NSA] to monitor North Korea’s activities.”).

62. This relationship goes at least as far back as Crypto War I. See Bruce Schneier, *History of the First Crypto War*, SCHNEIER ON SECURITY (June 22, 2015, 1:35 PM), https://www.schneier.com/blog/archives/2015/06/history_of_the_.html.

63. See Sam Biddle, *The NSA Leak Is Real, Snowden Documents Confirm*, INTERCEPT (Aug. 19, 2016, 6:00 AM), <https://theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm/>.

64. See Michelle Fox, *The Risk of Contractors is Real, Justice Dept. National Security Head Says*, CNBC (Oct. 5, 2016, 3:04 PM), <https://www.cnbc.com/2016/10/05/the-risk-of-contractors-is-real-justice-dept-national-security-head-says.html>; see also Carol Matlack, Michael Riley & Jordan Robertson, *The Company Securing Your Internet Has Close Ties to Russian Spies*, BLOOMBERG (Mar. 19, 2015, 6:00 AM), <https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies>.

65. The FBI appeared somewhat quick to assert that the attack on Sony originated in North Korea. See Alex Hern, *FBI Doubles Down on North Korea Accusation for Sony Pictures Hack*, GUARDIAN (Jan. 8, 2015, 11:07 AM), <http://www.theguardian.com/technology/2015/jan/08/fbi-north-korea-accusation-sony-pictures-hack>. However, the technical comm-

This question of the inextricable nature of public-private sector security vulnerability surfaced again six months later. In June 2015,⁶⁶ the Office of Personnel Management (OPM) revealed that it had suffered at least two large data breaches,⁶⁷ implicating a private sector contractor as the responsible party.⁶⁸ Described by experts as “an absolute calamity”⁶⁹ whose national security impact may last forty years or more,⁷⁰ the breaches exposed over 21 million⁷¹ records of federal employees,⁷² including those of covert CIA operatives.⁷³ Troublingly, investigations⁷⁴ appear to indicate that the breach was likely avoidable⁷⁵ and that OPM had a “long history of systemic

unity of security experts remained unconvinced in significant part regarding North Korea’s involvement. *E.g.*, Bruce Schneier, *We Still Don’t Know Who Hacked Sony*, ATLANTIC (Jan. 5, 2015), <http://www.theatlantic.com/international/archive/2015/01/we-still-dont-know-who-hacked-sony-north-korea/384198>.

66. Evan Perez & Shimon Prokupecz, *First on CNN: U.S. Data Hack May Be 4 Times Larger than the Government Originally Said*, CNN (June 24, 2015, 2:59 AM), <http://edition.cnn.com/2015/06/22/politics/opm-hack-18-million/index.html>.

67. *Cyber Security Resource Center*, U.S. OFFICE PERSONNEL MGMT., <https://www.opm.gov/cybersecurity> (last visited Jan. 1, 2018). For a discussion of the OPM compromise, see, for example, Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, WASH. POST (July 9, 2015), <http://www.washingtonpost.com/blogs/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/>. See, *e.g.*, Kenneth Corbin, *How OPM Data Breach Could Have Been Prevented*, CIO (July 13, 2015, 4:10 AM), <http://www.cio.com/article/2947453/data-breach/how-opm-data-breach-could-have-been-prevented.html>.

68. See Aaron Boyd, *Contractor Breach Gave Hackers Keys to OPM Data*, FED. TIMES (June 23, 2015), <http://www.federaletimes.com/story/government/omr/opm-cyber-report/2015/06/23/keypoint-isis-opm-breach/28977277/>.

69. Andrew Tilghman & David B. Larter, *Military Clearance OPM Data Breach ‘Absolute Calamity’*, NAVY TIMES (June 17, 2015), <http://www.navytimes.com/story/military/2015/06/17/sf-86-security-clearance-breach-troops-affected-opm/28866125/>.

70. See Dan Verton, *Impact of OPM Breach Could Last More than 40 Years*, FEDSCOOP (July 10, 2015), <http://fedscoop.com/opm-losses-a-40-year-problem-for-intelligence-community>.

71. This figure is over five times larger than OPM’s original estimates. See Corbin, *supra* note 67.

72. See Joe Davidson, *New OPM Data Breach Numbers Leave Federal Employees Anguished, Outraged*, WASH. POST (July 9, 2015), <http://www.washingtonpost.com/blogs/federal-eye/wp/2015/07/09/new-opm-data-breach-numbers-leave-federal-employees-anguished-outraged/>.

73. See Nakashima, *supra* note 67.

74. Perhaps most tellingly, the U.S. Government Accountability Office had rated the OPM cybersecurity apparatus a “D.” Kaveh Waddell, *OPM Just Now Figured Out How Much Data It Owns*, ATLANTIC (Nov. 30, 2015), <https://www.theatlantic.com/technology/archive/2015/11/opm-just-figured-out-how-much-data-it-owns/417669/>.

75. See Corbin, *supra* note 67.

failures to properly manage its IT infrastructure.”⁷⁶ Although the facts differed from the Sony breach, again the private and public sector elements of security co-mingled inextricably. This problem of interdependence of public and private sector information security is what we might term *the problem of reciprocal security vulnerability*.

1. *Cyber is sad*:⁷⁷ *The problem of reciprocal security vulnerability*

I don't know about you, but I intend to write a strongly worded letter to the White Star Line about all of this.

—Jack, *Titanic*⁷⁸

As the Sony and OPM compromises illustrate, information security problems are often not discrete, organizational problems. They are instead often cross-cutting, sector-neutral problems that impact third parties. The reason is a technical one: effective security requires vigilant coordination across institutional and legal silos *wherever the particular vulnerable code has been deployed*. In other words, technologically speaking, we need to fix all the vulnerable systems in both the public and the private sector because the compromise of *either* could potentially lead to compromise of *both*. Public sector and private sector information security concerns cannot be discretely cabined off from each other.⁷⁹ This technical reality underpins the problem of reciprocal security vulnerability.

The problem of reciprocal security vulnerability is pervasive. Vulnerable critical infrastructure systems—smart grids,⁸⁰ power and

76. *Id.* (quoting *IT Spending and Data Security at OPM Hearing Before the S. Comm. On Appropriations*, 114th Cong (2015) (statement of Michael R. Esser, Assistant Inspector General for Audits), <https://www.appropriations.senate.gov/imo/media/doc/Esser%20Testimony.pdf>).

77. *Keanu Is Sad / Sad Keanu*, KNOW YOUR MEME, <http://knowyourmeme.com/memes/keanu-is-sad-sad-keanu> (last visited Jan. 1, 2018).

78. *TITANIC* (Paramount Pictures 1997).

79. For example, the infamous Heartbleed vulnerability impacted both public and private systems. See Julie Pace, *HealthCare.gov Website Flagged in Heartbleed Review*, NBC 10 (Apr. 19, 2014, 8:36 AM), <http://www.nbcphiladelphia.com/news/national-international/Heartbleed-computer-bug-Open-SSL-Homeland-Security-Department-HealthCaregov-President-Obama-healthcare-cybersecurity-255850391.html>.

80. See, e.g., CAL. STATE UNIV. SACRAMENTO, SMART GRID CYBER SECURITY POTENTIAL THREATS, VULNERABILITIES AND RISKS (2012), <http://www.energy.ca.gov/2012publications/CEC-500-2012-047/CEC-500-2012-047.pdf>.

water stations,⁸¹ air traffic control systems⁸² and other communication systems,⁸³ health systems,⁸⁴ and nuclear power plants⁸⁵—all blend private and public-sector elements, simultaneously impacting both national security and consumer protection concerns. For example, some nuclear submarines run a version of Windows XP, a private sector operating system.⁸⁶ With the right malware, compromised networks of personal computers,⁸⁷ consumer smartphones,⁸⁸ and even Internet of Things (IoT) webcams⁸⁹ can easily be remotely repurposed for

81. See Kim Zetter, *Researchers Uncover Holes that Open Power Stations to Hacking*, WIRED (Oct. 16, 2013, 12:00 PM), <http://www.wired.com/2013/10/ics/>.

82. See Heather Kelly, *Researcher: New Air Traffic Control System is Hackable*, CNN (July 26, 2012, 6:49 PM), <http://www.cnn.com/2012/07/26/tech/web/air-traffic-control-security>.

83. See NAT'L CYBER SEC. DIV. CONTROL SYS. SEC. PROGRAM, POTENTIAL VULNERABILITIES IN MUNICIPAL COMMUNICATIONS NETWORKS (2006), https://ics-cert.us-cert.gov/sites/default/files/documents/Potential_Vulnerabilities_Municipal_Communications_Networks_v1_S508C.pdf.

84. See, e.g., Dan Kaplan, *Indiana University Hospital Hacked to Steal Data*, SC MEDIA, <http://www.scmagazine.com/indiana-university-hospital-hacked-to-steal-data/article/225887/> (last visited Jan. 12, 2018).

85. See Andy Greenberg, *America's Hackable Backbone*, FORBES (Aug. 22, 2007, 6:00 PM), http://www.forbes.com/2007/08/22/scada-hackers-infrastructure-tech-security-cx_ag_0822hack.html.

86. See Kyle Mizokami, *Britain's Doomsday Nuke Subs Still Run Windows XP*, POPULAR MECHANICS (Jan. 21, 2016), <http://www.popularmechanics.com/military/weapons/a19061/britains-doomsday-subs-run-windows-xp/>.

87. See Andy Greenberg, *Hackers Are Already Using the Shellshock Bug to Launch Botnet Attacks*, WIRED (Sept. 25, 2014, 4:49 PM), <http://www.wired.com/2014/09/hackers-already-using-shellshock-bug-create-botnets-ddos-attacks/>.

88. See Steven J. Vaughan-Nichols, *First Case of Android Trojan Spreading Via Mobile Botnets Discovered*, ZDNET (Sept. 5, 2013, 9:33 AM), <http://www.zdnet.com/first-case-of-android-trojan-spreading-via-mobile-botnets-discovered-7000020292/>.

89. See Lily Hay Newman, *The Botnet that Broke the Internet Isn't Going Away*, WIRED (Dec. 9, 2016, 7:00 AM), <https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/>.

attacking critical national assets⁹⁰ such as stock exchanges,⁹¹ dams,⁹² or power grids.⁹³

To crystalize the problem of reciprocal security vulnerability, let us briefly analyze a case study of another Sony public relations nightmare. In 2005, Sony imprudently deployed overzealous digital rights management (DRM)⁹⁴ technology in some of its music CDs. This DRM code has been described by experts as a rootkit—a security-invasive tool used by malicious attackers to open a backdoor into a system while hiding from the machine’s owner.⁹⁵ Although Sony considered this security-invasive DRM to be a reasonable exercise of the type of intellectual property protection⁹⁶ authorized by the DMCA, the practical result was a national security emergency.⁹⁷ Unsuspecting federal and private sector employees played Sony music CDs infected with this DRM in their work machines, which caused the security compromise of “many military and government networks,”⁹⁸ including the networks of the Department of Defense

90. Purchasing time on a botnet for purposes of attacking infrastructure is relatively inexpensive. See Dancho Danchev, *Study Finds the Average Price for Renting a Botnet*, ZDNET (May 26, 2010, 7:16 AM), <http://www.zdnet.com/article/study-finds-the-average-price-for-renting-a-botnet/>. The price for botnet creation kits has now fallen to approximately \$20. See Tim G., *Renting a Zombie Farm: Botnets and the Hacker Economy*, SYMANTEC (Aug. 8, 2014), <http://www.symantec.com/connect/blogs/renting-zombie-farm-botnets-and-hacker-economy>.

91. See, e.g., Michael Riley, *How Russian Hackers Stole the Nasdaq*, BLOOMBERG (July 21, 2014, 2:11 PM), <http://www.businessweek.com/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq>.

92. See, e.g., Joseph Berger, *A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case*, N.Y. TIMES (Mar. 25, 2016), https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html?_r=0.

93. See, e.g., Jamie Condliffe, *Ukraine’s Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks*, MIT TECH. REV. (Dec. 22, 2016), <https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/>.

94. Mark Russinovich, *Sony, Rootkits and Digital Rights Management Gone Too Far*, MICROSOFT: MARK’S BLOG (Oct. 31, 2005, 11:04 AM), <https://blogs.technet.microsoft.com/markrussinovich/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far/>.

95. *Id.*

96. Schneier, *supra* note 55.

97. *Id.*

98. Robert Lemos, *Researcher: Sony BMG “Rootkit” Still Widespread*, SECURITYFOCUS (Jan. 16, 2006), <http://www.securityfocus.com/news/11369>.

and the Department of Homeland Security.⁹⁹ Security experts estimate that over 500,000 networks were compromised by the Sony DRM,¹⁰⁰ and owners alleged millions of dollars of damage to those systems.¹⁰¹ In other words, private sector computer code caused a national security problem.

Now, more than a decade later, flawed code¹⁰² in IoT¹⁰³ devices exposes consumers, public¹⁰⁴ and private sector employers,¹⁰⁵ and our national defense to security risks in somewhat parallel ways. As Professors Scott Peppet¹⁰⁶ and Paul Ohm¹⁰⁷ have correctly noted in the context of IoT, the legal discussion about regulating software changes

99. Schneier, *supra* note 55.

100. Lemos, *supra* note 98 (“[R]esearch . . . suggested some 570,000 networks had computers affected by the software . . .”).

101. Ingrid Marson, *Sony Settles ‘Rootkit’ Class Action Lawsuit*, C|NET (Dec. 29, 2005, 9:17 AM), <https://www.cnet.com/news/sony-settles-rootkit-class-action-lawsuit/>; see also Elizabeth Bowles & Eran Kahana, *The ‘Agreement’ that Sparked a Storm*, BUS. L. TODAY, Jan. & Feb. 2007, <https://apps.americanbar.org/buslaw/blt/2007-01-02/kahana.shtml>.

102. For example, in one study, HP Fortify analyzed ten IoT devices in 2015, and found that each device had about twenty-five vulnerabilities. HEWLETT PACKARD ENTERS., INTERNET OF THINGS RESEARCH STUDY: 2015 REPORT (2015), <http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en>; see also Matthew Sparkes, *Average Internet of Things Device Has 25 Security Flaws*, TELEGRAPH (July 30, 2014, 11:26 AM), <http://www.telegraph.co.uk/technology/internet-security/11000013/Average-Internet-of-Things-device-has-25-security-flaws.html>.

103. According to the FTC, “[t]he Internet of Things (‘IoT’) refers to the ability of everyday objects to connect to the Internet and to send and receive data.” FTC STAFF, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD, at ii (2015), <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>.

104. Pacemakers have similarly raised security concerns. See, e.g., Andrea Peterson, *Yes, Terrorists Could Have Hacked Dick Cheney’s Heart*, WASH. POST: THE SWITCH (Oct. 21, 2013), <http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart>.

105. For example, vulnerable Internet of Things devices risk compromising corporate networks. See Mark Piesing, *Hacking Attacks on Printers Still Not Being Taken Seriously*, GUARDIAN (July 23, 2012, 6:29 AM), <http://www.theguardian.com/technology/2012/jul/23/hacking-attack-printers>.

106. Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85 (2014) (arguing sensor-based technologies including the Internet of Things devices will be inherently prone to security flaws, and the difficulty of meaningful consumer consent in this context can create discrimination, privacy, security, and consent problems).

107. Paul Ohm & Blake Reid, *Regulating Software When Everything Has Software*, 84 GEO. WASH. L. REV. 1672 (2016) (arguing that a shift in the modern administrative state is underway from the regulation of things to the regulation of code).

when software becomes part¹⁰⁸ of most products.¹⁰⁹ IoT products can be leveraged to surreptitiously compromise the confidentiality of systems,¹¹⁰ attack others' systems,¹¹¹ put employers¹¹² or children at risk,¹¹³ and even physically¹¹⁴ harm¹¹⁵ their human owners.¹¹⁶ These problems exist regardless of whether the vulnerable devices are deployed in the public or private sector.

Legal scholars and policymakers have generally failed to recognize this problem of reciprocal security vulnerability as dispositive for the ways that we regulate security. As such, the two dominant legal

108. Code errors also have also been found in IoT medical devices including radiation machines. At least six people died or were seriously injured due to a software malfunction, security flaw or vulnerability in the Therac 25 radiation machine. See Nancy G. Leveson & Clark S. Turner, *An Investigation of the Therac-25 Accidents*, COMPUTER, July 1993, at 18.

109. For a discussion of product liability and IoT, see, for example, Mauricio Paez & Mike La Marca, *The Internet of Things: Emerging Legal Issues for Businesses*, 43 N. KY. L. REV. 29 (2016) (analyzing unsettled legal issues for businesses to consider when evaluating IoT adoption).

110. Even our smart toilets can be compromised—a truly crappy state of information security affairs. See Kashmir Hill, *When 'Smart Homes' Get Hacked*, FORBES (July 26, 2013, 9:15 AM), <http://www.forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/>.

111. IoT cameras were recently harnessed as part of the Mirai botnet. For a discussion of Mirai, see, for example, Newman, *supra* note 89.

112. See, e.g., William J. Barath, *The Internet of Things: Don't Forget Your Employees*, LAW360 (Sept. 2, 2016, 4:29 PM), <https://www.law360.com/articles/836130/the-internet-of-things-don-t-forget-your-employees>.

113. For example, baby monitors have experienced vulnerabilities allowing remote attackers to monitor children. See, e.g., Nitesh Dhanjani, *The Belkin WeMo Baby Monitor, the WeMo Switch, and the Wi-Fi NetCam*, DHANJANI.COM (Oct. 22, 2013), <http://www.dhanjani.com/blog/2013/10/the-belkin-wemo-baby-monitor-the-wemo-switch-and-the-wi-fi-netcam.html> (reviewing vulnerabilities in a specific internet camera).

114. At least one person has boasted of remotely modifying the thermostat of his ex-spouse. See *Guy Trolls His Ex-wife via Programmable Thermostat*, REDDIT, [https://www.reddit.com/r/ProRevenge/comments/2cme0c/guy_trolls_his_exwife_via_programmable_thermosta t/](https://www.reddit.com/r/ProRevenge/comments/2cme0c/guy_trolls_his_exwife_via_programmable_thermosta_t/) (last visited Jan. 12, 2018).

115. A vulnerable toaster could potentially be made to overheat and start a fire. Water heaters could be made to explode potentially, if settings are manipulable. See Kashmir Hill, *The Terrifying Search Engine That Finds Internet-Connected Cameras, Traffic Lights, Medical Devices, Baby Monitors and Power Plants*, FORBES (Sept. 4, 2013, 10:35 AM), <https://www.forbes.com/sites/kashmirhill/2013/09/04/shodan-terrifying-search-engine/#4b268b0f525d>.

116. IoT medical devices present a similar list of troubling vulnerabilities. Insulin pumps have presented security threats. See, e.g., Jordan Robertson, *McAfee Hacker Says Medtronic Insulin Pumps Vulnerable to Attack*, BLOOMBERG (Feb. 29, 2012, 8:00 AM), <http://www.bloomberg.com/news/2012-02-29/mcafee-hacker-says-medtronic-insulin-pumps-vulnerable-to-attack.html>.

“cybersecurity” paradigms—information sharing and deterrence—are not an ideal fit.

2. *Cybering so hard*:¹¹⁷ *Information sharing and deterrence*

Politicians, like generals, have a tendency to fight the last war.

—John Bolton¹¹⁸

Although information security professionals warned Congress of the dire state of security over fifteen years ago,¹¹⁹ widespread political acknowledgment and legal interest in this “emerging national crisis”¹²⁰ has only recently emerged. Despite intense,¹²¹ recent Congressional interest¹²² in “cybersecurity,”¹²³ or simply “cyber,”¹²⁴ the two dominant legal approaches to information security—information

117. *Adulting*, KNOW YOUR MEME, <http://knowyourmeme.com/memes/adulting> (last visited Jan. 12, 2018).

118. See Robert Mann, *This Is Why David Vitter Lost: Gutter Politics from a Prostitute-Procuring Politician Don't Work Against a Conservative Democrat from West Point*, SALON (Nov. 22, 2015, 3:59 AM), http://www.salon.com/2015/11/22/this_is_why_david_vitter_lost_gutter_politics_from_a_prostitute_procuring_politician_dont_work_against_a_conservative_democrat_from_west_point/ (“Politicians, like generals, have a tendency to fight the last war.” — John Bolton”).

119. Craig Timberg, *Net of Insecurity: A Disaster Foretold — and Ignored*, WASH. POST (June 22, 2015), <http://www.washingtonpost.com/sf/business/2015/06/22/net-of-insecurity-part-3/>; *Computer Security in Government: Is the Public at Risk?: Hearing Before S. Comm. On Homeland Sec. & Governmental Affairs*, 105th Cong. (1998), https://www.youtube.com/watch?v=VVJldn_MmMY.

120. See O'Neill, *supra* note 20 (testimony of Professor Blaze).

121. At least 105 proposals related to “cybersecurity” were introduced during the 2015 legislative session. David J. Bender, *Congress Passes the Cybersecurity Act of 2015*, NAT. L. REV. (Dec. 20, 2015), <http://www.natlawreview.com/article/congress-passes-cybersecurity-act-2015>.

122. See, e.g., *Promoting and Incentivizing Cybersecurity Best Practices: Hearing Before the Subcomm. on Cybersecurity and Infrastructure Protection of the H. Comm. of Homeland Sec.*, 114th CONG. 1 (2015), <https://homeland.house.gov/hearing/subcommittee-hearing-promoting-and-incentivizing-cybersecurity-best-practices>.

123. For an explanation of why “cybersecurity” is a suboptimal term, see *infra* Section II.B.3.

124. See, e.g., U.S. DEP'T OF DEFENSE, *THE DOD CYBER STRATEGY* (2015), https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (explaining that “Cyber” is a prefix, not a noun).

sharing¹²⁵ and deterrence¹²⁶—are unfortunately primarily a rehashing of last century’s legal approaches. As such, they are a suboptimal fit for grappling with this century’s security challenges, challenges whose hallmark feature is the problem of reciprocal security vulnerability.

a. Information sharing. Information sharing paradigms have been used for decades in various regulatory and self-regulatory initiatives.¹²⁷ They underpin bodies of law, such as securities regulation¹²⁸ and patent law,¹²⁹ in which certain benefits are granted in exchange for socially useful self-reporting. As Professor Julie Cohen has argued, the discourse of information policy reform has also often been organized principally around the theme of access to information.¹³⁰ Therefore, it is perhaps unsurprising¹³¹ that information sharing is the paradigm at the heart of the Cybersecurity Act of 2015.¹³² Specifically, the Act

125. See *infra* text accompanying notes 127–39.

126. See *infra* text accompanying notes 140–78.

127. For a discussion of information sharing, see, for example, Elena Kagan, *Presidential Administration*, 114 HARV. L. REV. 2245, 2353 (2001) (“The ever-widening appreciation of the role of cost-benefit analysis and comparative risk assessment in the formulation of administrative policy testifies to this need; so too does the emerging call for experimentalism and information sharing”) (citation omitted); Robert L. Rabin, *Federal Regulation in Historical Perspective*, 38 STAN. L. REV. 1189, 1192 (1986) (“[U]ntil the New Deal, a policing model of regulation invariably triumphed over efforts to elicit government support for various forms of business price-fixing, information-sharing and market-allocating schemes—regulatory initiatives which I will refer to as associational forms of regulation.”); David J. Teece, *Information Sharing, Innovation, and Antitrust*, 62 ANTITRUST L.J. 465 (1994).

128. See, e.g., Bruce A. Hiler, *The SEC and the Courts’ Approach to Disclosure of Earnings Projections, Asset Appraisals, and Other Soft Information: Old Problems, Changing Views*, 46 MD. L. REV. 1114 (1987) (explaining historical reliance of securities regulation on information disclosure and sharing obligations); Brian Lewis et al., *Securities Fraud*, 52 AM. CRIM. L. REV. 1567, 1634 (2015) (“Most recently, the SEC became a signatory to the International Organization of Securities Commissions (‘IOSCO’) MOU, the first global multilateral information-sharing arrangement.”).

129. See, e.g., Stephen Yelderman, *Coordination-Focused Patent Policy*, 96 B.U. L. REV. 1565, 1588 (2016) (discussing patent law as a system of information coordination where “success is measured by the amount of privately beneficial information sharing that occurs in reliance on patent rights”).

130. See, e.g., JULIE E. COHEN, *CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE* 223 (2012) (“Within U.S. legal and policy circles, the discourse of information policy reform has been organized principally around the themes of access to knowledge and network neutrality.”).

131. See, Derek E. Bambauer, *Sharing Shortcomings*, 47 LOY. U. CHI. L.J. 465, 465 (2015) (“Current cybersecurity policy emphasizes increasing the sharing of threat and vulnerability information. Legal reform is seen as crucial to enabling this exchange”).

132. See Cybersecurity Act of 2015, Pub. L. No. 114-113, § 102(13), 129 Stat. 2242, 2938 (2015).

created a regime in which entities are encouraged to voluntarily “monitor” their “information system” for “cybersecurity purposes.”¹³³ The Act granted authority to use defensive measures¹³⁴ and to provide information to a federal or nonfederal entity in exchange for a limitation of liability¹³⁵ under the Electronic Communications Privacy Act (ECPA)¹³⁶ and other privacy laws.¹³⁷

Superficially, such an approach may appear to target the problem of reciprocal security vulnerability. However, upon closer inspection, it actually may obscure and exacerbate the problem. Professor Orin Kerr has correctly argued that a lack of definitional clarity exists regarding what constitutes a “cybersecurity purpose” for purposes of the Act.¹³⁸ Similarly, the Act creates a voluntary information sharing regime in which the most egregious security deficits may also be the most likely to go undisclosed and unaddressed in both the public and private sector.

As Part IV will explain, most security information sharing statutes fail to address a dispositive, pre-existing problem: a deficit in the underlying information “infrastructures” required to create accurate and meaningful technical context for the shared security information. These types of information security infrastructures are necessary *precursors* to effective private and public-sector information sharing regimes.¹³⁹ Without first correcting underlying security infrastructure

133. *See id.* § 104(a).

134. *See id.* § 104(b).

135. *See id.* § 106.

136. For a discussion of ECPA’s approach, see, for example, 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 (2004) (explaining the historical background and structure of ECPA).

137. *See, e.g.*, Jennifer Granick, *OmniCISA Pits DHS Against the FCC and the FTC on User Privacy*, JUST SECURITY (Dec. 16, 2015, 6:09 PM), <https://www.justsecurity.org/28386/omnicisa-pits-government-against-self-privacy/>.

138. *See* Orin Kerr, *How Does the Cybersecurity Act of 2015 Change the Internet Surveillance Laws?*, WASH. POST (Dec. 24, 2015), <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/12/24/how-does-the-cybersecurity-act-of-2015-change-the-internet-surveillance-laws/>.

139. For example, this lesson regarding how absence of infrastructures results in information sharing failures was amply demonstrated by the Books and Records Crisis in the financial markets in the late 1960s-early 1970s. For a discussion of the Books and Records Crisis, see, for example, Andrea M. Matwyshyn, *Corporate Cyborgs and Technology Risks*, 11 MINN. J.L. SCI. & TECH. 573, 573–74 (2010) (“Using the securities industry as a case study . . . this article points to the historical example of the Books and Records Crisis that plagued the securities markets in the 1960s and 1970s and required SEC intervention.”).

deficits, information-sharing approaches that trade liability limitation for voluntary security “information” are limited in their effectiveness from inception.

b. Deterrence. In any circumstance involving criminal conduct, a superficially appealing and uncontroversial legal paradigm will be rooted in deterrence. In theory, subsequent sanctions for computer intrusions and security violations might dissuade would-be perpetrators from engaging in criminality. As explained by Professor Daniel Medwed,¹⁴⁰ deterrence has long been a core goal of criminal law, law enforcement, and defense initiatives.¹⁴¹ To wit, the Department of Justice’s dominant enforcement paradigm in approaching information security can be described as one focused on deterrence,¹⁴² and U.S. Cyber Command identifies deterrence as a key goal,¹⁴³ although disagreement exists regarding what exactly this deterrence posture means in practice.¹⁴⁴

But, in practice, because of the problem of reciprocal security vulnerability, the picture is more complex than contemplated by these usual models of deterrence. Attackers’ behaviors and strategies strain these traditional notions of deterrence, with respect to both definition, on the one hand, and enforcement reality, on the other.¹⁴⁵ Even if we assume for the sake of argument that the meaning of deterrence is

140. See Daniel S. Medwed, *Deterrence Theory and the Corporate Criminal Actor: Professor Utset’s Fresh Take on an Old Problem*, 1 VA. J. CRIM. L. 329, 329 (2013) (“Deterrence is a core theory underlying much of American criminal law.”).

141. For discussion of the role of deterrence in criminal law, see, for example, Steven Shavell, *Criminal Law and the Optimal Use of Nonmonetary Sanctions as a Deterrent*, 85 COLUM. L. REV. 1232 (1985) (analyzing the theoretically optimal use of nonmonetary sanctions as a deterrent); Note, *Victim Restitution in the Criminal Process: A Procedural Analysis*, 97 HARV. L. REV. 931, 937 (1984) (explaining the role of deterrence in criminal law and arguing that “restitution is best suited to the criminal sphere” rather than a deterrence focus).

142. See Orin S. Kerr, *Cybercrime’s Scope: Interpreting “Access” and “Authorization” in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1656 (2003) (“In the context of computer crimes, the most important of these utilitarian goals is deterrence . . .”).

143. Leticia Hopkins, *Fighting in the Cyber Domain: US Army Central Creates Cyberspace Strategy*, U.S. ARMY (Dec. 23, 2016), https://www.army.mil/article/180101/fighting_in_the_cyber_domain_us_army_central_creates_cyberspace_strategy (“The strategy seeks to deter current and emerging threats . . .”).

144. See Jan Kallberg, *After Twenty Years of Cyber – Still Unchartered Territory Ahead*, CYBER DEF. REV. (Dec. 28, 2016), <http://www.cyberdefensereview.org/2016/12/28/after-twenty-years-of-cyber/> (“From a military standpoint, there is still a debate about what cyber deterrence would look like . . .”).

145. *Id.*

straightforward in U.S. domestic criminal contexts, information security criminality and deterrence are not solely domestic.¹⁴⁶ As a result, at least two different (sets of) field-specific definitions of “deterrence” currently clash in information security—one from domestic criminal law and the other from international relations theory.¹⁴⁷ While the domestic definition of deterrence involves discouraging criminals from engaging in crime, the international relations framing of “deterrence” questions is more complex. Questions of information security on an international level also involve national security questions of international criminality, espionage, and international conflict.¹⁴⁸ As explained by Ann-Marie Slaughter, several different schools of thought exist with respect to international relations theory,¹⁴⁹ and each of these schools analyzes questions of “deterrence” differently.¹⁵⁰

With respect to enforcement, the practical difficulties of attack attribution and logistics of criminal prosecution across international boundaries make successful deterrence less likely. Therefore, even assuming domestic information security criminality can be partially deterred,¹⁵¹ international criminality, particularly criminality arising

146. Tonya L. Putnam & David D. Elliott, *International Responses to Cyber Crime*, in THE TRANSNATIONAL DIMENSION OF CYBER CRIME AND TERRORISM 35 (Abraham D. Sofaer & Seymour E. Goodman eds., 2001), http://www.hoover.org/sites/default/files/uploads/documents/0817999825_35.pdf (“Concerned technical experts well understand that information security issues are inherently and unavoidably global in nature.”).

147. For a discussion of various theories and strategies of deterrence in international contexts, see, for example, Branislav L. Slantchev, *Introduction to International Relations Lecture 8: Deterrence and Compellence*, U.C. SAN DIEGO (May 2, 2005), <http://slantchev.ucsd.edu/courses/ps12/08-deterrence-and-compellence.pdf>.

148. See Harold Edgar & Benno C. Schmidt, Jr., *The Espionage Statutes and Publication of Defense Information*, 73 COLUM. L. REV. 929, 1084 (1973) (“[F]or deterrence purposes the penalties for espionage are and should be exceptionally steep.”); Melanie J. Teplinsky, *Cybersecurity and the Cyberthreat Deterrence Trend*, in RECENT TRENDS IN NATIONAL SECURITY LAW (2015 ed.) (“The goal of threat deterrence is to make cyber espionage so costly that it no longer pays. Cyber espionage can be made more costly through improved detection, attribution, and punishment of cyber intruders.”).

149. Anne-Marie Slaughter, *International Relations, Principal Theories*, in MAX PLANCK ENCYCLOPEDIA OF PUB. INT’L L. (Wolfrum, R. ed., 2011), https://www.princeton.edu/~slaughter/Articles/722_IntlRelPrincipalTheories_Slaughter_20110509zG.pdf.

150. *Id.*

151. Not all commentators agree that deterrence presents the most desirable strategy in either traditional criminal law contexts or technology contexts. See, e.g., *Victim Restitution*, *supra* note 141 (explaining the role of deterrence in criminal law and arguing that “restitution is best suited to the criminal sphere” rather than a deterrence focus).

from countries without extradition agreements with the United States or with interests adverse to the United States, is highly unlikely to be substantially deterred. Attacks also often come from non-state actors¹⁵² outside U.S. jurisdictional reach.¹⁵³ While it is true that these non-state actors sometimes work at the request of a hostile foreign group or nation state, they nevertheless upend the traditional power asymmetries that have worked in favor of law enforcement.¹⁵⁴ Although non-state actors¹⁵⁵ have historically faced challenges in obtaining and deploying conventional weapons in physical space, the right security vulnerability and exploit for an attack may be available for purchase or discovery from the comfort of home.¹⁵⁶ An effective

152. See, e.g., George Jackson, *Hayden: Rogue Attacks are the Biggest Cyber Threat*, GOVERNMENT MATTERS (June 2, 2016), <http://govmatters.tv/hayden-rogue-attacks-are-the-biggest-cyber-threat/>.

153. Professor Susan Brenner and a co-author explain that:

Courts have invoked four different bases, or “nexuses,” to justify their exercise of jurisdiction in criminal cases: (1) the territorial nexus, i.e., where the offense was committed; (2) the nationality of the person committing the offense; (3) a protective nexus that allows the exercise of jurisdiction when a national interest of the forum state is at stake; and (4) the universality nexus which gives courts jurisdiction over “certain offenses that are recognized by the community of nations as being of universal concern.”

Susan W. Brenner & Bert-Jaap Koops, *Approaches to Cybercrime Jurisdiction*, 4 J. HIGH TECH. L. 1, 8 n.25 (2004) (quoting Ray August, *International Cyber-jurisdiction: A Comparative Analysis*, 39 AM. BUS. L.J. 531, 534 (2002)).

154. Traditionally, warfare has been contemplated as a conflict between two nations, and international relations theory has generally defined a state as a group of people with a territory, a language and a military. These traditional definitions strain in the context of attacks that happen partially through the Internet. See, e.g., Slantchev, *supra* note 147.

155. For a discussion of non-state actors and their impact on international crime, see, for example, Robert McLaughlin, *Improving Compliance: Making Non-State International Actors Responsible for Environmental Crimes*, 11 COLO. J. INT’L ENVTL. L. & POL’Y 377, 387 (2000) (“[R]ecognition of the role of non-state international actors in IEL has allowed some shift of focus toward identifying ‘the author of the damage,’ as opposed to recognizing only state responsibility for obligations.” (quoting Alexandre Kiss, *Present Limits to the Enforcement of State Responsibility for Environmental Damage*, in INTERNATIONAL RESPONSIBILITY FOR ENVIRONMENTAL HARM 3, 14 (Francesco Francioni & Tullio Scovazzi eds., 1991))); Kimberley N. Trapp, *The Use of Force Against Terrorists: A Reply to Christian J. Tams*, 20 EUR. J. INT’L L. 1049, 1050 (2009) (“By requiring that ‘armed attacks’ by non-state terrorist actors be attributable to the host state in whose territory defensive force is used, the violation of the host state’s territorial integrity is excused.”).

156. See Andy Greenberg, *Shopping for Zero-Days: A Price List For Hackers’ Secret Software Exploits*, FORBES (Mar 23, 2012, 9:43 AM), <https://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/#20cc4e7a2660>.

exploit can be leveraged by small numbers of people to remotely cause physical harms directly to civilians through vulnerabilities in those citizens' commercial products and infrastructure.¹⁵⁷ The recent shut-down of Ukrainian power grids through code attributed to (but disclaimed by) Russia demonstrates this dynamic.¹⁵⁸ This comparative ease of such an attack renders traditional deterrence analysis in either international relations¹⁵⁹ or criminal law¹⁶⁰ theory a poor fit for guiding information security.

A misguided focus on deterrence has also led some legal scholars to argue in broad strokes for speech-related restrictions, specifically suggesting restrictions on informational speech about security vulnerabilities but for a narrow set of conduct covered by a proposed statutory "safe harbor"¹⁶¹ and legal rules broadly prohibiting the sales of exploits.¹⁶² But such proposals are likely incompatible in substantial part with the broader protections of the First Amendment for informational speech,¹⁶³ the Copyright Office's more generous

157. See Condliffe, *supra* note 15; Pavel Polityuk, *Ukraine Investigates Suspected Cyber Attack On Kiev Power Grid*, REUTERS (Dec. 20, 2016, 8:57 AM), <http://www.reuters.com/article/us-ukraine-crisis-cyber-attacks-idUSKBN1491ZF>; Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED (Mar. 3, 2016, 7:00 AM), <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>; Kim Zetter, *The Ukrainian Power Grid Was Hacked Again*, MOTHERBOARD (Jan 10, 2017, 8:07 AM), https://motherboard.vice.com/en_us/article/ukrainian-power-station-hacking-december-2016-report.

158. Zetter, *The Ukrainian Power Grid Was Hacked Again*, *supra* note 157.

159. See *supra* text accompanying note 147.

160. See *supra* text accompanying notes 150–53.

161. Such proposals put the burden on the researcher to functionally obtain permission to speak and do not consider the nuances and practical difficulties experienced by security researchers attempting to disclose vulnerabilities. See Derek E. Bambauer & Oliver Day, *The Hacker's Aegis*, 60 EMORY L.J. 1051, 1089 (2011) ("The first conduct-based rule would require a researcher who discovers a security vulnerability to report it to the vendor of the affected software before publishing any information about the flaw.").

162. See *id.* at 1090 (proposing an affirmative defense where researchers must comport with a series of behavior rules, for example, "[t]he second behavior rule would ban sales of vulnerability data to third parties").

163. See Andrea M. Matwyshyn, *Hacking Speech: Informational Speech and the First Amendment*, 107 NW. U. L. REV. 795, 795 (2013) ("Using the case study of 'vulnerability speech'—speech that identifies a potentially critical flaw in a technological system but may indirectly facilitate criminality—this Article proposes a four-part 'repurposed speech scale' for crafting the outer boundaries of First Amendment protection for informational speech.").

interpretation of copyright law,¹⁶⁴ and the nuanced realities¹⁶⁵ of information security in practice.¹⁶⁶ Perhaps most importantly, such proposals fail to grapple with the problem of reciprocal security vulnerability in an adequately granular manner.¹⁶⁷ Vulnerability and exploit “purchasers” are not solely rogue non-state actors¹⁶⁸ and foreign governments seeking to attack U.S. systems.¹⁶⁹ They also include both public and private sector U.S. entities seeking to defend their systems¹⁷⁰ and improve the code in their products¹⁷¹—products

164. See Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 65944-01 (Oct. 28, 2015) (codified at 37 C.F.R. pt. 201) (“Based on this record, the Register recommended adopting an exemption to enable good-faith security research on computer programs within devices or machines primarily designed for use by individual consumers (including voting machines), motorized land vehicles, and implanted medical devices and their corresponding monitoring systems.”).

165. Sometimes vulnerabilities impact such a large number of vendors that notifying each impacted party is impracticable. See, e.g., U.S. COPYRIGHT OFFICE, SIXTH TRIENNIAL 1201 RULEMAKING HEARINGS 36 (2015), <https://www.copyright.gov/1201/2015/hearing-transcripts/1201-Rulemaking-Public-Roundtable-05-26-2015.pdf> (“Indeed, just last week, Professor Green, Professor Heninger . . . and a number of their colleagues released a report disclosing the logjam vulnerability in the core protocol we use to keep the Web secure.”).

166. For example, the finder of a security flaw may be an accidental finder or a curious teen, not a professional security researcher. See, e.g., Michael Mimoso, *Meet the 18-Year-Old Who Hacked the Pentagon*, THREATPOST (June 21, 2016, 3:15 PM), <https://threatpost.com/meet-the-18-year-old-who-hacked-the-pentagon/118802/>.

167. For example, one set of authors advocates restricting truthful speech about security vulnerabilities through a narrow safe harbor ostensibly because standardized vulnerability price lists have not emerged. See Bambauer & Day, *supra* note 161, at 1100 (“Even once a willing seller locates, and communicates with, a willing buyer, the parties will have difficulty coming to terms due to information asymmetry. There is no price list, or set of criteria, to determine what a bug is worth.”). However, as a practical matter of security, bug bounty programs and private sector intermediaries do offer precisely that kind of pricing guidance. See *generally* BUGCROWD, <https://bugcrowd.com/programs> (last visited Jan. 12, 2018); *Bug Bounty Programs*, HACKERONE, <https://hackerone.com/bug-bounty-programs> (last visited Jan. 12, 2018).

168. See Nicole Arce, *Hacking Team Warns Hacked Data and Codes Can Be Used By Cybercriminals and Terrorists*, TECH TIMES (July 10, 2015, 7:22 AM), <http://www.techtimes.com/articles/67377/20150710/hacking-team-warns-hacked-data-and-codes-can-be-used-by-cybercriminals-and-terrorists.htm>.

169. Sui-Lee Wee & Alexel Oreskovic, *Google Reveals Gmail Hacking, Says Likely from China*, REUTERS (June 1, 2011, 9:34 PM), <http://www.reuters.com/article/us-google-hacking-idUSTRE7506U320110602>.

170. In fact, an industry of bug purchasing intermediaries has arisen to assist companies in buying information about their vulnerabilities and running bug bounty programs. HACKERONE, <https://www.hackerone.com/> (last visited Jan. 12, 2018).

171. For example, Facebook has paid out over \$5 million in bug bounties to make its code more secure. Liam Tung, *Facebook’s Bug Bounty: Now it’s Paid Out \$5m for Security Flaws to 900 Hunters*, ZDNET (Oct. 13, 2016, 11:47 AM), <http://www.zdnet.com/article/facebooks-bug-bounty-now-its-paid-out-5m-for-security-flaws-to-900-hunters/>.

often deployed simultaneously in both the public and private sector.¹⁷² Particularly because vulnerability finders and exploit (re)sellers are often not U.S. citizens,¹⁷³ U.S. deterrence-driven prohibitions will neither reach them nor make prosecution more feasible.

But, one might ask, if information sharing and deterrence (using either definition¹⁷⁴) are not an optimal fit for a world defined by reciprocal security vulnerability, why have lawmakers and scholars¹⁷⁵ repeatedly embraced these two flawed paradigms for “cybersecurity”? The section that follows identifies a series of underlying theoretical errors and structural deficits that have led us to today’s “cyberized” legal paradigms.

B. CyberFacepalm:¹⁷⁶ The Three CyberFlaws

You keep using that word. I do not think that it means what you think it means.

—Inigo Montoya¹⁷⁷

Legal scholarship on topics related to information security has increased substantially in the last five years.¹⁷⁸ In addition to neglecting the problem of reciprocal security vulnerability, this newer scholarship usually refers to information security using the imprecise policy term “cybersecurity.” Three analytical flaws plague both this

172. Nuclear submarines, for example, can run on a variant of Windows. See Mizokami, *supra* note 86.

173. The first reported vulnerability in the Hack the Pentagon program was reported by a foreign national, for example. For comments of Lisa Wiswell, see *Bug Bounty*, YOUTUBE (Dec. 20, 2016) <https://www.youtube.com/watch?v=acWWT2R3LiI&index=15&list=PLtUuPz3a0Gz-PJOFb55O6jDZ68Ya9O9eS>.

174. See *supra* text accompanying notes 145–50.

175. Within the last five years, “cybersecurity” practice groups have sprung up seemingly ubiquitously in law firms. Orin Kerr, *What is ‘Cybersecurity Law’?*, WASH. POST (May 14, 2015), <http://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/05/14/what-is-cyber-security-law/>. But, as Professor Orin Kerr has again correctly pointed out, “[i]f you look closely, though, there isn’t much clarity about what ‘cybersecurity law’ actually means.” *Id.*

176. *Facepalm*, KNOW YOUR MEME, <http://knowyourmeme.com/memes/facepalm> (last visited Jan. 12, 2018).

177. THE PRINCESS BRIDE (Twentieth Century Fox Film Corporation 1987).

178. For example, a Westlaw query on “hackers” appearing at least twenty times in law review articles, yields approximately 150 results. Over half of these articles have been written in the last five years. The remaining half was written between 1986 and 2010.

“cybersecurity” legal scholarship and policy discourse—privacy conflation, incommensurability, and internet exceptionalism.

*1. Ermahgerd, cybers:*¹⁷⁹ *Privacy conflation*

Perhaps the most common error made by “cybersecurity” scholars and policymakers involves attempting to somehow cram security into the more familiar (and more subjective) legal box of privacy. This analytical error might be termed the mistake of *privacy conflation*. More colloquially, we might call this the “security-as-privacy-with-cybersprinkles” problem. Scholarship and policy suffering from the privacy conflation error mistakenly frame information security law as inextricably reliant upon and subservient to privacy law. Therefore, privacy conflated work argues, security must be subject to all of privacy law’s doctrinal, social, and normative messiness.¹⁸⁰ In other words, the mistake of privacy conflation is the erroneous belief held by many legal scholars and policymakers that information security is merely a subfield of, or contingent upon, privacy law and, consequently, that it is similarly socially-constructed.¹⁸¹

For example, one legal scholar has argued that security merely “implements privacy’s choices”¹⁸² and that the “futile obsession”¹⁸³ with preventing breaches¹⁸⁴ should be replaced with a focus on simply mitigating them post-occurrence.¹⁸⁵ But, this argument strains

179. *Ermahgerd*, KNOW YOUR MEME, <http://knowyourmeme.com/memes/ermahgerd> (last visited Jan. 12, 2018).

180. *See, e.g.*, Derek E. Bambauer, *Schrödinger’s Cybersecurity*, 48 U.C. DAVIS L. REV. 791, 791–92 (2015) (arguing that “cybersecurity” should be driven by “accuracy” and “accuracy is constructed through social processes, rather than emerging from information itself” or technical facts).

181. *See, e.g.*, Derek E. Bambauer, *Privacy Versus Security*, 103 J. CRIM. L. & CRIMINOLOGY 667, 676 (2013) (“Security implements privacy’s choices.”).

182. *Id.*

183. Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1012 (2014) (“Existing scholarship on cyberespionage and cyberwar is undermined by its futile obsession with preventing attacks.”).

184. This position has been subsequently adopted by at least one additional scholar. David Thaw, *Enlightened Regulatory Capture*, 89 WASH. L. REV. 329, 354 (2014) (“[P]rivacy is a normative exercise in making ‘decisions about competing claims to legitimate access to, use of, and alteration of information.’ Security . . . ‘implements those choices . . . mediat[ing] between information and [normative] privacy selections’ about the use of/access to that information.” (quoting Bambauer, *supra* note 181, at 667–68)).

185. *Id.* (“Cybersecurity must focus on mitigating breaches rather than preventing them.”).

credulity when security of critical infrastructure systems, weapons,¹⁸⁶ hospital equipment, medical devices,¹⁸⁷ or connected cars is at stake. A single¹⁸⁸ exploited code flaw can result in multiple deaths.¹⁸⁹ Mitigation post-breach is simply not enough, even in superficially low-stakes contexts.¹⁹⁰ Failing to prevent avoidable losses of human life due to errors in your company's products or services is not legally (or morally) acceptable: traditional legal principles dictate that an author or operator likely has an affirmative duty to prevent even a single security compromise when the means to prevent the harm are readily available and severe harm is foreseeable.¹⁹¹

Another scholar worries that data can be too secure and that security can inhibit “socially useful” data collection—a privacy concern that is irrelevant for security.¹⁹² Still other privacy-conflated legal

186. For example, the compromise of a nuclear power reactor, missile system, or nuclear submarine offer examples where the optimal level of compromise from the perspective of the compromised entity is clearly zero.

187. Also, if we are asking a patient wearing a pacemaker the optimal number of intrusions for a pacemaker, we can be confident the patient will state the optimal number of times that her pacemaker should be compromised by remote attackers is zero.

188. Economic-sounding “cybersecurity” arguments are a poor fit for the stakes and practical reality of information security law and policy unless we assume that a certain number of human lives are expendable. For example, another legal scholar argues that “[t]he optimal level of cyber-intrusions is not zero.” Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1511 (2013).

189. For a discussion of death due to code flaws in a hospital machine, see, for example, Leveson & Turner, *supra* note 108, at 18, 20.

190. Even flaws in pedestrian IoT devices can be harnessed into botnets directed at disrupting critical infrastructure and healthcare targets.

191. For a discussion of the duty to prevent avoidable harms see, for example, Stephen G. Gilles, *Causation and Responsibility After Coase, Calabresi and Coleman*, 16 QLR 255, 273–75 (1996) (“Today, the rejection of Good Samaritan liability is increasingly seen as an *exception* to ‘the general principle that a person is liable for injuries caused by his failure to exercise reasonable care in the circumstances’ A person whose activities involve the creation of risk (to self or others) is ordinarily by that very fact in a position to reduce or avoid those risks, either by taking additional care or by refraining from engaging in the activity. Risk-creators . . . are thus *prima facie* good risk-avoiders. That may be why we normally assume that our causal judgments can appropriately be translated into judgments about responsibility” (alteration in original) (quoting *Rowland v. Christian*, 443 P.2d 561, 564 (Cal. 1968))). See also Andrea M. Matwyshyn, *Hidden Engines of Destruction: The Reasonable Expectation of Code Safety and the Duty to Warn in Digital Products*, 62 FLA. L. REV. 109, 110 (2010) (“Even if we assume arguendo that a harmed consumer will have difficulty quantifying actual damages, an independent duty to warn on the part of the digital product creator or operator may still exist.”).

192. See, e.g., 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, 264 (2007) (“A database operator’s uncertainty about the contours of due care may prompt it to take too much

scholarship views security as simply the debate over appropriate notice and remedy after the “privacy failure” of a data breach¹⁹³ or a failure in compliance.¹⁹⁴ In other words, this scholarship focuses on a data breach as functionally the cause of security “harm,”¹⁹⁵ rather than merely a visible symptom of a deeper problem. In reality, a breach is merely one of many possible consequences of the real problem—the underlying security inadequacy in technical and corporate governance processes.¹⁹⁶ Each of these framings falls prey to the privacy conflation error¹⁹⁷ and misses the bigger picture, both in terms of computer science and law.

a. Security!=¹⁹⁸ privacy as a technical matter of computer science. Defining information security law solely in relation to privacy law yields incorrect analysis, both as a technical computer-science matter and as a normative policy matter. As a technical matter, privacy-conflated analysis contradicts basics of the science of computer

[security] precaution. Such overcompliance with the law risks inhibiting socially useful data collection.”).

193. See, e.g., Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CAL. L. REV. 877, 889 (2014) (“The third approach of U.S. privacy law is to list specific types of data that constitute personal information . . . State data breach notification laws take this approach.”).

194. See *infra* notes 496–97 and accompanying text.

195. See Daniel Solove, *Privacy and Data Security Harms*, CONCURRING OPINIONS (Aug. 4, 2014), <http://www.concurringopinions.com/archives/2014/08/privacy-and-data-security-harms.html>.

196. For a discussion of possible consequences of security failures, see *infra* text accompanying notes 464–80.

197. One scholar has correctly argued that security is not the “handmaiden” of privacy. See Lauren Henry, *Information Privacy and Data Security*, 2015 CARDOZO L. REV. DE NOVO 107, 107 (2015) (“Legal academic and policy discourse generally presumes that information privacy and data security are interchangeable goals. The conventional wisdom is that data security is a handmaiden of information privacy . . .”).

198. != is commonly used in programming languages to express the idea “does not equal.” *Equality Operators: == and !=*, MICROSOFT, <https://msdn.microsoft.com/en-us/library/c35t2ffz.aspx> (last visited Jan. 12, 2018).

security. Computer scientists draw a technical distinction between the study of “security”¹⁹⁹ and the study of “privacy.”²⁰⁰

Security, in the technical community, historically refers to questions of data confidentiality,²⁰¹ integrity,²⁰² and availability²⁰³ as engineering properties of a system²⁰⁴—questions likely to be disconnected from the identity of any individual human person.²⁰⁵

199. For example, a computer security curriculum in a computer science department might include courses such as Security Management: Systems Administration, Database Security, Computer Security Operating Systems, Systems Administration, Network Security Computer Networks, Formal Methods for Security Software Engineering, and Cryptography. *See, e.g.*, Alec Yasinsac, Information Security Curricula in Computer Science Departments: Theory and Practice 6 (Nov. 2, 2002) (unpublished paper), <http://www.cs.fsu.edu/~yasinsac/Papers/Yas01b.pdf>.

200. Privacy curriculum in computer science might include courses focused on assisting students in obtaining skills such as designing products and services that leverage big data while preserving privacy, proposing and evaluating solutions regarding privacy risks, understanding how privacy-enhancing technologies can be used to reduce privacy risks, using techniques to aggregate and de-identify data, understanding the limits of de-identification, understanding current privacy regulatory and self-regulatory frameworks, conducting privacy-related risk assessments and compliance reviews, responding to incidents, integrating privacy into the software engineering lifecycle phases, and conducting basic usability evaluations of privacy-related features and processes. *See Privacy Engineering*, CARNEGIE MELLON U., <http://privacy.cs.cmu.edu/> (last visited Jan. 12, 2018).

201. Confidentiality has classically been defined as the maintenance of technical properties set a priori regarding a system’s limitations of data access. *See Confidentiality [of data]*, in *Glossary of Computer Security Acronyms*, NIST.GOV, <http://csrc.nist.gov/publications/secpubs/rainbow/tg004.txt> (“The concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations.”) (last visited Jan. 12, 2018).

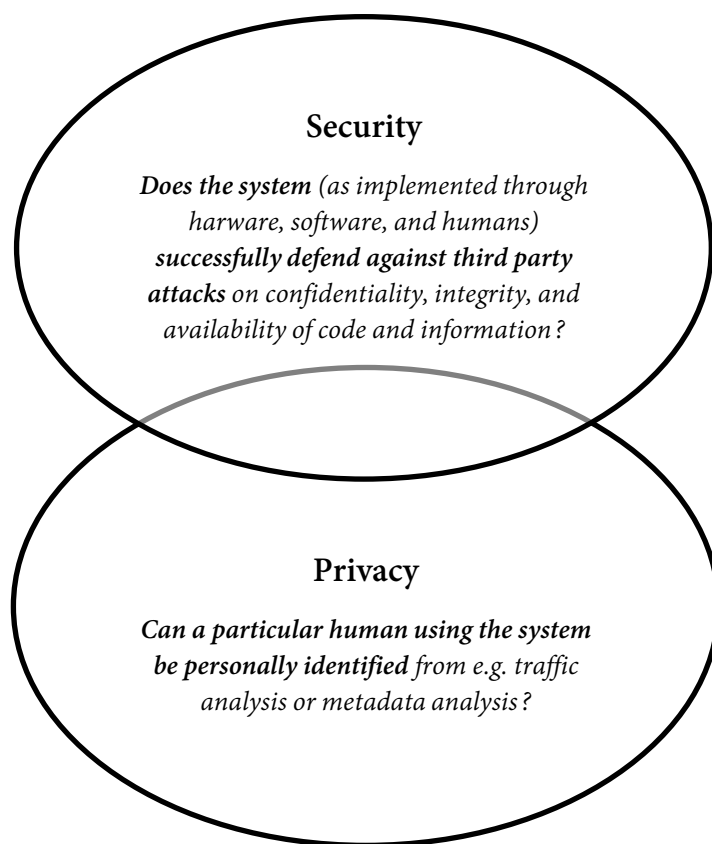
202. Integrity has classically been defined as the preservation of data or a system properties set a priori, free from manipulation or impairment. *See id.* at *system integrity*, (“The quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.”); *id.* at *data integrity*, (“The property that data meet a priori expectation of quality.”); *id.* at *integrity* (“Sound, unimpaired or perfect condition.”).

203. Availability has classically referred to preservation of the technical property set a priori regarding the ability of a user to access data in the system. *See id.* at *availability of data*, (“The state when data are in the place needed by the user, at the time the user needs them, and in the form needed by the user.”).

204. Part of the privacy conflation error may arise because scholars and policymakers hear security discussions of “confidentiality” and erroneously believe them to somehow map to the privacy law concept of “confidentiality” as it appears in tort law among human litigants. It does not. For a discussion of the privacy tort concept of confidentiality, see, for example, Woodrow Hartzog, *Reviving Implied Confidentiality*, 89 IND. L.J. 763, 763 (2014) (“This Article urges a revival of implied confidentiality by identifying from the relevant case law a set of implied confidentiality norms based upon party perception and inequality that courts should be, but are not, considering in online disputes.”).

205. *See infra* text accompanying notes 209–10.

Privacy, on the other hand, encompasses questions of anonymity, metadata, and traffic analysis²⁰⁶—questions that relate to identities of particular humans and their outputs.²⁰⁷ In other words, the unit of analysis can materially differ for questions of security and questions of privacy; they are orthogonal computer science fields that merely conceptually overlap in part. Imagine a Venn diagram with two circles—one security, one privacy—that overlap slightly in the middle.



206. See, e.g., Jelle van den Hooff, et al., Vuvuzela: Scalable Private Messaging Resistant to Traffic Analysis 137 (Oct. 4, 2015) (unpublished paper), <https://pdos.csail.mit.edu/papers/vuvuzela:sosp15.pdf> (“Private messaging over the Internet has proven challenging to implement, because even if message data is encrypted, it is difficult to hide metadata about *who* is communicating in the face of traffic analysis.”).

207. See *infra* text accompanying notes 210–13.

In summary, some technical conceptual overlap can be argued to exist in the broadest of terms between security questions and privacy questions because both implicate raw underlying data. However, *the field of security is not defined in relation to privacy as a technical matter of computer science*. Privacy-conflated “cyberized” legal scholarship is, therefore, definitionally at loggerheads with computer science.

b. The legal and policy difference between security and privacy. As a legal and policy matter, it is both logical and useful to map policy and legal distinctions of security and privacy onto the existing computer science distinctions to the greatest extent possible.²⁰⁸ Indeed, as described in Part II, doing otherwise has previously resulted in decades of avoidable legal morass.²⁰⁹ Thus, rather than a privacy-conflated view, this Article, instead, advocates a more rigorous definition for security. It advocates drawing as crisp a line between security and privacy as possible and mirroring the distinctions of computer science as closely as feasible.

Let us start with a definition for security:

Security refers to the hybrid scientific and legal inquiry into (1) whether particular implemented systems, products, and processes can successfully defend against all possible third-party attackers in both physical and digital space, and (2) what legal consequences arise when they cannot.

As explained above, the technical field of information security investigates whether a system as implemented in hardware, software, and (by and in) humans can withstand a third-party attack and maintain the core properties of data confidentiality, integrity, and availability. Security inadequacies are, therefore, objectively-testable, replicable failures of technological and human measures to maintain the system’s confidentiality, integrity, and availability. The legal and policy analysis of security consequently asks whether the failure was foreseeable in light of the state of the art of scientific knowledge and standards of security care deemed necessary by the community of technical security experts. Information security law, in other words, creates legal duties and recourse for violations of objectively-testable

208. A scientifically-consonant legal and policy definition of security allows more effective and efficient interdisciplinary policy conversations with computer security experts— a desirable result. *See* discussion of epistemological humility *infra* Section III.C.

209. *See supra* Section II.B.

minimum standards of care in the creation, deployment, and operation of a system, as such standards are determined by the scientific community of computer security technical experts *a priori*.

Now let us turn to privacy:

Privacy refers to the legal and policy inquiry regarding conflicts between (1) what information a person reasonably expects²¹⁰ will be or can be collected and used²¹¹ about her (based in part on the legally-binding promises made to her, whose enforceability arises from dictates of either criminal or civil law²¹²), on the one hand, and (2) the technical and business reality of possible or actual collection and repurposing by the collector, on the other.

Unlike security, which focuses on properties of systems, privacy analysis uses a particular person—not a technical system—as the focal point of analysis. Privacy relates to the negotiated rights and privileges of a (usually) human person in her own information and her choice to engage in its selective transmission under certain terms. Privacy law, therefore, creates legal recourse for violations of a person’s ability to *prevent the collection or repurposed use of data by a particular collector* in specific ways. In other words, privacy rights reflect a partially normative inquiry that is relationship-specific: they turn on subjective and objective social expectations of a particular person in a particular context—what the criminal law has called a “reasonable expectation” and what Professor Helen Nissenbaum has called “contextual.”²¹³

Consequently, the presence of a privacy violation is not objectively testable without knowing the terms of a consensual idiosyncratic agreement between parties, the nature of the information, and the

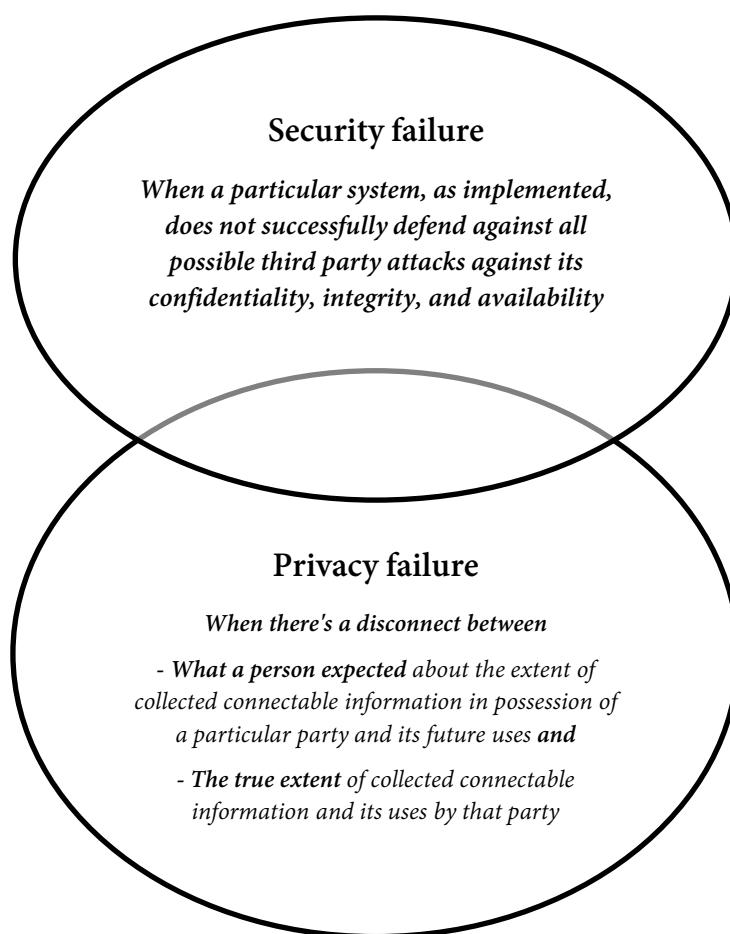
210. This expectation is constructed either subjectively or objectively depending on context and legal constraints in contract and other law. For a discussion of reasonable expectations in contract, see, for example, Matwyshyn, *supra* note 49, at 532 (proposing to ease doctrinal noise in consent through creating an objective “reasonable digital consumer” standard based on empirical testing of real consumers).

211. This use encompasses any additional information that can be derived from that information, either directly or through aggregation with information from other sources.

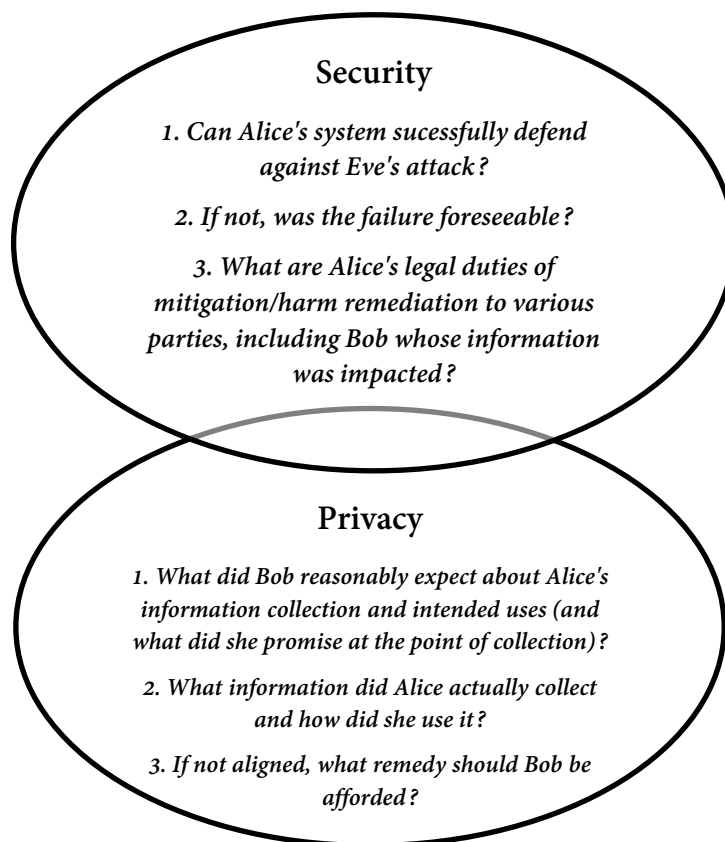
212. For a discussion of criminal and tort privacy, see, for example, Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis’s Privacy Tort*, 68 CORNELL L. REV. 291, 294 (1983) (encouraging a re-evaluation of the prevailing privacy doctrine).

213. See Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 119 (2004) (“Contextual integrity ties adequate protection for privacy to norms of specific contexts, demanding that information gathering and dissemination be appropriate to that context and obey the governing norms of distribution within it.”).

social context within which these promises exist. In this way, privacy contrasts sharply with security; security of a system is always objectively testable by third-parties on the four corners of the system, process, or product with no additional information. Regardless of what interpersonal or legal obligations may or may not exist, whether a system maintains confidentiality, integrity, and availability is a statement reflecting the state of the art of technical knowledge and the functioning of a particular system, as this system was built *a priori* and as it is operated and maintained. It is not a contextual analysis after the fact (like privacy).



In other words, information security policy and law relate to Alice's legal duties arising from the (objectively testable) success or failure of her system in defending the confidentiality, availability, and integrity of its code and information against Eve, an attacker, who wants to read, manipulate, or steal the data. Privacy policy and law, meanwhile, relate to the idiosyncratic terms of the agreement²¹⁴ where Bob allows Alice to collect and use certain information about him that he selectively discloses to her on certain terms.



214. For a discussion of privacy policies see, for example, Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1856 (2011) (“[S]tudies have shown that few consumers read privacy policies, and that those who do frequently fail to understand them.”).

Let us briefly further elaborate on the separateness of security from privacy with an example. Recently, a security researcher stumbled across the control systems of multiple hydroelectric plants in France²¹⁵ and a steel mill²¹⁶ that had been (dangerously) connected to the internet. Because of public accessibility, these connections potentially allowed for remote manipulation and disruption of operations.²¹⁷ If a hydroelectric plant or a steel mill control system is accessible through the internet, its operators have made a grievous security error with respect to availability. If the control system code can also be manipulated or altered to modify its operation, its security also reflects an inadequacy with respect to integrity. If information about the control system structure and other sensitive content is disclosed to attackers as well, the security error also impacts confidentiality.²¹⁸ As an information security policy matter, there is no logical argument in favor of implementing the code of hydroelectric plant or steel mill control systems in a vulnerable manner that may put human lives at risk.²¹⁹ In this example, no privacy concerns exist and no human's subjective privacy choices are implicated or implemented; leaving the control system of a hydroelectric plant vulnerable and connected to the internet is simply a dangerously irresponsible security blunder with national security implications.

Thus, the privacy conflation error highlights an undesirable muddling of technical reality. It also means that lawmakers, technologists, companies, and consumers are likely to end up talking

215. Dartmouth, *"It's Fine," They Said. "Just Ship It," They Said.*, at 46:00, YOUTUBE (June 9, 2016), <https://www.youtube.com/watch?v=yBA6u5IsXycat> (last visited Jan. 12, 2018).

216. *See id.* at 9:05 ("Who thought this was a good idea?").

217. A power plant in Italy was also recently available on Shodan, apparently suffering from a security vulnerability and granting access to remote attackers to an on/off switch. Dan Tentler (@Viss), TWITTER (Apr. 11, 2016, 8:57 AM), <https://twitter.com/Viss/status/719554936208363520>.

218. A vulnerable system may suffer from inadequacies of security with respect to any or all of confidentiality, integrity, and availability. For a discussion of the distinction among these three properties, see *supra* notes 201–03.

219. A similar argument might be made in connection with the vulnerability where four lines of code enabled the remote compromise of a Jeep in 2015, resulting in a journalist being driven into a ditch. *See supra* note 10; David Schneider, *Jeep Hacking 101*, IEEE SPECTRUM (Aug. 6, 2015, 5:44 PM), <https://spectrum.ieee.org/cars-that-think/transportation/systems/jeep-hacking-101> (discussing that there was no implementation "choice" to write vulnerable code, but that it was an uncaught error that may have resulted in thousands of deaths in the hands of attackers unless patched).

past each other. In this way, the privacy conflation error introduces us to our second flaw, the flaw of incommensurability.

2. *Seems cyberlegit*.²²⁰ *Incommensurability*

*Cyber pathogens*²²¹ are so unspeakably dangerous that the open research community has wisely never published a single paper about them.

—Professor Matt Blaze²²²

Mastering security requires years of rigorous study. Consequently, lawyers have sometimes developed the coping strategy of simply making up vaguely technical-sounding “computer-y” terms²²³ or making flawed (quasi)technical assumptions²²⁴ or assertions,²²⁵ often

220. *Seems Legit / Sounds Legit*, KNOW YOUR MEME, <http://knowyourmeme.com/memes/seems-legit-sounds-legit> (last visited Jan. 10, 2018).

221. Jonathan Zdziarski, *On Dormant Cyber Pathogens and Unicorns*, ZDZIARSKI’S BLOG THINGS (Mar. 3, 2016), <https://www.zdziarski.com/blog/?p=5849>.

222. Matt Blaze (@mattblaze), TWITTER, (Mar. 3, 2016, 10:24 PM), https://twitter.com/mattblaze/status/705640145056190464?ref_src=twsrc%5Etfw.

223. HAL 90210, *What’s a ‘Cyber Pathogen’? San Bernardino DA Baffles Security Community*, GUARDIAN (Mar. 4, 2016, 5:52 AM), <http://www.theguardian.com/technology/2016/mar/04/san-bernardino-da-baffles-security-community-lying-dormant-cyber-pathogen-iphone>.

224. For example, one scholar asserts (without citation) that “inefficiency creates resiliency.” Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584, 638 (2011). He argues that “a key goal for cybersecurity is increasing the inefficiency with which information is stored.” *Id.* at 640. Yet, computer scientists who study security will tell you that technology complexity/inefficiency is actually the enemy of security—it is how mistakes happen. *See Deciphering the Debate over Encryption: Hearing Before Subcomm. on Oversight and Investigations of the H. Comm. on Energy & Commerce*, 114th Cong. (Apr. 19, 2016) (statement of Matt Blaze, Professor, University of Pennsylvania), <http://docs.house.gov/meetings/IF/IF02/20160419/104812/HHRG-114-IF02-Wstate-BlazeM-20160419-U3.pdf> (“Adding key escrow renders even the specification of the protocol itself far more complex, making it virtually impossible to assure that any systems using it will actually have the security properties that these systems are intended to have.”). Instead, what this author perhaps meant to argue was that data storage redundancy has benefits for recovery in case of system failures. But, that is a prudent act of efficient risk management, not an “inefficiency.”

225. For example, one scholar recently provided an inaccurate understanding of the definition of “integrity” per computer science. *See* Bambauer, *supra* note 180, 798–99 (“Most broadly, [integrity] signals that the authorized user entered valid and reliable data.”). In computer science, integrity refers to the state where information and a system have been unaltered. It does not, however, generally concern the validity or reliability of the data as an independent construct before it entered the system. *See supra* note 202. Indeed, a computer science aphorism warns of this technical reality—“Garbage in, garbage out.” *See Garbage in,*

predicated on questionable physical space analogies.²²⁶ Although these coping strategies may seem harmless or desirable to the lawyers, legal academics, and policymakers using them, they are often problematically counterproductive for purposes of crafting optimal security policy. These “computer-y” legal terms often create avoidable conflicts with rigorously-defined terms from computer science. Indeed, this phenomenon generally leads to an incommensurability problem: a situation in which divergent baselines of understanding create a counterproductive language barrier to meaningful communication.²²⁷

a. Security lessons from section 1201 of the DMCA. Incommensurability challenges for security and law are not new. The case study of the history of section 1201 of the Digital Millennium Copyright Act²²⁸ (DMCA) offers a cautionary tale of how lawyers’ faux-technical words end badly for security. The DMCA, a copyright statute with both criminal and civil penalties,²²⁹ was passed in 1998,²³⁰ ostensibly as part of the U.S. embodiment of World Intellectual Property Organization (WIPO) obligations²³¹ that intended to strengthen digital copyright against acts of circumvention.²³² Under

Garbage out (GIGO), TECHTARGET, <http://searchsoftwarequality.techtarget.com/definition/garbage-in-garbage-out> (last updated Mar. 2008).

226. See, e.g., Timothy A. Wiseman, *Encryption, Forced Decryption, and the Constitution*, 11 I/S: J.L. & POL’Y FOR INFO. SOC’Y 525, 552 (2015) (“One frequently used analogy is to say that encryption is like a safe, the data is like its contents, and the password is like the combination. This analogy, like all analogies, is not perfectly accurate.”).

227. As used here, the term incommensurability adopts the primitive dictionary definition—“lacking a basis of comparison in respect to a quality normally subject to comparison.” *Incommensurable*, MERRIAM-WEBSTER, <https://www.merriam-webster.com/dictionary/incommensurable> (last visited Jan. 12, 2018). The term “incommensurability” has also been used by several philosophers of science such as Thomas Kuhn, who argued that conceptual incommensurability is manifest in different structures and methodologies used in laws and theories, leading to upheaval of paradigms. See THOMAS S. KUHN, *THE STRUCTURE OF SCIENTIFIC REVOLUTIONS* (1962). However, Kuhn’s analysis and definitions of “incommensurability” questions are contested in the philosophy of science, and this article does not wade into this philosophical conflict.

228. See Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, 112 Stat. 2860 (codified as amended in scattered sections of 17 U.S.C.); 17 U.S.C. § 1201 (2012).

229. See, e.g., Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519, 545–46 (1999) (“[T]here are serious criminal penalties for willfully violating section 1201.”).

230. 17 U.S.C. § 1201.

231. See Samuelson, *supra* note 229, at 521.

232. *Id.*

the DMCA, the act of circumvention of a “technological measure” itself became a violation of copyright law, even without any further copying.²³³ Congress built in a few statutory exceptions by design, including an exception for “encryption research.” But Congress also presciently anticipated that digital copyright circumstances might change across time, and it wisely built in a feedback loop—a process for new exemptions to section 1201’s anti-circumvention provisions that would be granted by the Librarian of Congress²³⁴ in consultation with the Register of Copyrights.²³⁵ Despite incorporating this feedback loop, however, Congress failed to anticipate a serious incommensurability problem in one of the DMCA’s key legal terms: “technological measure.”²³⁶

While the term “technological measure” may sound self-evident to a legal ear, the term is neither self-evident²³⁷ nor technical to the ears of computer scientists.²³⁸ Because of Congress’s use of this pseudo-technical legal term in the DMCA,²³⁹ computer security

233. For a discussion of the impact of the DMCA, see, for example, Stefan Bechtold, *Digital Rights Management in the United States and Europe*, 52 AM. J. COMP. L. 323 (2004); Urs Gasser, *Legal Frameworks and Technological Protection of Digital Content: Moving Forward Towards a Best Practice Model*, 17 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 39 (2006); Gwen Hinze, *Brave New World, Ten Years Later: Reviewing the Impact of Policy Choices in the Implementation of the WIPO Internet Treaties’ Technological Protection Measure Provisions*, 57 CASE W. RES. L. REV. 779 (2007); Jacqueline Lipton, *A Framework for Information Law and Policy*, 82 OR. L. REV. 695 (2003); Peter S. Menell, *Envisioning Copyright Law’s Digital Future*, 46 N.Y.L. SCH. L. REV. 63 (2002–2003); David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673 (2000); David Nimmer, *Appreciating Legislative History: The Sweet and Sour Spots of the DMCA’s Commentary*, 23 CARDOZO L. REV. 909 (2002); Jerome H. Reichman, Graeme B. Dinwoodie & Pamela Samuelson, *A Reverse Notice and Takedown Regime to Enable Public Interest Uses of Technically Protected Copyrighted Works*, 22 BERKELEY TECH. L.J. 981 (2007).

234. See Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, 112 Stat. 2860 (codified as amended in scattered sections of 17 U.S.C.); 17 U.S.C. § 1201.

235. *Id.*

236. *Id.*

237. For example, noted computer scientists have pointed to cases of the absence of an extraction interface as one type of technology circumstance that creates ambiguity regarding whether a technological protection measure exists. See STEVEN M. BELLOVIN ET AL., LONG COMMENT REGARDING A PROPOSED EXEMPTION UNDER 17 U.S.C. 1201, http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_SecurityResearchers_Class25.pdf (last visited Jan. 12, 2018).

238. *Id.* (filing by proponents of the (granted) security research exemption to section 1201 of the DMCA explaining why the pre-exemption DMCA framework chilled security research and enabled frivolous litigation).

239. *Id.*

researchers (and their counsel) struggled for the next fifteen years to interpret the DMCA anti-circumvention provisions.²⁴⁰ Additionally, just as Professor Jacqui Lipton has warned of the potential for the DMCA to be used to quash competition,²⁴¹ the DMCA's ambiguities were sometimes used by civil litigants to quash unflattering security research.²⁴² Wielding section 1201's faux-technical language as a sword, litigious companies began to threaten security researchers in an attempt to avoid discourse about security and particular products' security failures.²⁴³ In this way, critical security research was materially chilled²⁴⁴ because of the fear of accidentally running afoul of the DMCA.²⁴⁵ Finally, in 2015, the Copyright Office and Librarian of Congress acknowledged and partially corrected this problematic state of affairs by granting²⁴⁶ the exemption²⁴⁷ request²⁴⁸ of a group of computer security academics²⁴⁹ represented by this author,²⁵⁰ determining that a circumvention of any technological protection measures in the course of most²⁵¹ security research falls outside the conduct deemed verboten by the DMCA.²⁵²

240. *Id.*

241. Jacqueline Lipton, *The Law of Unintended Consequences: The Digital Millennium Copyright Act and Interoperability*, 62 WASH. & LEE L. REV. 487 (2005) (citing the DMCA's potential "to be used to quash commercial competition . . . where a copyright work . . . is a purely incidental facet of [a] product").

242. *See* BELLOVIN, *supra* note 237.

243. *Id.*

244. According to leading computer security academics, because of this DMCA incommensurability problem and the looming threat of possible legal sanction, computer security researchers were often able to analyze less than forty percent of the code they had hoped to research in particular projects. *See id.*

245. *Id.*

246. *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 65944, 65955–56 (2015) (codified 37 CFR pt. 201).

247. *Id.* at 65950–51.

248. Our original requested exemption covered a broader swath of research activity, But, the grant reflected a substantial piece of our original request, focusing on consumer-purchased goods. *Id.*

249. *See* BELLOVIN, *supra* note 237.

250. *Id.*

251. *See* Press Release, Fed. Trade Comm'n, FTC Kicks Off "Start with Security" Business Education Initiative (June 30, 2015), <https://www.ftc.gov/news-events/press-releases/2015/06/ftc-kicks-start-security-business-education-initiative>.

252. *Id.*

Two key lessons are visible in this case study of the DMCA's incommensurability problem. The first is the danger of analyzing security questions in legal silos. While trying to protect the security of a particular part of our system—copyrighted digital works—the DMCA's faux-technical language inadvertently harmed the security of our system as a whole.²⁵³ It chilled academic and private sector research because of its incommensurate terminology.²⁵⁴ The second lesson relates to the importance of legal feedback loops to enable correction of legal errors. Although the DMCA's exemption process is far from ideal,²⁵⁵ the DMCA incommensurability problem was partially remedied solely because of the existence of a feedback loop²⁵⁶ open to the private sector and built in by statutory design.²⁵⁷

b. The current state of “cyberized” incommensurability. Much like the struggles of interpreting the meaning of “technological measures” under the DMCA, “cybersecurity” is a term that means different things to different people.²⁵⁸ Indeed, “cyberized” information security legal discourse makes the incommensurability problems of security worse. It exacerbates communication difficulty and social distance²⁵⁹

253. See BELLOVIN *supra* note 237, at 4.

254. See *supra* note 227. For a legal discussion of incommensurability, see, for example, Brian Leiter, *Incommensurability: Truth or Consequences?*, 146 U. PA. L. REV. 1723, 1727 (1998) (“[T]he thesis that values are incommensurable appeals to our ordinary ways of thinking and talking about values, but not necessarily to our actual behavior.”). *But see* Frederick Schauer, *Instrumental Commensurability*, 146 U. PA. L. REV. 1215, 1216 (1998) (“[T]hose who argue for incommensurability or incomparability deny the phenomenon of commensurability or comparability, and thus maintain that the members of some pairs or sets of reasons, values, options, or norms are irreducibly different.”).

255. For a critique of the DMCA, see Steve P. Calandrillo & Ewa M. Davison, *The Dangers of the Digital Millennium Copyright Act: Much Ado About Nothing?*, 50 WM. & MARY L. REV. 349, 350 (2008).

256. For a discussion of the value of feedback loops in design, see generally NORBERT WIENER, *CYBERNETICS: OR CONTROL AND COMMUNICATION IN THE ANIMAL AND THE MACHINE* (2d ed. 1965) (arguing that feedback loops play an essential role in systems functioning properly).

257. See, e.g., Menell, *supra* note 233, at 155.

258. See Orin Kerr, *What is ‘Cybersecurity Law’?*, WASH. POST (May 14, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/05/14/what-is-cybersecurity-law/?utm_term=.a5628328338f.

259. For a discussion of social distance, see Jacqueline B. Helfgott & Elaine Gunnison, *The Influence of Social Distance on Community Corrections Officer Perceptions of Offender Reentry Needs*, 72 FED. PROBATION 2, 3–4 (2008) (“‘Social distance’ has been defined in the research literature as the level of trust one group has for another . . . and the degree of perceived similarity of beliefs between a perceiver and target.”).

between the language of technical information security experts on the one hand, and legislators, policymakers and legal practitioners on the other. Professor Orin Kerr has correctly observed that “cybersecurity” even means different things to different lawyers in various law firms.²⁶⁰ But, perhaps surprisingly, the term “cybersecurity” also exacerbates incommensurability problems across government policymakers and various federal agencies. The term “cybersecurity” and even the concept of “good” security currently mean different things to different *governmental* organizations. As Professor Julie Cohen has argued, scholars have also often preferred to debate particular security measures “rather than to delve too deeply into the ways in which public discourse invests that term with particular, contingent meanings.”²⁶¹

To wit, due to this incommensurability problem, federal agencies tasked with enforcing some aspect of information security are beginning to function at cross-purposes with each other, despite ostensibly sharing a goal of improving security. In interpreting their mission in light of security, they diverge in the paradigms they apply to the problem. For example, perhaps the most starkly perceived difference in posture currently exists between the two agencies that are perhaps most active in security enforcement, the Federal Trade Commission (FTC) and the Department of Justice (DOJ).²⁶²

In furtherance of its dual mission to encourage fair competition and enhance consumer protection,²⁶³ the FTC has adopted a socially-

260. Kerr offers a four-part division of what he states is being called a new field of “cybersecurity” law. According to Professor Kerr, this emerging field spans (1) the law governing steps that potential or actual victims of Internet intrusions can take in response to potential or actual intrusions; (2) the law governing liability for computer intrusions, both for the perpetrator and the victim; (3) the regulatory law of computer security; and (4) special issues raised by government network offense and defense. *See* Kerr, *supra* note 175.

261. COHEN, *supra* note 130, at 185.

262. ELEC. FRONTIER FOUND., THE COMPUTER FRAUD AND ABUSE ACT HAMPERS SECURITY RESEARCH, <https://www EFF.ORG/document/cfaa-and-security-researchers> (last visited Jan. 12, 2018); Jerry Markon, *Computer Hacker Andrew Auernheimer’s Conviction is Overturned by Appeals Court*, WASH. POST (Apr. 11, 2014), http://www.washingtonpost.com/politics/computer-hacker-andrew-auernheimers-conviction-is-overturned-by-appeal-s-court/2014/04/11/0744a3bc-c1bc-11e3-b195-dd0c1174052c_story.html. *But see* Aaron Boyd, *More from Black Hat: DOJ Official Draws Line Between Cyber Crime, Legitimate Research*, FED. TIMES (Aug. 5, 2015), <https://www.federaltimes.com/2015/08/05/more-from-black-hat-doj-official-draws-line-between-cyber-crime-legitimate-research/>.

263. *About the FTC*, FED. TRADE COMM’N, <https://www.ftc.gov/about-ftc> (last visited Jan. 12, 2018).

porous,²⁶⁴ holistic²⁶⁵ stance on what it calls “data security”²⁶⁶—not “cybersecurity.” The FTC both proactively issues security guidance²⁶⁷ and engages in enforcement activity.²⁶⁸ Perhaps most importantly, the FTC has embraced the importance of feedback loops and formally sought out technical expertise in security from the private sector in order to inform its work. These proactive steps have included the creation of a Chief Technologist²⁶⁹ and a Senior Policy Advisor/Scholar in Residence program,²⁷⁰ organizing²⁷¹ and participating in technical information security conferences,²⁷² community outreach events,²⁷³ and security contests under the America Competes Act in collaboration with the private sector security research community.²⁷⁴ In lieu of adopting an information sharing or deterrence-focused paradigm,²⁷⁵ the FTC instead has advocated an

264. The FTC maintains feedback loops with the private sector in multiple ways, including through an outside chief technologist and academic in-residence program. *See, e.g.*, Press Release, Fed. Trade Comm’n, FTC Names Latanya Sweeney as Chief Technologist; Andrea Matwyshyn as Policy Advisor (Nov. 18, 2013), <https://www.ftc.gov/news-events/press-releases/2013/11/ftc-names-latanya-sweeney-chief-technologist-andrea-matwyshyn>.

265. The FTC considers the totality of reasonable security measures—both online and offline—in its analysis. FED. TRADE COMM’N, START WITH SECURITY (2015), <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

266. *Id.*

267. The FTC advocates for organizations to “Start with Security” in the name of consumer protection and protection of their own intangible assets. *Id.*

268. The FTC has completed over 50 enforcement actions to date. *See* FED. TRADE COMM’N, 2014 PRIVACY AND DATA SECURITY UPDATE (2015), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf.

269. *See, e.g.*, *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM’N (Mar. 20, 2015), <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions>.

270. *See, e.g.*, FED. TRADE COMM’N, *supra* note 268.

271. *See PrivacyCon: Call for Presentations*, FED. TRADE COMM’N, <https://www.ftc.gov/privacycon-call-for-presentations> (last visited Jan. 12, 2018).

272. *See DEF CON 23 Speakers*, DEF CON, <https://www.defcon.org/html/defcon-23/dc-23-speakers.html#McSweeney> (last visited Jan. 12, 2018) (McSweeney speaking at Def Con 23).

273. *See, e.g.*, Press Release, *supra* note 251.

274. Press Release, Fed. Trade Comm’n, FTC Announces Internet of Things Challenge to Combat Security Vulnerabilities in Home Devices (Jan. 4, 2017), <https://www.ftc.gov/news-events/press-releases/2017/01/ftc-announces-internet-things-challenge-combat-security>.

275. *See* Terrell McSweeney, *Security is a Must for the Internet of Things*, RECODE (Jan. 27, 2015, 6:26 AM), <http://www.recode.net/2015/1/27/11558088/security-is-a-must-for-the-internet-of-things>.

approach focused on security by design.²⁷⁶ In particular, FTC Commissioners have also advocated the use of encryption by companies and consumers as a successful tool to protect themselves against identity theft, trade secret theft, and other data harms.²⁷⁷ In short, it can be said that the FTC has adopted a decentralized approach to its security mission akin to what I have elsewhere called a “security through process” model²⁷⁸ with multiple private sector feedback loops.

In contrast to the FTC and in line with its different overall mission, DOJ has adopted a more cloistered, reactive approach that reflects a primary focus on deterrence of attackers as a focal point of its approach to “cybersecurity.” DOJ engaged in over 200 prosecutions of criminal computer intrusion offenses in 2016,²⁷⁹ supported proposals to eliminate all misdemeanor offenses for computer intrusion, and advocated increased sentences.²⁸⁰ DOJ does not currently appear to have an extensive set of formal feedback loops²⁸¹ with the private sector to update attorneys’ knowledge of security.²⁸² Meanwhile, because DOJ enforces, among other

276. The FTC has encouraged all businesses to “Start with Security” in their internal and external operations, and the FTC’s guidance nudges organizations to build reasonable security into their products and services by design. FED. TRADE COMM’N, *supra* note 265.

277. Terrell McSweeney (@TMcSweeneyFTC), TWITTER (Jan. 5, 2016, 12:40 PM), <https://twitter.com/tmcsweenyftc/status/684474547131826177>.

278. See Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation*, 3 BERKELEY BUS. L.J. 129, 135 (2005) (“Known in information security and cryptography theory as ‘security through obscurity,’ this paradigm is considered inferior to a security paradigm predicated on Kerckhoff’s Law, or ‘security through process.’”).

279. See OFFICE OF THE INSPECTOR GEN., AUDIT OF THE U.S. DEPARTMENT OF JUSTICE ANNUAL FINANCIAL STATEMENTS FISCAL YEAR 2016 (2016), <https://oig.justice.gov/reports/2016/a1703.pdf>.

280. Orin Kerr, *Obama’s Proposed Changes to the Computer Hacking Statute: A Deep Dive*, WASH. POST (Jan. 14, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/01/14/obamas-proposed-changes-to-the-computer-hacking-statute-a-deep-dive/?utm_term=.bdf219365cc4 (“Instead of the current approach, which starts with a misdemeanor and becomes a 5-year-max felony if one of the enhancements applies, the Administration proposes that liability should start as a 3-year felony and become a 10-year-max felony if one of the enhancements applies.”).

281. However, it is noteworthy that individual attorneys in DOJ attend and speak at security conferences and have relationships in the security research community. See, e.g., *Speaker: Leonard Bailey*, BLACK HAT, <https://www.blackhat.com/us-15/speakers/Leonard-Bailey.html> (last visited Jan. 12, 2018).

282. For example, based on its website, DOJ does not appear to currently organize conferences at main Justice with external security researchers for the benefit of its attorneys, nor

information security statutes, the Computer Fraud and Abuse Act (CFAA)—a statute currently suffering from contentious circuit splits²⁸³—the deficit of formal feedback loops heightens the private sector’s feeling of uncertainty regarding prosecutorial discretion²⁸⁴ and interpretations of the law.²⁸⁵ Lawyers counsel clients that much gray area exists, and historic indictments are not always freely available for review.²⁸⁶ DOJ rarely issues enforcement guidance, with an exception occurring in the area of security information and antitrust enforcement.²⁸⁷ Perhaps most notably, the positions of the FTC and DOJ on the desirability²⁸⁸ of basic defensive technical

does it appear to have a Scholar in Residence program similar to that of the FTC. Although DOJ hosts training sessions for its attorneys and investigators in digital forensics at its conference center in South Carolina, budgetary constraints and time pressure undoubtedly limit the number of attorneys who can actually attend these sessions. See *Course Offerings: FY 2018*, U.S. DEP’T OF JUSTICE, <https://www.justice.gov/usao/training/course-offerings/schedule-2017> (last updated Sep. 21, 2017).

283. For a discussion of circuit splits in the CFAA, see, for example, Andrea M. Matwyshyn, *The Law of the Zebra*, 28 BERKELEY TECH. L.J. 155, 159 (2013) (“Applying the restrained technology exceptionalist paradigm to the case study of the CFAA-contract law circuit split . . .”); Jones Walker LLP, “*Cannibal Cop*” *Decision Deepens Circuit Split On Federal Hacking Statute*, TRADE SECRET INSIDER (Jan. 26, 2016), <http://www.tradesecretsinsider.com/cannibal-cop-decision-deepens-circuit-split-on-federal-hacking-statute/>.

284. See, e.g., Jamie Williams, *New Federal Guidelines for Computer Crime Law Do Nothing to Reign in Prosecutorial Overreach Under Notoriously Vague Statute*, ELECTRONIC FRONTIER FOUND. (Oct. 31, 2016), <https://www.eff.org/deeplinks/2016/10/what-were-scared-about-halloween-prosecutorial-discretion-under-notoriously-vague>.

285. *Id.*

286. The primary free method available to the public, apart from a Google query or the limited number of Pacer terminals available in libraries, requires searching through press releases on DOJ website. These press releases may not reflect all indictments or link to them. See *Justice News*, U.S. DEP’T JUST., <https://www.justice.gov/news> (last visited Jan. 12, 2018). By contrast, the SEC and CFPB website offer more robust searching capability. See *Division of Enforcement*, U.S. SEC. & EXCH. COMMISSION, <https://www.sec.gov/enforce> (last visited Jan. 12, 2018); *Enforcement Actions*, CONSUMER FIN. PROT. BUREAU, <https://www.consumerfinance.gov/policy-compliance/enforcement/actions/> (last visited Jan. 12, 2018).

287. For example, in 2014, DOJ and the FTC, the two agencies most active in antitrust law matters, signed a memorandum of cooperation regarding the permissibility of corporate information security information sharing under antitrust law. See DEP’T OF JUST. & FED. TRADE COMM’N: ANTI-TRUST POLICY STATEMENT ON SHARING OF CYBERSECURITY INFORMATION (2014), <https://www.justice.gov/sites/default/files/atr/legacy/2014/04/10/305027.pdf>; see also DEP’T OF JUST., A FRAMEWORK FOR A VULNERABILITY DISCLOSURE PROGRAM FOR ONLINE SYSTEMS, VERSION 1.0 (2017), <https://www.justice.gov/criminal-ccips/page/file/983996/download>.

288. The Pentagon also supports use of encryption. See *Pentagon Invites Hackers in and Backs Encryption*, BBC NEWS (Mar. 2, 2016), <http://www.bbc.com/news/technology-35706988>; Spencer Ackerman & Danny Yadron, *US Defense Chief Tells Silicon Valley:*

security measures such as encryption²⁸⁹ appear to the public to fundamentally conflict.

When baselines of understanding and approach are unintentionally balkanized in this manner, meaningful policy progress is hampered. Well-intentioned experts from both sides begin to talk past each other and can miss the bigger picture. This brings us to our third flaw: internet exceptionalism.

3. *Honeybadger don't cyber*:²⁹⁰ *Internet exceptionalism*

*Number of cybers in POTUS cybersecurity cyberspeech:
twenty-seven.*

—Professor Ed Felten²⁹¹

The term “cybersecurity” itself is a bug and not a feature of the security conversation. On any given day, Twitter is full of technical experts engaging in dark humor,²⁹² pointing out undesirable *internet exceptionalism*—what this Article calls the “cyberization”²⁹³ of information security policy by lawyers and policymakers. Security experts fear that in lieu of rigorously addressing the formidable security challenges our nation faces, our legal and policy discussions have instead devolved into a self-referential, technically inaccurate, and destructively amorphous “cyber-speak,”²⁹⁴ a legalistic mutant called

²⁸⁹ ‘Encryption is Essential’, GUARDIAN (Mar. 2, 2016, 4:39 PM), <https://www.theguardian.com/technology/2016/mar/02/apple-fbi-fight-silicon-valley-ashton-carter>.

²⁸⁹. For a discussion of the encryption law enforcement debate, see Stephanie K. Pell, *You Can't Always Get What You Want: How Will Law Enforcement Get What It Needs in A Post-CALEA, Cybersecurity-Centric Encryption Era?*, 17 N.C. J.L. & TECH. 599 (2016).

²⁹⁰. *Honey Badger*, KNOW YOUR MEME, <http://knowyourmeme.com/memes/honey-badger> (last visited Jan. 12, 2018).

²⁹¹. Ed Felten (@EdFelten), TWITTER (Feb. 13, 2015, 1:37 PM), <https://twitter.com/EdFelten/status/566350488820789248>.

²⁹². A Twitter account, @cybercyber, has also emerged mocking the over usage of cyber. See Danny Yadron & Jennifer Valentino-DeVries, *This Article Was Written with the Help of a ‘Cyber’ Machine*, WALL STREET J. (Mar. 4, 2015, 11:11 AM), <http://www.wsj.com/articles/is-the-prefix-cyber-overused-1425427767>.

²⁹³. The overuse of the prefix “cyber” regularly triggers snide commentary from prominent security professionals. See, e.g., SwiftonSecurity (@SwiftonSecurity), TWITTER (Feb. 21, 2016, 6:50 PM), <https://twitter.com/SwiftOnSecurity/status/701599848772927488>.

²⁹⁴. As explained recently by The Wall Street Journal, “[c]onscientious objectors like Mr. Stamos say cyber-buzzwords are short-circuiting a debate on an important issue, amid recent

“cybersecurity.”²⁹⁵ In other words, they worry that instead of valuing genuine technical expertise in security, the legal and policy audience erroneously believes that an accurate measure of expertise in security is determined by how many times a speaker can gratuitously attach²⁹⁶ the prefix “cyber” to various words in a sentence,²⁹⁷ sounding to a security-trained ear much like someone suffering from an unfortunate linguistic tick.

Superficially, this language discussion regarding the gratuitous attachment of the prefix²⁹⁸ “cyber” may seem to be merely the pedantic quibbling of veteran security experts. However, this “cyberization” problem is, in fact, significant for legal and policy reasons. Internet exceptionalist language implicitly neglects the physical aspects of security and unnecessarily injects damaging definitional imprecision into an already-complex security conversation.

*a. Put a cyber on it:*²⁹⁹ *Technical reality and cyberimprecision.*

[Cyber] means nothing.

—Michael McNerney³⁰⁰

Information security often involves nothing particularly “cyber.” A recent episode of the television series *Mr. Robot*³⁰¹ illustrates this

large-scale computer breaches at Anthem Inc., Target Corp., Sony Pictures Entertainment and others.” See Yadron & Valentino-DeVries, *supra* note 292.

295. See Joseph Blankenship, *Cybersecurity or Cyber Anything Usage*, NTT SECURITY: CYBERSECURITY USAGE BLOG (Oct. 18, 2013), <https://www.solutionary.com/resource-center/blog/2013/10/cybersecurity-usage/>; Yadron & Valentino-Devries, *supra* note 292.

296. Indeed, cyber is a popular buzzword bingo term: As explained by the WSJ, Yahoo!’s (then) CISO, “Mr. Stamos quipped on Twitter that he had won ‘CyberBingo’ at his table after a conference speaker warned of a ‘Cyber Pearl Harbor.’” Yadron & Valentino-Devries, *supra* note 292.

297. @allanfriedman, TWITTER (Nov. 15, 2017, 8:54 AM), <https://twitter.com/allanfriedman/status/930841552024428545>

298. See Sarah Laughton, *The History of the Prefix “-Cyber”*, GATEWAY TO THE LAUGHTON’S (2003), <http://www.laughton.com/cougar/writing/cyber.htm>.

299. *Put a Bird on It*, KNOW YOUR MEME, <http://knowyourmeme.com/memes/put-a-bird-on-it> (last visited Jan. 10, 2018).

300. Former “cyber policy adviser” for the Office of the Secretary of Defense. Yadron & Valentino-Devries, *supra* note 292.

301. *Mr. Robot* (USA television broadcast). *Mr. Robot* has fast acquired a loyal following among information security professionals and industry outsiders alike. See, e.g., Abigail Tracy,

reality.³⁰² The main character, an information security professional and “hactivist”³⁰³ named Elliot plots a large-scale attack on a multinational corporation.³⁰⁴ While the attack is to be carried out remotely through the internet, perhaps the most critical component of the attack involves physical security—it requires gaining physical access to a server farm in order to plant a device in an improperly-installed³⁰⁵ network of thermostats.³⁰⁶ In this way, a server farm that went to extremes in implementing internet security measures³⁰⁷ is, nevertheless, undermined in its overall information security³⁰⁸ through a series of human errors in physical space.³⁰⁹

As the compromise described above illustrates, there may be nothing “cyber” about the key step in an information security compromise. Yet, using the term “cybersecurity” seems to imply that information security issues are limited to code connected to the internet. As a technical matter, good information security is never solely “cyber”—physical security of machines and human manipulability through social engineering are always key aspects of information security in both the private and public sector. For

Mr. Robot's' Cyber Crime Expert Talks Accuracy, Hacking Misconceptions and What Other Shows Get Wrong, FORBES (July 8, 2015, 8:59 PM), <http://www.forbes.com/sites/abigailtracy/2015/07/08/mr-robots-cyber-crime-expert-talks-accuracy-hacking-misconceptions-and-what-other-shows-get-wrong/>; Kim Zetter, *Mr. Robot Is the Best Hacking Show Yet – But It's Not Perfect*, WIRED (July 8, 2015, 7:00 AM), <http://www.wired.com/2015/07/mr-robot-fact-check/>.

302. *Mr. Robot* is much lauded for the relative accuracy of its code breaking and fictionalized intrusion sequences. The major caveat to the accuracy of the show entails the timing of the depicted intrusions. Breaking code usually entails significantly longer periods of attack than the show can depict without boring a large portion of its audience. See, e.g., Tracy, *supra* note 301; Zetter, *supra* note 301.

303. For a discussion of hactivism, see, for example, GABRIELLA COLEMAN, HACKER, HOAXER, WHISTLEBLOWER, SPY (2014).

304. See generally *Mr. Robot* (USA television broadcast).

305. The thermostats in question were apparently all connected to a single network and compromising one allowed access to all the thermostats in the building. See Tim Surette, *Mr. Robot “Exploits” Review*, TV.COM (July 23, 2015), <http://www.tv.com/shows/mr-robot/community/post/mr-robot-season-1-episode-5-exploits-review-143758904580/>.

306. *MR. ROBOT: eps1.3_da3m0ns.mp4* & *eps1.4_3xpl0its.wmv*, (USA Network broadcasts July 15, 2015 & July 22, 2015).

307. *Id.*

308. *Id.*

309. See Abigail Tracy, *Humans as Exploits: ‘Mr. Robot’ Episode 5 Reality Check*, FORBES (July 22, 2015, 11:01 PM), <http://www.forbes.com/sites/abigailtracy/2015/07/22/humans-as-exploits-mr-robot-episode-5-reality-check/>.

example, there was nothing particularly “cyber” about Private Manning’s inserting a physical compact disc³¹⁰ or Edward Snowden’s using a thumb drive³¹¹ to copy sensitive government information,³¹² nor was it an exclusively “cyber” problem that HVAC contractor employees’ conduct compromised Target’s point of sale terminals.³¹³ The Target contractor in question provided heating and cooling services solely in physical space.³¹⁴ When an attacker socially engineers³¹⁵ a receptionist on the phone into issuing new credentials for a network or when an attacker dumpster dives³¹⁶ through a company’s improperly-shredded financials and proprietary information to repurpose them as part of an attack, these attacks are not primarily internet-driven. The dispositive information compromise often happens in *physical* space. As I have explained in my prior scholarship,³¹⁷ information security refers to the totality³¹⁸ of physical space and internet-enabled information control practices that a corporate or governmental organization maintains in a holistic manner.³¹⁹ Thus, not only is the “cybering” of security technically

310. See Jared Newman, *Fearing More Wikileaks, Military Bans DVDs, Thumb Drives*, PCWORLD (Dec. 10, 2010, 9:39 AM), http://www.pcworld.com/article/213226/Fearing_More_Wikileaks_Military_Bans_DVDs_Thumb_Drives.html.

311. See Shaun Waterman, *NSA Leaker Ed Snowden Used Banned Thumb-Drive, Exceeded Access*, WASH. TIMES (June 14, 2013), <http://www.washingtontimes.com/news/2013/jun/14/nsa-leaker-ed-snowden-used-banned-thumb-drive-exce/?page=all>; see also David Leigh, *How 250,000 US Embassy Cables Were Leaked*, GUARDIAN (Nov. 28, 2010, 1:14 PM), <http://www.theguardian.com/world/2010/nov/28/how-us-embassy-cables-leaked>.

312. Waterman, *supra* note 311.

313. See Thor Olavsrud, *11 Steps Attackers Took to Crack Target*, CIO (Sept. 2, 2014, 4:45 AM), <http://www.cio.com/article/2600345/security0/11-steps-attackers-took-to-crack-target.html>.

314. *Id.*

315. Jared Kee, *Social Engineering: Manipulating the Source* (Apr. 28, 2008) (unpublished paper), <https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-manipulating-the-source-32914>.

316. *Id.*

317. See Andrea M. Matwyszyn, *Hacking Speech: Informational Speech and the First Amendment*, 107 NW. U. L. REV. 795, 817 n.99 (2013).

318. *Id.* (“Information security is not solely an Internet phenomenon. Information security questions involve both computer security and physical security. They must be analyzed as a holistic enterprise relating to the systemic assessment of information risk throughout the life cycle of a piece of information—from the creation of a bit of information to its destruction.”).

319. RICHARD KISSEL ET AL., NAT’L INST. OF STANDARDS AND TECHNOLOGY, *SECURITY CONSIDERATIONS IN THE SYSTEM DEVELOPMENT LIFE CYCLE* (2008), <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-64r2.pdf>.

incorrect³²⁰ in its description of attack surface, but it is also likely to cause legal confusion and failed policy outcomes. In light of this technical reality, we might next ask from whence did all this legal cybering arrive?

b. The Knights Who Say Cyber: The cyber origin story.

*We are the Knights who say . . . NI . . . We are the keepers
of the sacred word.*

—Knight I³²¹

*We are no longer the knights who say Ni! We are now the
knights who say ekki-ekki-ekki-ptang-zoom-boing!*

—Knight I (later)³²²

Silicon Valley veterans regularly query, with a degree of befuddlement, why the term “cybersecurity” dominates policy discourse in Washington, D.C. around information security, when it is not the preferred term of art in Silicon Valley.³²³ In essence, the term “cybersecurity” is the consequence of a cultural divide between the two coasts: “cybersecurity” is the Washington, D.C. legal rebranding for what Silicon Valley veterans have historically usually called “infosec” or simply “security.”³²⁴ The origin story of the term “cybersecurity”³²⁵ varies a bit depending on source, but it is generally believed to be a combination of 1980’s science fiction terminology³²⁶

320. Matwyshyn, *supra* note 317 (“Referring to all of information security, particularly in private sector contexts, as ‘cybersecurity’ is technically incorrect.”).

321. MONTY PYTHON AND THE HOLY GRAIL (Michael White Productions 1975).

322. *Id.*

323. Yadron & Valentino-DeVries, *supra* note 292.

324. *See id.*; One data at a time (@curtisokrant), TWITTER (June 25, 2015, 12:32 AM), <https://twitter.com/curtisokrant/status/613973046420901889>; Michail S., *Closing Plenary: Information Security Programs in Academia [ShmooCon 2016]*, YOUTUBE (Feb. 5, 2016), <https://www.youtube.com/watch?v=rn0BdODPSbA> (video of a panel discussion of academics at ShmooCon, an annual security conference).

325. Annalee Newitz, *The Bizarre Evolution of the Word “Cyber,”* 109 (Sept. 16, 2013, 3:00 PM), <http://io9.com/today-cyber-means-war-but-back-in-the-1990s-it-mean-1325671487>.

326. *See generally* WILLIAM GIBSON, NEUROMANCER (1984).

and military- speak.³²⁷ The prefix “cyber”³²⁸ derives from the work of William Gibson,³²⁹ the science fiction author who coined the term “cyberspace.”³³⁰ In the 1990s, members of the military began to speak of “the cyberspace domain”³³¹—a hypothetical separate battlefield³³² that is distinct from and often perceived to be compartmentalized³³³ away from terrestrial space.³³⁴ Thus, when members of the military speak of security on this hypothetical battlefield, they speak of security “of the cyber domain” or “cyber security.”³³⁵ This military parlance then likely crept into DC policy conversations more generally.³³⁶

However, I will also posit a second contributing origin story—a uniquely legal one that might be termed the “cyberlaw legacy problem.” Many policymakers are attorneys, and very few attorneys have received any formal legal education in information security law.³³⁷ At best, assuming that attorneys graduated after 2000, the one

327. See DEP’T OF THE ARMY, NO. 3-38 CYBER ELECTROMAGNETIC ACTIVITIES, *in* ARMY FIELD MANUALS (2014), <http://fas.org/irp/doddir/army/fm3-38.pdf>.

328. The prefix *cyber-* comes from the word *cybernetic*, arising “from the Greek word *kubernētēs* (κυβερνήτης), ‘steersman’, from *kubernan* ‘to steer’”. Taylor Coe, *Where is the Origin of ‘Cyber’?*, OXFORD DICTIONARIES: BLOG (Mar. 5, 2015), <http://blog.oxforddictionaries.com/2015/03/cyborgs-cyberspace-csi-cyber/>.

329. Gibson recently expressed his concerns regarding the rampant overuse and datedness of the “vintage” prefix “cyber.” See Yadron and Valentino-DeVries, *supra* note 292. Gibson stated, “[c]yberspace is a heritage term for a heritage concept . . . We [now] drive cybercars, chill our food in cyberfridges, conduct the majority of our affairs over cyberphones, in, literally, a cyberworld.” *Id.*

330. See generally GIBSON, *supra* note 326.

331. See DEP’T OF THE ARMY, *supra* note 327.

332. See *id.*

333. For instance, the Army Field Manual No. 3-38 Cyber Electromagnetic Activities describes “cyberspace” as being distinct from the other “domains” as follows: “The four traditional domains (air, land, maritime, and space) and the EMS exist naturally. The fifth domain, cyberspace, is manmade.” *Id.*

334. *Id.*

335. See, e.g., *Introduction to the Cyber Domain*, US NAVAL ACADEMY, <https://www.usna.edu/CyberDept/sy110/lec/crsIntro/lec.html>.

336. Despite coining the term “cyber domain,” the military has recently begun to worry about what one officer termed the “dolphin speak” of its cyber branch members. See Sydney J. Freedberg Jr., *Army Fights Culture Gap Between Cyber & Ops: ‘Dolphin Speak’*, BREAKING DEFENSE (Nov. 10, 2015, 5:58 PM), <http://breakingdefense.com/2015/11/army-fights-culture-gap-between-cyber-ops-dolphin-speak/>. Efforts are underway to better incorporate these soldiers into physical operations to eliminate a siloed approach to security. See *id.* Thus, the military is arguably shifting away from an internet exceptionalist paradigm.

337. Indeed, even most technology professionals have received little or no training in information security. Michail S, *supra* note 324.

technology class they may have taken in law school was an internet law overview class often entitled “Cyberlaw.”³³⁸ While the vernacular of technology experts was already moving away from using the term “cyber” in the early 2000s,³³⁹ most attorneys were just beginning to become comfortable with (using search engines and) the term “cyberspace.”³⁴⁰ Indeed, a debate raged in the legal scholarship (and in law school classrooms) at the time regarding whether the internet was a separate space,³⁴¹ an extension of physical space,³⁴² or a hybrid thereof.³⁴³ Thus, when later faced with this “new” set of legal problems partially involving computers and security, many lawyers’ instinct would have likely been toward internet exceptionalism—to fixate on the presence of an internet aspect to information security. Harkening back to “cyberlaw” class, it would have seemed logical to them to append a “cyber”³⁴⁴ to the front of security and attempt to conceptually compartmentalize it for themselves as a subfield of

338. The earliest information security law courses in law schools were taught circa 2006–07. See, e.g., *Faculty Course Evaluations*, U. FLA., <https://evaluations.ufl.edu/results/instruct.or.aspx?ik=-131504421> (last visited Jan. 12, 2018).

339. See Newitz, *supra* note 325.

340. For example, Professor Lawrence Lessig’s seminal internet law book *Code and Other Laws of Cyberspace* was published in 1999. See LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* (1999).

341. For a discussion of the debate, see generally Charles Fried, *Perfect Freedom or Perfect Control?*, 114 HARV. L. REV. 606, 618–20 (2000); Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1199–1200 (1998); David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); Andrew L. Shapiro, *The Disappearance of Cyberspace and the Rise of Code*, 8 SETON HALL CONST. L.J. 703, 709 (1998).

342. Compare, Frank Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207 (1996), with Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999).

343. For a discussion of the hybrid nature of the internet, see, for example, Matwyshyn, *supra* note 283, at 155 (introducing a paradigm of “restrained technology exceptionalism”).

344. A humorous language problem has now emerged for these “cyberized” security attorneys as DC policy-speak mutated and began to drop the “security” in “cybersecurity,” leaving only a “cyber.” These “cybersecurity” attorneys are now in the awkward position of saying they practice “cyber law” and needing to explain that they don’t mean “cyberlaw” (i.e. internet law) but rather they mean “cyber law” (i.e. the policy area formerly known as “cybersecurity”) or “cyber cyberlaw.” This evolution likely resulted from the definitional deficit described above—the failure to consider physical security as key to information security.

“cyberlaw.”³⁴⁵ Legal academics have also, unfortunately, widely³⁴⁶ embraced this “cyberized” information security legal discourse.³⁴⁷ Yet, as the prior sections have explained, framing our national security and economic security questions in an internet exceptionalist way likely exacerbates the problem of reciprocal security vulnerability rather than remedying it.

Having identified these three analytical flaws of privacy-conflation, incommensurability, and internet exceptionalism, let us now begin to reframe the security conversation in more constructive directions in Part III.

III. I SEE WHAT YOU CYBERED THERE:³⁴⁸ KLUDGING TOGETHER A ROBUST SECURITY PARADIGM

*Once you've accepted your flaws, no one can use them
against you.*

—Tyrion Lannister³⁴⁹

The future of information security, though superficially bleak, is not beyond improvement. With the technical realities introduced in Part II in mind, Part III begins to address the problem of reciprocal security vulnerability. This Part borrows themes from the work of noted philosopher of science Michael Polanyi, the famous cognitive exercise of the Monty Hall problem, and the First Amendment theory construct of epistemological humility. It theoretically sets the stage for

345. Also, calling the policy space “cyber” but the legal space “cyberlaw” will confuse the listener as to whether the speaker is using the antiquated name for internet law or referring to information security law.

346. This author eschews the word “cyber” except in jest or in reference to other people’s branding. She refers to the field as information security law, data security, or simply security. *See, e.g.*, Andrea Matwyshyn (@amatwyshyn), TWITTER (Jan. 20, 2015, 1:28 PM), <https://twitter.com/amatwyshyn/status/557650958583599104>. I also may or may not have been instrumental in bestowing the name CYBER! on a neighborhood weasel. *See* Andrea Matwyshyn (@amatwyshyn), TWITTER (May 10, 2015, 4:21 PM), <https://twitter.com/amatwyshyn/status/597541926192185344>; Andrea Matwyshyn (@amatwyshyn), TWITTER (May 16, 2015, 9:25 AM), <https://twitter.com/amatwyshyn/status/599611692255813632>.

347. Running a Westlaw query for articles with at least 25 instances of “cybersecurity” yields results of 195; the same query using “cyber security” yields 33 results; “information security” and “data security” yields results of 43 and 97 respectively.

348. *I See What You Did There*, KNOW YOUR MEME, <http://knowyourmeme.com/memes/i-see-what-you-did-there> (last visited Jan. 12, 2018).

349. *Game of Thrones: The North Remembers* (HBO television broadcast Apr. 1, 2012).

reframing the paradigms of information sharing and deterrence into a novel security paradigm better suited to addressing the problem of reciprocal security vulnerability.

A. Cybers, How Do They Work?:³⁵⁰ Lessons from Polanyi

We can never see past the choices we don't understand.

—The Oracle³⁵¹

The philosophy of Friedrich Hayek has been widely applied in legal scholarship to analyze questions of innovation.³⁵² For example, Professor Tim Wu has applied Hayek's analysis of the benefits of decentralization and emerging order to questions of intellectual property rights, industry structure and "the effect of rights assignments on the decision architectures of affected industries."³⁵³ But, before there was Hayek's well-known concept of "spontaneous order," there was Michael Polanyi's notion of "dynamic order."³⁵⁴

It is Polanyi's work rather than Hayek's that better lends itself to inspiring novel frameworks for innovation policy areas such as information security. Polanyi's work reflects an embeddedness of the individual within a broader society that stands wholly apart from economic considerations; unlike Hayek's work, Polanyi's work does not focus on the primacy of economics. Instead, it views emergent scientific knowledge and law as equal, if not more important, forces alongside economics. This three-part focus—science, law, and

350. "Miracles" / *Fucking Magnets, How Do They Work?*, KNOW YOUR MEME, <http://knowyourmeme.com/memes/fucking-magnets-how-do-they-work> (last visited Jan. 11, 2018).

351. THE MATRIX (Village Roadshow Pictures 1999).

352. See, e.g., Ellen Frankel Paul, *Hayek on Monopoly and Antitrust in the Crucible of United States v. Microsoft*, 1 N.Y.U. J.L. & LIBERTY 167 (2005); Richard S. Whitt, *Adaptive Policymaking: Evolving and Applying Emergent Solutions for U.S. Communications Policy*, 61 FED. COMM. L.J. 483 (2009).

353. See Tim Wu, *Intellectual Property, Innovation, and Decentralized Decisions*, 92 VA. L. REV. 123, 124 (2006).

354. Michael Polanyi was an underappreciated predecessor to and contemporary of Friedrich Hayek. Some of Hayek's core observations regarding spontaneously emerging order are asserted to be more correctly attributed to Polanyi. See, e.g., Struan Jacobs, *Michael Polanyi and Spontaneous Order, 1941-1951*, 24 POLANYI SOC'Y PERIODICAL, no. 2, 1997, at 14, <http://polanysociety.org/TAD%20WEB%20ARCHIVE/TAD24-2/TAD24-2-pg14-28-pdf.pdf> ("[W]ork of Polanyi, an essay-collection published in 1951, predated Hayek's *The Constitution of Liberty* by almost a decade and, indeed, several of the essays had been published in journals well before 1951.").

economics—makes Polanyi’s work a compelling and logical touchstone for innovation policy discussions.

Despite its natural fit for innovation law and policy, Polanyi’s work has never been expansively³⁵⁵ applied in the law review literature to questions of security,³⁵⁶ and only a small number of articles in the current legal scholarship engage with Polanyi’s scholarship substantially.³⁵⁷ Three scholars have applied Polanyi’s work to intellectual property concerns: Professor Russell Hardin has analyzed a concrete proposal made by Polanyi for patent reform,³⁵⁸ Professor Ron Bouchard has applied Polanyi to the discussion of appropriate PHOSITA skill construction in pharmaceutical patent litigation,³⁵⁹ and Professor Margaret Chon has used Polanyi’s construct of tacit knowledge to discuss what she has termed “sticky knowledge” in copyright.³⁶⁰ Non-intellectual property scholarship employing Polanyi’s theory includes the work of Professor Kevin Keeler, who has presented an alternative account of mental state inference processes based upon Polanyi’s theory of tacit knowledge.³⁶¹ Professor Charles Barzun has explained that Polanyi’s work likely influenced the legal theory of H.L.A. Hart and Lon Fuller, who corresponded with Polanyi.³⁶² And, finally, Professor David ButleRitchie has applied Polanyi’s insights to legal pedagogy.³⁶³ This Part contributes to the existing scholarship by using Polanyi’s philosophy of science to reframe the legal discussion of information security and to address reciprocal security vulnerability.

355. It has been mentioned briefly by some authors, however. *See infra* note 356.

356. The two most extensive uses appear in Russell Hardin, *Valuing Intellectual Property*, 68 CHI.-KENT L. REV. 659, 660 (1993) (discussing patent reform), and Charles L. Barzun, *The Forgotten Foundations of Hart and Sacks*, 99 VA. L. REV. 1, 49 (2013) (discussing Hart and Sacks).

357. A Westlaw query of secondary sources with 15+ mentions of Michael Polanyi’s work yielded limited results.

358. Hardin, *supra* note 356, at 659.

359. *See generally* Ron A. Bouchard, *Living Separate and Apart is Never Easy: Inventive Capacity of the PHOSITA as the Tie That Binds Obviousness and Inventiveness in Pharmaceutical Litigation*, 4 U. OTTAWA L. & TECH. J. 1 (2007).

360. *See generally* Margaret Chon, *Sticky Knowledge and Copyright*, 2011 WIS. L. REV. 177.

361. *See generally* Kevin L. Keeler, *Direct Evidence of State of Mind: A Philosophical Analysis of How Facts in Evidence Support Conclusions Regarding Mental State*, 1985 WIS. L. REV. 435.

362. Barzun, *supra* note 356, at 49–52.

363. David T. ButleRitchie, *Situating “Thinking Like a Lawyer” Within Legal Pedagogy*, 50 CLEV. ST. L. REV. 29 (2002).

1. *Forever cyberalone*:³⁶⁴ *The pain of polycentric problems*

For Polanyi, humans are driven in part by notions of progress, innovation, and science as ends in themselves. As Polanyi puts it: “Freedom of science, freedom of worship, freedom of thought in general, are public institutions by which society opens to its members the opportunity for serving aims that are purposes in themselves.”³⁶⁵ This assertion of significant, intrinsic, nonpecuniary³⁶⁶ motivation resonates with the scholarly findings of the psychology of creativity³⁶⁷ and with those of legal scholars such as Professor Jessica Silbey.³⁶⁸ This resonant framing also makes Polanyi a fit for the ethos and culture of the information security community.

Polanyi’s work offers us important insights on a way forward in information security: as a philosopher of science, he was committed to scientific inquiry as the route to solving what he defined as “polycentric” problems—those that involve “balancing a large number of elements.”³⁶⁹ For Polanyi, “[t]he proper method of managing a polycentric task is . . . not by collecting all the data at one centre and evaluating them jointly” but rather by relying on an uncoordinated “team of independent calculators,” each of whom solves the problem “in respect to one centre at a time.”³⁷⁰ Indeed, Polanyi explains the process toward solutions of polycentric problems as inherently and intentionally incremental³⁷¹:

Imagine that we are given the pieces of a very large jigsaw puzzle, and suppose that for some reason it is important that our giant puzzle be put together in the shortest possible time. . . . The only way the assistants can effectively co-operate, and surpass by far what

364. *Forever Alone*, KNOW YOUR MEME, <http://knowyourmeme.com/memes/forever-alone> (last visited Jan. 12, 2018).

365. MICHAEL POLANYI, *THE LOGIC OF LIBERTY: REFLECTIONS AND REJOINDERS* 193 (1951).

366. See McLaughlin, *supra* note 155.

367. See, e.g., JENNIFER MUELLER, *CREATIVE CHANGE* (2017).

368. See JESSICA SILBEY, *THE EUREKA MYTH: CREATORS, INNOVATORS, AND EVERYDAY INTELLECTUAL PROPERTY* (2014).

369. See POLANYI, *supra* note 365, at 176.

370. *Id.* at 180–81. Polanyi called this “the Relaxation Method.” *Id.* at 180–83

371. *Id.* at 159 (“When order is achieved among human beings by allowing them to interact with each other on their own initiative—subject only to laws which uniformly apply to all of them—we have a system of spontaneous order in society.”).

any single one of them could do, is to let them work on putting the puzzle together in sight of the others so that every time a piece of it is fitted in by one helper, all the others will immediately watch out for the next step that becomes possible in consequence. Under this system, each helper will act on his own initiative, by responding to the latest achievements [of] the others, and the completion of their joint task will be great accelerated. We have here in a nutshell the way in which a series of independent initiatives are organized to a joint achievement by mutually adjusting themselves at every successive stage to the situation created by all the others who are acting likewise.³⁷²

Applying lessons from Polanyi, it might be said that the challenges we are witnessing in crafting successful information security law and policy potentially result at least in part from four factors. The first two are a natural consequence of the substantive character of information security as a discipline—first, the polycentrism of the challenges of information security and, second, the necessity of incrementalism under time pressure. The third and fourth factors relate to what Polanyi calls “tacit knowledge” and “subsidiary awareness.”

2. *Y U NO cyber?*³⁷³ *Transmission of tacit knowledge*

Polanyi’s work identifies a third factor that may be less obvious but is equally important—tacit knowledge. A “tacit knowledge” conflict currently exists within the two “dynamic orders,” security researchers and lawyers, who are working to try to address the challenges of information security.³⁷⁴ Polanyi views both science and law as “dynamic orders,”³⁷⁵ or iteratively self-adjusting groups of individuals with influence.³⁷⁶ He characterizes science as predominantly a “cognitive” dynamic order, but he deemed law a

372. See Michael Polanyi, *The Republic of Science: Its Political and Economic Theory*, 1 *Minerva*, no.1, 1962, at 54, http://sciencepolicy.colorado.edu/students/envs_5100/polanyi_1967.pdf.

373. “Y U NO” Guy, KNOW YOUR MEME, <http://knowyourmeme.com/memes/y-u-no-guy> (last visited Jan. 12, 2018).

374. See discussion of incommensurability, *supra* Section II.B.2.

375. Just as scientific and technical communities build knowledge internally in a dynamically ordered manner, common or case law, Polanyi explained, “arises by a process of direct adjustments between succeeding judges.” Michael Polanyi, *The Growth of Thought in Society*, 8 *ECONOMICA* 428, 436 (1941).

376. *Id.*

“mainly normative” one.³⁷⁷ He explains that “[i]n each field” generations pass on “a public mental heritage”³⁷⁸ comprised of both substantive and “tacit knowledge,”³⁷⁹ the unspoken but shared culture of “knowing how” one obtains only from being inside the community.³⁸⁰ Thus, in information security, two dynamically ordered professions—one cognitive (security researchers) and one normative (lawyers)³⁸¹—clash. Two meaningfully different types of “public mental heritage”³⁸²—law and computer security—with different and elaborate bodies of “tacit knowledge” must learn to cooperate with each other to address the polycentric problem of information security. In other words, these two communities, lawyers and security professionals, must reconcile not only the patent process of dynamic cooperation on the substance of information security, but also more generally they must address the latent conflict of their baselines of tacit knowledge. Both relevant dynamic order of experts—security researchers and lawyers—must acquire each others’ perspectives. This is the challenge that lurks beneath the surface of the security policy debate—the challenge of what Polanyi calls “comprehension.”³⁸³

As Polanyi explains, “The structure of tacit knowing is manifested most clearly in the act of understanding. It is the process of *comprehending*: a grasping of disjointed parts into a comprehensive whole.”³⁸⁴ In other words, both relevant dynamic orders of experts—security researchers and lawyers—must become part of Polanyi’s metaphorical jigsaw puzzle team. Making progress in information security law and policy will require that the tacit

377. *Id.* at 438.

378. *Id.*

379. Through consultation, competition, or a combination of the two, new participants adjust to the evolution of the space. “Then, when they suggest their own additions or reforms, they return to the public and claim publicly that these be accepted by society—to become in their turn a part of the common heritage.” *Id.*

380. He explains that “[p]ractical skills and practical experience contain much more information than people possessing this expert knowledge can ever tell. Particulars that are not known focally are unspecifiable . . . A man’s mind can be known *only comprehensively, by dwelling within the unspecifiable particulars of its external manifestations.*” MICHAEL POLANYI, *THE STUDY OF MAN* 33 (1958).

381. Polanyi would describe both as “circles of special interest and professional bodies” who act as gatekeepers. Polanyi, *supra* note 375, at 441.

382. *Id.* at 438.

383. *See* POLANYI, *supra* note 380, at 28.

384. *See id.*

knowledge of both security researchers and lawyers become mutually comprehended. Employing the perspectives of lawyers alone in policy, quashing the technical objections of researchers and security engineers, will irreparably harm both innovation and the national security of the United States.³⁸⁵

3. *Wow! Such cyber:*³⁸⁶ *Subsidiary awareness*

Without becoming Polanyi's hypothetical cooperating jigsaw puzzle team, both security researchers and lawyers will arrive at suboptimal and inefficient processes and outcomes.³⁸⁷ Polanyi explains that "[b]y looking very closely at the several parts of a whole, we may succeed in diverting our attention from the whole and even lose sight of it altogether."³⁸⁸ In this way, Polanyi explains and cautions against the risks of the privacy conflation problem identified in Part II.

Polanyi's work also offers a warning to be vigilant of the incommensurability problems introduced in Part II.³⁸⁹ He asserts:

We have seen how comprehension can be destroyed altogether by shifting attention from its focus to its subsidiary particulars. It is not

385. *See supra* Section II.B.3.

386. *Doge*, KNOW YOUR MEME, <http://knowyourmeme.com/memes/doge> (last visited Jan. 12, 2018).

387. As Polanyi explains, "[w]e cannot comprehend a whole without seeing its parts, but we can see the parts without comprehending the whole. Thus we may advance from a knowledge of the parts to the understanding of the whole." POLANYI, *supra* note 380, at 29.

388. *Id.* Polanyi explains further:

Once comprehension is achieved, we are not likely to lose sight again of the whole; yet comprehension is not completely irreversible. . . .

These psychological observations can be transposed now into the elements of a theory of knowledge. We may say that when we comprehend a particular set of items as parts of a whole, the focus of our attention is shifted from the hitherto uncomprehended particulars to the understanding of their joint meaning. This shift of attention does not make us lose sight of the particulars, since one can see a whole only by seeing its parts, *but it changes altogether the manner in which we are aware of the particulars. We become aware of them now in terms of the whole on which we have fixed our attention.* I shall call this a *subsidiary awareness* of the particulars, by contrast to a *focal awareness* which would fix attention on the particulars in themselves, and not as parts of a whole. I shall also speak correspondingly of a *subsidiary* knowledge of such items, as distinct from a *focal* knowledge of the same items.

Id. at 29–30 (emphasis in original).

389. *See supra* Section II.B.2.

surprising, therefore, that we may often apprehend wholes without ever having focally attended to their particulars. In such cases we are actually ignorant, or perhaps more precisely speaking, focally ignorant of these particulars; we know them only subsidiarily in terms of what they jointly mean, but cannot tell what they are in themselves.³⁹⁰

Finally, Polanyi's work similarly holds insights on addressing the internet exceptionalism problem we see in information security law and policy as detailed in Part II.³⁹¹ He reminds us to focus on technologies' purpose, not on technologies as objects themselves.³⁹² He warns that, for example, "[t]he skillful use of a tennis racket can be paralysed by watching our racket instead of attending to the ball and the court in front of us."³⁹³ He calls this focus on the whole while engaging with particulars the state of "subsidiary awareness,"³⁹⁴ and he contrasts subsidiary awareness with the less productive state of "focal awareness,"³⁹⁵ focusing on particulars while missing the whole.³⁹⁶ When examining the highly compartmentalized and definitionally-muddled approaches to security in the public and private sector described in Part II, it becomes obvious that our first step in improving the state of information security involves striving for subsidiary awareness.

Polanyi's work, however, still leaves us without guidance regarding learning to anticipate the next generation of information security problems specifically. With this query, let us turn to the Monty Hall problem for a lesson on perspective-taking.

390. *See* POLANYI, *supra* note 380, at 32–33.

391. *See supra* Section II.B.3.

392. *See* POLANYI, *supra* note 380, at 30–31 ("Symbols can serve as instruments of meaning only by being known subsidiarily while fixing our focal attention on their meaning. And this is true similarly of tools [and] machines. . . . Their meaning lies in their purpose; they are not tools, machines, etc., when observed as objects in themselves, but only when viewed subsidiarily by focusing attention on their purpose.").

393. *Id.* at 31.

394. *Id.* at 30.

395. *Id.*

396. *Id.*

B. You Had One Cyberjob:³⁹⁷ The Monty Hall Problem

Buttercup: *And to think, all that time it was your cup that was poisoned.*

Man in Black: *They were both poisoned. I spent the last few years building up an immunity to iocane powder.*³⁹⁸

The Monty Hall problem³⁹⁹ is a notorious⁴⁰⁰ probability question that initially foiled some of the greatest minds in mathematics.⁴⁰¹ Although the question appears simple,⁴⁰² it is frequently confounding⁴⁰³ because it exploits the conflict between human intuition and math.⁴⁰⁴ The problem is set forth as follows: imagine that you are a contestant on a game show where Monty Hall⁴⁰⁵ is the host. Monty tells you that behind the three doors in front of you, there are two goats and one car.⁴⁰⁶ Your task is to guess which of the doors conceals the car.⁴⁰⁷ You select one door, say door number one. Monty

397. *You Had One Job*, KNOW YOUR MEME, knowyourmeme.com/memes/you-had-one-job (last visited Jan. 12, 2018).

398. *THE PRINCESS BRIDE* (Act III Communications 1987).

399. *The Monty Hall Problem*, RANDOM, www.math.uah.edu/stat/games/MontyHall.html (last visited Jan. 12, 2018).

400. See Zachary Crockett, *The Time Everyone “Corrected” the World’s Smartest Woman*, PRICEONOMICS (Aug. 2, 2016), <https://priceonomics.com/the-time-everyone-corrected-the-worlds-smartest/>.

401. *Id.*

402. *Now Playing Let’s Make A Deal*, UCSD MATHEMATICS, <https://math.ucsd.edu/~crypto/Monty/montybg.html> (last visited Jan. 11, 2018).

403. *Id.*

404. *Id.*

405. Monty Hall was a television personality in the 1970s on the TV game show, *Let’s Make a Deal*. See, *Monty Hall Biography*, BIOGRAPHY, www.biography.com/people/monty-hall-9542238 (last updated Oct. 2, 2017).

406. *Game Show Problem*, MARILYNVOSSAVANT.COM, marilynvoissant.com/game-show-problem/ (last visited Jan. 12, 2018).

407. *Id.* The framing of this problem presumes that a car is preferable to a goat—a bold assumption. Goats are charming creatures whose lawn mowing and garbage consumption capabilities are both formidable and ecologically desirable. Indeed, an industry of goat rentals has emerged. See *Hire a Goat Grazer*, COOLEST STUFF EVER, <https://thecooleststuffever.com/hire-goat-grazer> (last visited Jan. 12, 2018). Goats have also introduced new market segmentation into yoga, and current demand for goat yoga classes outstrips supply. *“Pee on Your Yoga Mat”: Goat Yoga Craze is Sweeping the Country*, USA TODAY (Apr. 28, 2017, 12:28 PM) <https://www.usatoday.com/story/news/nation-now/2017/04/28/pee-your-yoga-mat-goat>

Hall opens a different door, say door number two, and it reveals a goat.⁴⁰⁸ Monty Hall then asks you if you would like to change your selected door to door number three.⁴⁰⁹ By working through the probability analysis, mathematically it makes sense to switch doors to the unselected door.⁴¹⁰ Yet, intuitively, most people hesitate to align their choices with the math and fail to switch.⁴¹¹ The Monty Hall problem has been referenced in legal literature in, for example, discussions of offender profiling,⁴¹² standards of proof,⁴¹³ paternalism,⁴¹⁴ the psychology of litigation,⁴¹⁵ and bias in decision-making.⁴¹⁶ It has not to date been applied to questions of information security, technology, or innovation.

Now, let us try the Monty Hall problem again, but this time let us analyze it as an information security problem of adversarial perspective-taking. Because you are assigned the role of the contestant, your assigned perspective has likely colored your analysis of the situation—in much the same way that we are taught that wall clocks with hands run clockwise.⁴¹⁷ Now, invert your thinking. Let us rerun the problem where you analyze the decisions and your conduct not from your assigned role, but instead from the strategic position of

-yoga-craze-sweeping-country/307495001/1; *Goat Yoga? A Look at the Latest Fitness Craze*, NBC NEWS (June 16, 2017) <https://www.nbcnews.com/nightly-news/video/goat-yoga-a-look-at-the-latest-fitness-craze-969581123698>; AJ Willingham, “Goat Yoga” is a Thing – and Hundreds are Lining Up for it, CNN (Jan 12, 2017, 11:08 AM) <http://www.cnn.com/2017/01/12/health/goat-yoga-oregon-trnd/index.html>.

408. *Now Playing Let’s Make a Deal*, *supra* note 402.

409. *Id.*

410. In other words, it has a 2/3 chance of hiding the car. *Id.*

411. They erroneously intuit their chances to be 50/50 between the two doors. One reply to this failing of intuition is that one should simply trust the math. Yet, this response is not intuitively satisfying. *Id.*

412. See D. Michael Risinger & Jeffrey L. Loop, *Three Card Monte, Monty Hall, Modus Operandi and “Offender Profiling”: Some Lessons of Modern Cognitive Science for the Law of Evidence*, 24 CARDOZO L. REV. 193 (2002).

413. See Kevin M. Clermont, *Death of Paradox: The Killer Logic Beneath the Standards of Proof*, 88 NOTRE DAME L. REV. 1061 (2013).

414. See Jeffrey J. Rachlinski, *The Uncertain Psychological Case for Paternalism*, 97 NW. U. L. REV. 1165 (2003).

415. See Jeffrey J. Rachlinski, *Gains, Losses, and the Psychology of Litigation*, 70 S. CAL. L. REV. 113 (1996).

416. See Gregory Mitchell, *Second Thoughts*, 40 MCGEORGE L. REV. 687 (2009).

417. For an example of a clock whose hands run backwards see, e.g., Andrea Matwyshyn (@amatwyshyn), TWITTER (Dec. 9, 2015, 5:45 AM), <https://twitter.com/amatwyshyn/status/674585635211079680>.

Monty Hall. By understanding Monty, you understand both sets of information dynamics—both yours and his—empowering yourself with a more thorough analytical framework. Monty Hall is your adversary⁴¹⁸ who acts as an “oracle”:⁴¹⁹ he knows a secret, and you can ask him about that secret, but he has no incentive to help you. Still, his responses reveal potentially useful information about the secret. He knows where the car is and, therefore, when he reveals where the car isn’t, he “leaks” potentially useful information to you.

At the beginning of the problem, both you and Monty each had a one-third chance that you would guess the car correctly. But, in the second round, the dynamics have changed. Monty knows whether you have, in fact, guessed correctly. But he has no incentive to tell you. The information balance has now shifted in his favor. He will now act strategically to his advantage when he opens a particular door hiding a goat. In doing so, he has potentially steered your attention away from another door—the door more likely to have a car. In this way, he provides you with useful information when analyzed in the context of *his* motivations and superior knowledge. You should, therefore, logically change your chosen door and pick the door from which Monty has potentially steered you away.⁴²⁰

This type of strategic adversarial thinking is the “secret sauce” of most skilled information security researchers and strategists. One might view it as akin to the skill of being able to tell time on clocks that run not only clockwise, but also on clocks that run counterclockwise. It is only by putting yourself in the mind of the adversary and understanding his incentives, motivations, and “tells” that you develop the skills to correctly anticipate *your own* vulnerabilities. As Polanyi might say, it is through seeing the problem

418. In cryptography, an adversary is a malicious entity attempting to prevent you from achieving your goals. *See, e.g.*, Ananth Raghunathan, *Proofs in Cryptography* (2012), <https://crypto.stanford.edu/~ananthr/docs/crypto-proofs.pdf> (unpublished handout).

419. An oracle is “a black box input/output method. It will respond to any input with a pseudo-random response but will always give the same output for a specific input.” *See What is a Cryptographic Oracle?*, INFO. SECURITY (Jan. 12, 2012), <https://security.stackexchange.com/questions/10617/what-is-a-cryptographic-oracle>.

420. For a humorous depiction of this type of analytical process, see *Princess Bride*, *supra* note 398 (“But it’s so simple. All I have to do is divine from what I know of you: are you the sort of man who would put the poison into his own goblet or his enemy’s? Now, a clever man would put the poison into his own goblet, because he would know that only a great fool would reach for what he was given. I am not a great fool, so I can clearly not choose the wine in front of you. But you must have known I was not a great fool, you would have counted on it, so I can clearly not choose the wine in front of me.”).

as a whole and with the eyes of the attacker that you acquire the requisite tacit knowledge—the practical skills and practical experience—of thinking like an attacker in order to anticipate attacks.

When one begins to think like an attacker in security, it becomes apparent that choice of target for attackers is primarily driven by the nature of the information that the target holds and the extent of vulnerability of the target's system. In other words, *the fiercest information security adversaries do not generally distinguish between private sector and public sector entities. They strike wherever desirable information resides and where unpatched vulnerabilities allow for ease of security compromise.* This insight lies at the core of addressing the problem of reciprocal security vulnerability.

Thus, when we adopt this perspective taking approach from our analysis of the Monty Hall problem and blend it with the insights from Polanyi discussed in the previous section, we understand that the only path to successful information security policy is through a simultaneous, mutually reinforcing security effort in both the public and private sector. Both sectors must not only work together toward the common goal of comprehension of security but also lead each other by example and nudge each other toward continual improvement. This reciprocal leadership by example approach starts with the injection of a healthy dose of the critical self-reflection that First Amendment theorists have called epistemological humility.⁴²¹

*C. Are You a Cyberwizard?:⁴²²
The Principle of Epistemological Humility*

*Actually, I'm an overnight success, but it took
twenty years.*

—Monty Hall⁴²³

421. Martin H. Redish, *Product Health Claims and the First Amendment: Scientific Expression and the Twilight Zone of Commercial Speech*, 43 VAND. L. REV. 1433, 1435 (1990) (“The principle of epistemological humility’ . . . posits that whatever the currently prevailing beliefs may be, history teaches us that scientific or moral advances may at some future point make those beliefs appear either silly or monstrous.”).

422. *Are You a Wizard*, KNOW YOUR MEME, <http://knowyourmeme.com/memes/are-you-a-wizard> (last visited Jan. 12, 2018).

423. *Monty Hall Quotes*, BRAINY QUOTE, http://www.brainyquote.com/quotes/authors/m/monty_hall.html (last visited Jan. 12, 2018).

Security professionals have long warned of the arrival of a caste of security “charlatans.”⁴²⁴ But distinguishing goats from sheep⁴²⁵ in security itself requires training. People who hold themselves out as “cybersecurity experts” are not uniformly skilled.

In one of the most famous episodes of the British technology comedy *The IT Crowd*,⁴²⁶ two of the main characters—disgruntled technology professionals Moss and Roy—convince their technology-illiterate manager that the internet emanates from a small black box with a blinking red light that usually sits at the top of Big Ben.⁴²⁷ They present this magic box and encourage their manager, Jen, to use it as the centerpiece of her upcoming employee of the month talk, which they write for her and fill with techno-gibberish.⁴²⁸ Because of her lack of technical knowledge, she does not detect that anything is amiss and presents the talk exactly as Moss and Roy have scripted, including prominently displaying “The Internet” to her audience.⁴²⁹ As Moss and Roy sit in the back of the room hoping to revel in their cleverly orchestrated humiliation of their boss, their plans go horribly awry: the members of the audience—people apparently even more technologically-illiterate than their boss—believe every word of her techno-gibberish speech and chant enthusiastically, hoping for more of Jen’s pearls of technical wisdom.⁴³⁰

Thus, part of the security puzzle involves identifying the Jens of the world who overclaim their expertise; bad security decisions happen in part when people fail to recognize the limitations of their own knowledge and fail to defer to genuine expertise. Without recognizing the limitations of their own knowledge, they easily fall prey to the Mosses and Roys of the world, self-interested actors who inject disinformation. Indeed, a “cyberdabbler” problem has manifested in legal and policy circles in the last five years: a wave of policy and legal experts from other domains are seeking to rebrand themselves speedily

424. *Errata – Charlatans*, ATTRITION.ORG, <http://attrition.org/errata/charlatan/> (last visited Jan. 12, 2018).

425. Sheep is a term used to refer to compromised users and machines in security. See George Ou, *Wall of Sheep at DEFCON Illustrates What Not to Do*, ZDNET (Aug. 4, 2006, 9:35 AM), <http://www.zdnet.com/article/wall-of-sheep-at-defcon-illustrates-what-not-to-do/>.

426. See *The IT Crowd* (Channel 4 television broadcast).

427. See *The IT Crowd: The Speech* (Channel 4 television broadcast (Dec. 12, 2008)).

428. *Id.*

429. *Id.*

430. *Id.*

as “cyber” experts, mistakenly believing the field of information security policy to be something quickly learnable.⁴³¹ Understanding security, much like understanding law, requires years of tacit knowledge acquisition by learning from and engaging with technical security professionals on their turf and terms. Indeed, one leading security professional and former NSA employee⁴³² recently explained the problem as follows: “the law profession is not without its hubris and thinks that it can pretty much define anything. Sometimes they even try to redefine mathematical constants such as Pi.”⁴³³ He is not wrong. For example, one legal scholar has recently argued that security engineers and their long-standing, technically-rigorous definitions are part of the problem in security,⁴³⁴ arguing that “cybersecurity” definitions should be “socially-constructed” around “accuracy,” as such (new and vague⁴³⁵) term presumably would be defined by lawyers.⁴³⁶

First Amendment theorists would argue that the appropriate response to this type of legal hubris concern is conscious engagement with the principle of “epistemological humility.”⁴³⁷ As described by Professor Martin Redish, whose work most extensively references the

431. See Michail S, *Closing Plenary: Information Security Programs in Academia*, [SHMOOCON 2016], YOUTUBE (Feb. 5, 2016), <https://www.youtube.com/watch?v=rn0BdODPSbA>.

432. See *Dave Aitel*, RSA CONFERENCE, <https://www.rsaconference.com/speakers/dave-aitel> (last visited Jan. 12, 2018).

433. See Dave Aitel, *Why Oday is a Nebulous Concept, Part 1!*, CYBERSECPOLITICS (Feb. 16, 2016, 7:42 AM), <http://cybersecpolitics.blogspot.com/2016/02/why-oday-is-nebulous-concept-part-1.html>.

434. See Bambauer, *supra* note 180, at 827 (“Treating integrity as an inherent quality of the stored data has a long history, and engineers are reluctant to re-examine the concept.”).

435. As any transactional attorney will tell you, definitional precision and reliance on external technical standards is desirable; it creates greater certainty for all parties. Definitional vagueness or ambiguity, on the other hand, creates business risk. For example, companies participate in standard setting bodies for this reason, and contracts often specify that parties must be certified to comply with international standards. See, e.g., INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, <https://www.iso.org/home.html> (last visited Jan. 11, 2018).

436. See Bambauer, *supra* note 180, at 852–53 (“Informational accuracy is at the heart of cybersecurity . . . accuracy is an outcome of societal processes, into which data is an important but not singular input.”).

437. Martin H. Redish, *Product Health Claims and the First Amendment: Scientific Expression and the Twilight Zone of Commercial Speech*, 43 VAND. L. REV. 1433, 1435 (1990) (“[T]he ‘principle of epistemological humility’ . . . posits that whatever the currently prevailing beliefs may be, history teaches us that scientific or moral advances may at some future point make those beliefs appear either silly or monstrous.”).

concept,⁴³⁸ the “principle posits that whatever the currently prevailing beliefs may be, history teaches us that scientific or moral advances may at some future point make those beliefs appear either silly or monstrous.”⁴³⁹ Thus, argues Redish, “any attempt by the government to impose a national scientific orthodoxy could undermine or inhibit the advance of scientific knowledge, thus undermining a key value of the first amendment.”⁴⁴⁰

Discussions of epistemological humility and democracy permeate the First Amendment scholarship,⁴⁴¹ but references also exist outside of the First Amendment context. For example, Professor David Luban has referenced epistemological humility in the context of social responsibility of attorneys,⁴⁴² and Professor Rebecca Tushnet has used epistemological humility concerns in her work on fair use and copyright.⁴⁴³ However, to date, the law review literature has not injected epistemological humility into the information security debate—an injection long overdue.

In the context of information security, the principle of epistemological humility cautions us to create evolutionary legal frameworks deferential to technical expertise and the changing state of the art of security research. We should eschew imposing what Professor Redish has called “a national scientific orthodoxy”⁴⁴⁴ through law. Instead, we need policy and law with robust, formal input mechanisms from technical security experts, thereby avoiding the epistemological “sin” of legal hubris.

438. *See, e.g., id.*

439. *Id.*

440. *Id.*

441. *See, e.g.,* Andrew Koppelman, *Veil of Ignorance: Tunnel Constructivism in Free Speech Theory*, 107 NW. U. L. REV. 647, 677 (2013) (engaging with epistemological humility and stating that Redish claims that his rationale “does not represent a firmly held theory of moral epistemology so much as an instrumental construct designed to avoid totalitarianism” (internal quotation marks omitted)); Rebecca Tushnet, *Content, Purpose, or Both?*, 90 WASH. L. REV. 869, 890 (2015) (“The relatively new epistemological humility expressed in cases such as *Cariou* is a welcome respite from what Zahr Said has characterized as formalism in the mode of New Criticism, in which judges treat works as having only one correct meaning.”).

442. *See* David Luban, *The Social Responsibilities of Lawyers: A Green Perspective*, 63 GEO. WASH. L. REV. 955 (1995).

443. *See* Tushnet, *supra* note 441; Rebecca Tushnet, *Judges as Bad Reviewers: Fair Use and Epistemological Humility*, 25 L. & LIT. 20 (2013); Rebecca Tushnet, *Scary Monsters: Hybrids, Mashups, and Other Illegitimate Children*, 86 NOTRE DAME L. REV. 2133 (2011).

444. Redish, *supra* note 437, at 1435.

As such, the paradigm introduced in the next section strives for epistemological humility. It blends the insights of Polanyi with those of the Monty Hall problem, applying them to the jigsaw puzzle of reciprocal security vulnerability and offering a novel paradigm—the paradigm of *reciprocal security*.

IV. CYBERFRIENDSHIP IS MAGIC:⁴⁴⁵ RECIPROCAL SECURITY

In the iconic British television show *Doctor Who*,⁴⁴⁶ the protagonist, the Doctor,⁴⁴⁷ an alien⁴⁴⁸ Time Lord,⁴⁴⁹ travels across the space-time continuum⁴⁵⁰ inside a “police box”⁴⁵¹ called the TARDIS.⁴⁵² Externally, the TARDIS appears⁴⁵³ to be merely a typical blue UK police telephone box from the 1960s.⁴⁵⁴ Occasionally, the Doctor invites a new companion⁴⁵⁵ to travel with him. Upon entering, the companions quickly realize that the TARDIS is not really a police box at all.⁴⁵⁶ Rather, it is a complex⁴⁵⁷ living organism⁴⁵⁸ that simply looks like a police box externally as an act of operational security or

445. See *My Little Pony: Friendship is Magic*, KNOW YOUR MEME, <http://knowyourmeme.com/memes/subcultures/my-little-pony-friendship-is-magic> (last visited Jan. 12, 2018).

446. See *Doctor Who* (BBC television broadcast).

447. *Id.*

448. See *Doctor Who: Rose* (BBC television broadcast March 26, 2005) (“If you are an alien how come you sound like you’re from the North? The Doctor: Lots of planets have a North!”).

449. *Id.*

450. See, e.g., *The Tardis*, DOCTOR WHO SITE, <http://www.thedoctorwhosite.co.uk/tardis/> (last visited Jan. 12, 2018).

451. *Id.*

452. *Id.*

453. As such, it frequently triggers the curiosity of onlookers who scrutinize its exterior. See, e.g., *Doctor Who: An Unearthly Child: An Unearthly Child* (BBC One television broadcast Nov. 23, 1963).

454. See, e.g., *Tardis Exterior*, DOCTOR WHO SITE, <http://www.thedoctorwhosite.co.uk/tardis/exterior/> (last visited Jan. 12, 2018).

455. See, e.g., *The Doctor’s Companions*, BBC: DOCTOR WHO, <http://www.doctorwho.tv/50-years/companions/> (last visited Jan. 12, 2018).

456. See, e.g., *TARDIS Interior and Console Rooms*, DOCTOR WHO SITE, <http://www.thedoctorwhosite.co.uk/tardis/interior/> (last visited Jan. 12, 2018).

457. Its exterior is an inaccurate representation of its interior size. See, e.g., *DW Supercuts, Doctor Who Supercut*, YOUTUBE, <https://youtu.be/is-Gnyk4AWE> (last visited Jan. 12, 2018).

458. See, e.g., *Doctor Who Answers: Is the TARDIS Alive?*, FANDOM, http://doctorwho.answers.wikia.com/wiki/Is_the_TARDIS_alive (last visited Jan. 12, 2018).

“OPSEC.”⁴⁵⁹ Much like the TARDIS, the study of information security policy is deceptively simple from the outside, but, from an insider’s perspective, it is a sophisticated and evolving jigsaw puzzle. Any successful legal paradigm must account for and accommodate this evolving complexity. For this reason, building on Part III’s lessons from Polanyi, the Monty Hall problem, and the First Amendment theory principle of epistemological humility, this Part introduces a “reciprocal security” paradigm for the field of information security law and policy, the field that many lawyers and policymakers—for better or worse—currently call “cybersecurity law.”

A. Keep Calm and Cyber On:⁴⁶⁰ Shifting to Reciprocal Security

Former West Point professor Greg Conti recently explained to an audience at a security conference that the term “cybersecurity” has historically referred solely to the military concept of nations fighting nations through the internet, and everything else is more appropriately referenced as “information security” or “data security.”⁴⁶¹ This distinction has indeed historically seemed a logical one, and it reflects the general usage of security industry veterans like Conti.⁴⁶² However, in light of the technical reality of reciprocal security vulnerability, this section argues in favor of a new sector-neutral framing for security—the paradigm of reciprocal security.

The reciprocal security paradigm’s explicitly sector-neutral approach represents a key theoretical shift. Government information security is, as a matter of technology, essentially parallel to that of private sector organizations. Government entities are organizations with employees, assets, missions, and points of information vulnerability, as are private sector entities. Indeed, as the problem of reciprocal security vulnerability detailed in Part II highlights, because of the technological interdependence of both sectors,⁴⁶³ it becomes functionally impossible to cabin off the vulnerabilities of the government and private sector from each other.

459. See, e.g., *OPSEC Awareness for Military Members, DoD Employees and Contractors*, CDSE, <https://securityawareness.usalearning.gov/opsec/> (last visited Jan. 12, 2018).

460. *Keep Calm and Carry On*, KNOW YOUR MEME, <http://knowyourmeme.com/memes/keep-calm-and-carry-on> (last visited Jan. 12, 2018).

461. Michail S, *supra* note 324, at 13:30.

462. *Id.*

463. See *supra* Section II.A.1.

Therefore, the reciprocal security paradigm replaces the two dominant security paradigms currently in use—information sharing and deterrence—with a single sector-neutral, innovation-sensitive paradigm composed of two interrelated components: first, the construction of a security vigilance infrastructure and, second, the concept of defense-primacy from an attacker perspective.

1. The cyberbox is bigger on the inside.⁴⁶⁴ Building a security vigilance infrastructure

The Doctor: *Well, Sergeant? Aren't you going to say, "It's bigger on the inside than it is on the outside"? Everybody else does.*

Sgt. Benton: *Well, it's . . . pretty obvious, isn't it?*⁴⁶⁵

Knowledge creation and innovation in security progress through the independent but cooperative scientific and engineering efforts of a community of technical experts—security researchers. But therein lies the innovation policy challenge of information security: any successful legal structures in information security must be flexible enough to allow for evolution of technical solutions, but yet be structured enough to create a framework capable of preserving citizen trust. Simply collecting and sharing uncoordinated information without a sense of its place in the bigger picture, warns Polanyi, will not assemble the puzzle correctly.

Professor Brett Frischmann has argued that two types of infrastructure exist—traditional⁴⁶⁶ and non-traditional.⁴⁶⁷ Non-traditional infrastructure commons, he argues, incorporate what he

464. *Doctor Who - The Augmented Reality Tardis: It's Bigger on the Inside*, KNOW YOUR MEME, <http://knowyourmeme.com/videos/56515-doctor-who> (last visited Jan. 12, 2018).

465. *Doctor Who: The Three Doctors: Episode One* (BBC One television broadcast Dec. 30, 1972).

466. See generally Brett M. Frischmann, *Infrastructure Commons*, 2005 MICH. ST. L. REV. 121 (2005).

467. *Id.* at 124 (explaining that examples of non-traditional infrastructure include “environmental and information resources, such as lakes and ideas . . . [that] generate (or have the potential to generate) significant positive externalities that result in large social gains”).

calls “public infrastructure.”⁴⁶⁸ Public infrastructure for Frischmann includes ideas and information, such as basic research, when they meet three criteria: they can be consumed nonrivalrously, social demand is driven by downstream producers that require the resource as an input, and the range of goods produced downstream using these inputs varies across producers. He argues that public infrastructure requires additional government support “because of the inability of the market to process demand information for these goods.”⁴⁶⁹ This insight can be applied to meaningfully advance the conversation in security. The information structures needed for scaling security vulnerability information may fall within Professor Frischmann’s definition of information qualifying as public infrastructure.⁴⁷⁰ Indeed, it is precisely the absence of robust, scalable public infrastructure in security information that frustrates the efficacy of currently existing security information sharing initiatives.

Creating a security vigilance infrastructure requires us to carefully examine whether shared baselines of understanding and conduct exist in the ways that we discover, report, disclose, and react to the steady flow of changing information security threats across both the public and private sector. Currently, this type of information infrastructure exists to some extent in the security research community, but it suffers from inconsistencies in practice, high levels of informality and interpersonal relationship reliance, resource deficits, and an almost total absence of legal structures of enforcement.

For example, we currently lack adequately uniform, scalable structures for third-party security audit requirements,⁴⁷¹ vulnerability

468. *Id.* at 129.

469. *Id.* at 130.

470. *See id.*

471. A rigorous security audit would verify the handling of security vulnerabilities in line with the best practices of the information security industry at the time. For a discussion of current best practices in information security, see, for example, *CIS Controls*, CIS, <https://www.cisecurity.org/critical-controls.cfm> (last visited Jan. 12, 2018).

assessment,⁴⁷² indexing,⁴⁷³ and scoring⁴⁷⁴ in either the private or public sector. The existing vulnerability indexing structures, such as the Common Vulnerabilities and Exposures (CVE) system run by the MITRE Corporation,⁴⁷⁵ are struggling with the increased volume of vulnerabilities.⁴⁷⁶ Meanwhile, voluntary reporting structures, such as self-released security advisories, regularly suffer from inaccuracies and dramatic format variation to the point of sometimes rendering these disclosure documents incomparable in the opinions of vulnerability-indexing experts.⁴⁷⁷ We currently lack adequate consistency and uniformity across our security information flows to be able to harness them effectively to advance the state of security knowledge. Meaningful information sharing cannot exist without correcting and rebuilding the information infrastructure that frames current information sharing. Thus, each of the dominant information security information flows should be mapped and connected to each other, identifying and filling in information gaps to create a self-reinforcing web of good security behaviors and scalable information disclosure.⁴⁷⁸

In addition to these shortfalls regarding information silos and scalability, traditional paradigms of information sharing have created structures in which organizations share some information only after security failures *have already occurred*. While this is useful, a superior approach is one that is also predictive—one that, as Polanyi might say, facilitates comprehension of the big puzzle of security with subsidiary awareness. In other words, to whatever extent some deterrence of

472. For a discussion of vulnerability assessment see, for example, *Critical Infrastructure Vulnerability Assessments*, U.S. DEPT OF HOMELAND SECURITY, <https://www.dhs.gov/critical-infrastructure-vulnerability-assessments> (last updated Apr. 17, 2017).

473. For a discussion of vulnerability indexing, see, for example, *CVE List Home*, CVE, <https://cve.mitre.org/cve/> (last visited Jan. 12, 2018). *But see* Steve Ragan, *Over 6,000 Vulnerabilities Went Unassigned by MITRE's CVE Project in 2015*, CSO (Sept. 22, 2016, 4:00 AM), <http://www.csoonline.com/article/3122460/technology-business/over-6000-vulnerabilities-went-unassigned-by-mitres-cve-project-in-2015.html>.

474. For a discussion of vulnerability scoring, see, for example, *Vulnerability Metrics*, NATIONAL VULNERABILITY DATABASE, <https://nvd.nist.gov/cvss.cfm> (last visited Jan. 12, 2018). *But see, e.g.*, CARSTEN EIRAM & BRIAN MARTIN, *THE CVSSv2 SHORTCOMINGS, FAULTS, AND FAILURES FORMULATION*, <https://www.riskbasedsecurity.com/reports/CVSS-ShortcomingsFaultsandFailures.pdf> (last visited Jan. 12, 2018).

475. *See, e.g.*, *CVE List Home*, *supra* note 473. *But see* Ragan, *supra* note 473.

476. *See* Ragan, *supra* note 473.

477. *See supra* note 474.

478. *See infra* Part IV.

security criminality may be possible, it requires us to correctly predict the next generation of attacks *before* they occur. For this reason, the second element of the reciprocal security paradigm shifts the current dynamic away from an explicit deterrence focus toward the more anticipatory posture of defense primacy.

2. *More cybercowbell*:⁴⁷⁹ *Defense primacy*

This is one of the safest planets I know, there is never anything dangerous here!

—The Doctor

There are some sentences I should just keep away from.

—The Doctor (after discovering the planet is about to be covered in acid rain)⁴⁸⁰

A series of compromises in December 2009 offers yet another stark example of the problem of reciprocal security vulnerability. Almost a decade ago, Google and approximately twenty other Silicon Valley companies suffered a sophisticated and intense attack that they believe to have been carried out by the Chinese government.⁴⁸¹ According to press accounts, the attackers were apparently looking for information on court orders and other information indicating whether U.S. law enforcement knew the identities of Chinese intelligence operatives.⁴⁸² But Google also disclosed that the attackers had stolen intellectual property and targeted accounts of human rights activists perceived by China to oppose its government.⁴⁸³

This 2009 attack also demonstrates why some categories of threats are unlikely to fit within traditional deterrence paradigms.⁴⁸⁴ Highly

479. *Needs More Cowbell*, KNOW YOUR MEME, <http://knowyourmeme.com/memes/needs-more-cowbell> (last visited Jan. 12, 2018).

480. *Doctor Who: The Doctor: The Widow, and The Wardrobe* (BBC One television broadcast Dec. 25, 2011).

481. See Nakashima, *supra* note 60; Zetter, *supra* note 60.

482. In particular, it appears the attackers were looking for evidence of court orders gaining access to Gmail accounts. See Nakashima, *supra* note 60.

483. David Drummond, *Statement from Google: A New Approach to China*, WASH. POST (Jan. 12, 2010; 6:09 PM), <http://www.washingtonpost.com/wp-dyn/content/article/2010/01/12/AR2010011202903.html>.

484. For a discussion of deterrence paradigms, see *supra* text accompanying notes 140–76.

motivated adversaries will rarely be deterred. In the wake of the attack, Silicon Valley companies recommitted themselves to forward-looking security initiatives and working harder to anticipate vulnerabilities⁴⁸⁵ and attacks.⁴⁸⁶ Indeed, the success of bug bounty programs⁴⁸⁷ such as Google's Chrome Rewards⁴⁸⁸ and the Department of Defense's Hack the Army⁴⁸⁹ and Hack the Pentagon⁴⁹⁰ demonstrate that forward-looking public and private sector organizations are adopting a more market-driven,⁴⁹¹ defense-oriented model⁴⁹² with success.

Instead of deterrence alone, the second prong of the reciprocal security paradigm focuses on defense primacy. Defense primacy hinges on anticipating and preventing successful attacks to the greatest extent possible. It means taking a strategic long-term view of both public and private sector security in a forward-looking manner. In other words, it involves making sure that the puzzle pieces of security fit together.

485. For example, Google operates a robust bug bounty program. *See, e.g.*, Jonathan Keane, *Google Will Pay You \$100K If You Can Pull off the Ultimate Chrome Hack*, DIGITAL TRENDS (Mar. 15, 2016, 4:11 PM), <http://www.digitaltrends.com/computing/google-chrome-bug-bounty-raise/#ixzz4aNsZpYfk>.

486. Google's Chaos team is one example of this type of strategic preventative planning. *See* Julie Bort, *Meet Kripa Krishnan, Google's Queen of Chaos*, BUS. INSIDER (Aug. 6, 2016, 10:01 AM), <http://www.businessinsider.com/profile-of-google-disaster-recovery-testing-boss-kripa-krishnan-2016-8>.

487. For a discussion of the benefits and challenges of bug bounty programs, *see*, for example, *A Federal 'Bug Bounty' Program? HackerOne's Katie Moussouris Weighs in on the Challenges*, CYBERSCOOP, <https://www.cyberscoop.com/radio/a-federal-bug-bounty-program-hackerones-katie-moussouris-weighs-in-on-the-challenges/> (last visited Jan. 12, 2018).

488. *Chrome Reward Program Rules*, GOOGLE, <https://www.google.com/about/appsecurity/chrome-rewards/index.html> (last visited Jan. 12, 2018).

489. *See, e.g.*, Christopher Ophardt, *Army Secretary Issues Challenge with 'Hack the Army' Program*, U. S. ARMY (Nov. 21, 2016), <https://www.army.mil/article/178473>.

490. *See, e.g.* Lisa Ferdinando, *Carter Announces 'Hack the Pentagon' Program Results*, U.S. DEP'T OF DEF. (June 17, 2016), <https://www.defense.gov/News/Article/Article/802828/carter-announces-hack-the-pentagon-program-results>.

491. Some scholars have advocated formalizing these markets. Professor Jay Kesan and a coauthor recently proposed the formulation of vulnerability markets modeled on the commodity futures exchanges. *See* Jay P. Kesan & Carol M. Hayes, *Bugs in the Market: Creating A Legitimate, Transparent, and Vendor-Focused Market for Software Vulnerabilities*, 58 ARIZ. L. REV. 753, 754 (2016) (proposing "a revolutionary market for vulnerabilities aimed at facilitating legitimate, transparent, and vendor-focused transactions of critical security information at a fair market price").

492. As recently noted by Abigail Slater, the General Counsel of the Internet Association, the "ROI on bug bounty programs is phenomenal." For comments of Abigail Slater at CyConUS 2016, *see* Army Cyber Institute, *Bug Bounty*, at 35:52, YOUTUBE (Dec. 20, 2016), <https://www.youtube.com/watch?v=acWWT2R3LiI&index=15&list=PLtUuPz3a0Gz-PJOFb55O6jDZ68Ya9O9eS>.

Unlike deterrence, defense primacy shifts enforcement priorities in a preventative direction by placing the focus on legally nudging organizations to implement security governance processes and *become less attractive targets before attacks occur*. In lieu of the Sisyphean task of deterring (sometimes undeterrable) attackers,⁴⁹³ defense primacy fosters a sense of shared legal and ethical responsibility for the security of our economy and country. It explicitly considers the problem of reciprocal security vulnerability and focuses on starting with addressing what we know to be effective in meaningfully improving security: fixing already-known security problems.

Defense primacy involves not merely investigating and prosecuting computer intrusion offenders after intrusions have already occurred, it also involves enforcement activity and sanction of both public⁴⁹⁴ and private sector entities whose security governance inadequacies are obviously ripe for exploitation by attackers—in other words, intervening before an attack occurs, not merely after. Legal requirements to fix known security deficits are currently few.⁴⁹⁵ Particularly in industries driven by a “legal compliance”⁴⁹⁶ mindset, the lack of many legal nudges to be proactive about security risk means that incentives for security improvements are perceived to be low.⁴⁹⁷

493. See *supra* Part II.

494. The quality of internal operations security of some governmental organizations is also still unacceptably low, despite a continuing onslaught of security compromises. See GOV'T ACCOUNTABILITY OFFICE, INFORMATION SECURITY: AGENCIES NEED TO IMPROVE CONTROLS OVER SELECTED HIGH-IMPACT SYSTEMS (2016), <https://www.gao.gov/assets/680/677293.pdf>.

495. Apart from requirements of truthful descriptions of security practices in connection with the Children's Online Privacy Protection Act, Gramm-Leach-Bliley Act, and Health Insurance Portability and Accountability Act, to the extent a requirement to “fix” broken code currently exists in law, it arises primarily from sector-specific concerns—desire to avoid FTC enforcement actions for companies subject to FTC jurisdiction, and for medical device companies out of the new FDA postmarket guidance. *But see* Andrea M. Matwyshyn, *Hidden Engines of Destruction: The Reasonable Expectation of Code Safety and the Duty to Warn in Digital Products*, 62 FLA. L. REV. 109, 110 (2010) (proposing a “reasonable expectation of code safety,” along with a three-tiered framework inspired by systems theory and the land-based duty to warn, protect and repair).

496. See, e.g., Jonathan Sander, *Cyber security: How a Compliance Mindset can Prove Dangerous*, ECONOMIST (Aug. 2, 2016), <https://perspectives.eiu.com/technology-innovation/cyber-security-how-compliance-mindset-can-prove-dangerous>.

497. For a discussion of incentives and security, see, for example, Bruce H. Kobayashi, *Private Versus Social Incentives in Cybersecurity: Law and Economics*, in THE LAW AND ECONOMICS OF CYBERSECURITY 13 (Mark F. Grady & Francesco Parisi eds., 2005) (discussing cybersecurity information as a public good).

A shift in thinking and legal priorities is needed. The reciprocal security paradigm's shift toward defense primacy better allows Polanyi's metaphorical puzzle pieces to come together in security. It is characterized by an adversarial mindset and an eye on the bigger, scalable picture. Now, let us briefly explore a series of concrete legal and policy initiatives arising from the reciprocal security paradigm.

B. Cyberchallenge Accepted:⁴⁹⁸ Applying Reciprocal Security

*[People] love to say "We've always done it this way." . . .
That's why I have a clock on my wall that runs
counter-clockwise.⁴⁹⁹*

—Professor⁵⁰⁰/Rear Adm.⁵⁰¹ Grace Hopper⁵⁰²

This section applies the reciprocal security paradigm with a series of specific legislative, regulatory, and technical proposals. They are presented in two groups, mirroring the two prongs of the reciprocal security paradigm—security vigilance infrastructure and defense primacy. They explicitly blend the public and private sector dynamics of security to begin to address the problem of reciprocal security vulnerability.

498. *Challenge Accepted*, KNOW YOUR MEME, <http://knowyourmeme.com/memes/challenge-accepted> (last visited Jan. 12, 2018).

499. Dr. Grace Hopper famously quipped “Humans are allergic to change. They love to say, ‘We’ve always done it this way.’ I try to fight that. That’s why I have a clock on my wall that runs counter-clockwise.” Philip Schieber, *The Wit and Wisdom of Grace Hopper*, OCLC NEWSLETTER, no. 167, Mar./Apr. 1987, at 9.

500. For a discussion of Dr. Grace Hopper’s career as a professor, see *Grace Murray Hopper*, GRACE HOPPER CELEBRATION OF WOMEN IN COMPUTING CONFERENCE (1994).

501. For a discussion of Dr. Grace Hopper’s career as a naval officer, see *id.*

502. Dr. Grace Hopper was a pioneer of computer science and the “mother of software.” She was posthumously awarded the presidential Medal of Freedom in 2016. See April Grant, *Computer Science Legend, Rear Adm. Grace Hopper, Posthumously Receives Presidential Medal of Freedom*, NAVY (Nov. 22, 2016, 4:32 PM), http://www.navy.mil/submit/display.asp?story_id=97807.

*1. That cyberescalated quickly:*⁵⁰³ *Creating security vigilance infrastructure*

The first prong of the reciprocal security paradigm involves the creation of security vigilance infrastructures. A first cut at improving these structures should focus on the legal creation of robust, formalized feedback loops engaging technical experts.

a. Proposal 1: Create new formal federal government security feedback loops. In the legislative branch, Congress can begin to address the problem of reciprocal security vulnerability with three changes. First, Congress should amend the Technology Assessment Act to create a new Congressional Office of Information Technology Assessment (OITA) to assist policymakers and the public in understanding technical questions of information technology. In 1972 the Technology Assessment Act⁵⁰⁴ established the Congressional Office of Technology Assessment (OTA)⁵⁰⁵ with the goal of creating a feedback loop of bi-partisan⁵⁰⁶ technology expertise to inform lawmaking.⁵⁰⁷ OTA was defunded in 1995,⁵⁰⁸ but changed security circumstances now warrant reconsideration of this appropriations decision. A bi-partisan, in-house office of technology experts would assist Congress with new security challenges. This new OITA would maintain a bi-partisan advisory mission but would be limited in scope to matters of information technology policy, particularly advising on the technical aspects of information security. It would also include an advisory council with technical experts from the private sector.

503. See, e.g., *That Escalated Quickly*, KNOW YOUR MEME, <http://knowyourmeme.com/memes/that-escalated-quickly> (last visited Jan. 12, 2018).

504. Office of Technology Assessment Act, Pub. L. No. 92-484, 86 Stat. 797 (1972).

505. The Technology Assessment Act states in relevant part “The basic function of the Office shall be to provide early indications of the probable beneficial and adverse impacts of the applications of technology and to develop other coordinate information which may assist the Congress.” *Id.* § 3(c).

506. OTA was overseen by the “Technology Assessment Board” of 13 members: a non-voting director, six senators (three from each of the minority and majority party), and six representatives (three from each party). *Id.* § 4.

507. See *infra* note 533.

508. See, e.g., Celia Wexler, *Bring Back the Office of Technology Assessment*, NY TIMES (May 28, 2015, 6:45 AM), <http://www.nytimes.com/roomfordebate/2015/05/28/scientists-curbing-the-ethical-use-of-science/bring-back-the-office-of-technology-assessment>.

Second, Congress should follow the suggestion of the Copyright Office⁵⁰⁹ and amend the DMCA to make permanent the security research exemption granted during the 2015 triennial review of section 1201. As explained in Section II.B.2, the DMCA has historically chilled a portion of security research that benefits the safety of both the public and private sector.⁵¹⁰ With the approval of a broad DMCA security research exemption in 2015 covering research on all products purchased by a consumer,⁵¹¹ the security research climate has materially improved.⁵¹² However, the current exemption requires regular renewal. Amending the DMCA to make the exemption permanent benefits both the public and private sector without altering any of the numerous other legal remedies copyright holders have at their disposal,⁵¹³ as the Copyright Office explained. Congress should similarly update the CFAA to resolve confusion around its key terms in order to provide as much clarity as possible for security researchers.⁵¹⁴

Finally, Congress should instruct the Government Accountability Office to create an information security whistleblower “hotline” with a security ombudsman available to all government employees and government contractors. Some of the largest governmental breaches have occurred because employees and, in particular, private sector government contractors believed that their chain of command failed

509. U.S. COPYRIGHT OFF., SECTION 1201 OF TITLE 17, at 74 (2017), <https://www.copyright.gov/policy/1201/section-1201-full-report.pdf>

510. *See, e.g.*, Security Researchers filing (recounting various instances of security research that has not been performed on advice of counsel or performed only because of intervention and direct request from a Secretary of State and stating that “[a]ttorneys regularly counsel . . . that the DMCA is an unclear statute and that undertaking any such research exposes the researcher to legal risk. As such, attorneys usually counsel against continuing the research.”). BELLOVIN, *supra* note 237.

511. *See supra* text accompanying notes 245–52.

512. The exemption has already facilitated secondary analysis and critique by the press to arise regarding security of consumer products. *See, e.g.*, *Security Software Buying Guide*, CONSUMER REPORTS, <http://www.consumerreports.org/cro/security-software/buying-guide.htm> (last updated Nov. 2017).

513. *Id.*

514. For a proposal regarding reframing the CFAA around definitions from information security and eliminating the term “authorized access” see Andrea M. Matwyshyn and Stephanie K. Pell, *Broken* (Nov. 17, 2017) (draft on file with author).

to take their security concerns seriously.⁵¹⁵ Through setting up a Congressional whistleblower hotline as an official feedback loop, a portion of insider security compromises may be avoided.

In the executive branch, the White House should expand future membership of the National Science and Technology Council (NSTC) in the White House Office of Science and Technology Policy (OSTP) to include all agencies and organizations directly engaged with information security enforcement. Consumer protection agencies directly involved with security enforcement, in particular the FTC, SEC, FCC, and FDA, have historically been absent from OSTP's NSTC.⁵¹⁶ As such, this absence means that private sector innovation, competition, and consumer protection concerns are comparatively underrepresented in OSTP consultations on security policymaking.

Similarly, the White House should encourage the creation of a visiting technologist and scholar in residence program at every major agency (and ask Congress to appropriate funding accordingly). This private sector feedback loop has already been successfully launched at the FTC⁵¹⁷ and other agencies.⁵¹⁸ Fixed-term private sector technical and legal experts can nudge security policymaking inside agencies in ways that career employees and political appointees cannot, and formalized exchanges of this nature facilitate tacit security knowledge exchange in both directions.⁵¹⁹

The White House should also execute an executive order requiring that all government organizations comply with the principles embodied in ISO standards on security, in particular the principles reflected in ISO 30111⁵²⁰ and 29147.⁵²¹ These ISOs set forth baselines

515. Jason Leopold, Marcy Wheeler & Ky Henderson, *Exclusive: Snowden Tried to Tell NSA About his Concerns*, VICE (June 4, 2016), <https://news.vice.com/story/exclusive-snowden-tried-to-tell-nsa-about-his-concerns>.

516. These agencies were not included in NSTC under the Obama administration. See *NSTC Members*, WHITE HOUSE <https://obamawhitehouse.archives.gov/administration/eop/ostp/nstc/about/members>.

517. See, e.g., Steve Dent, *Meet the FTC's New Chief Technologist*, ENGADGET (Dec. 4, 2015), <https://www.engadget.com/2015/12/04/lorrie-cranor-ftc-chief-technologist/>.

518. See, e.g., *Technologist in Residence Program*, ENERGY.GOV, <http://energy.gov/eere/cemi/technologist-residence-program> (last visited Jan. 12, 2018).

519. For a discussion of tacit knowledge, see *supra* Section III.A.2.

520. *ISO/IEC 30111:2013*, ISO, <https://www.iso.org/standard/53231.html> (last visited Jan. 12, 2018).

521. *ISO/IEC 29147:2014*, ISO, <https://www.iso.org/standard/45170.html> (last visited Jan. 12, 2018).

of practice in the private sector with respect to organizational structure and processes in responding to security vulnerabilities. The principles embodied by these two standards make sense as governance baselines for organizations in the public sector as well.⁵²² In this way, the standards of security in the private and public sector will be nudged to converge and evolve in tandem.

Finally, the Department of Justice should take affirmative steps to protect technical private sector feedback through security research, particularly because Congress has not yet directly addressed the confusion surrounding the CFAA.⁵²³ First, DOJ should centralize CFAA indictment review, approval, and staffing in the Computer Crime and Intellectual Property Section (CCIPS) at Main Justice. Because of the importance of encouraging security research, CFAA indictments should not be within the exclusive or even predominant control of local US attorneys. Local US attorneys are more likely to lack an understanding of the bigger picture of security,⁵²⁴ a picture better understood by CCIPS attorneys.⁵²⁵ Second, DOJ could create a CFAA feedback structure by borrowing its own model from numerous other effective feedback loop structures—antitrust enforcement policy statements,⁵²⁶ Foreign Corrupt Practices Act

522. Meanwhile, the courts are likely to begin to incorporate these baselines of conduct into tort determinations of liability, creating a harmonized approach across both the public and private sector.

523. For a discussion of the circuit splits currently plaguing interpretation of the CFAA, see, for example, Matwyshyn, *supra* note 281.

524. The prosecution of Aaron Swartz raised questions for many observers regarding the appropriate balance between prosecutorial discretion and centralization of CFAA prosecutions. See, e.g., Justin Peters, *A Year After Aaron Swartz's Death, Our Terrible Computer Crime Laws Remain Unchanged*, SLATE (Jan. 13, 2014), http://www.slate.com/blogs/crime/2014/01/13/aaron_swartz_cfaa_a_year_after_aaron_swartz_s_death_the_computer_fraud_and.html. The recent indictment of Marcus Hutchins, a security researcher who stopped the WannaCry ransomware, by a Wisconsin US Attorney has again raised questions regarding the desirability of local prosecutors having control over CFAA prosecutions. Taylor Hatmaker, *FBI Arrests WannaCry Hero for Alleged Role in Kronos Banking Malware*, TECHCRUNCH (Aug. 3, 2017), <https://techcrunch.com/2017/08/03/marcus-hutchins-malwaretechblog-arrest-fbi/>.

525. See, e.g., OFFICE OF THE ATT'Y GEN., MEMORANDUM TO THE UNITED STATES ATTORNEYS AND ASSISTANT ATT'Y GENERALS FOR THE CRIMINAL AND NATIONAL SECURITY DIVISIONS 6 (2014), <https://www.justice.gov/criminal-ccips/file/904941/download>.

526. See, e.g., U.S. DEP'T OF JUSTICE & FED. TRADE COMM'N, STATEMENTS OF ANTITRUST ENFORCEMENT POLICY IN HEALTH CARE (1996), <https://www.justice.gov/sites/default/files/atr/legacy/2007/08/15/1791.pdf> [hereinafter STATEMENTS OF ANTITRUST ENFORCEMENT POLICY]; U.S. DEP'T OF JUSTICE & FED. TRADE COMM'N, STATEMENT OF ANTITRUST ENFORCEMENT POLICY REGARDING ACCOUNTABLE CARE ORGANIZATIONS

guidance,⁵²⁷ advisory statements,⁵²⁸ opinion procedure releases,⁵²⁹ resource manuals,⁵³⁰ investigation closure statements⁵³¹ or even the notice filing regime from its antitrust leniency program.⁵³² Any of these existing DOJ feedback models would offer improved certainty for security researchers on DOJ's interpretations of the CFAA as such positions evolve.⁵³³

In the judicial branch, the Federal Judicial Center (FJC) should create a roster of trusted technical experts on information security as a technical feedback loop to assist judges, and, in collaboration with these experts, FJC should create a curriculum on information security. Similarly, the Administrative Office of the U.S. courts should use redundancy as a security measure for PACER filings by permitting universities, libraries, and other approved parties to maintain backup archives of PACER at their own expense. This step would also assist in providing more cost-effective access to indictments, cases, and other filings that are essential to attorneys both inside and outside the government. Because of the speed of legal evolution in information security, cost-effective access to legal filings is essential for both the public and private sector. In particular, computer intrusion indictments and pleadings are not readily available for review by computer science students and faculty in an affordable manner.

PARTICIPATING IN THE MEDICARE SHARED SAVINGS PROGRAM (2011), <https://www.justice.gov/sites/default/files/atr/legacy/2011/10/20/276458.pdf>.

527. See, e.g., Eric W. Sitarchuck & Alison Tanchyk, *Department of Justice Quietly Revises Foreign Corrupt Practices Act Resource Guide*, NAT'L L. REV. (Aug. 5, 2015), <http://www.natlawreview.com/article/departments-justice-quietly-revises-foreign-corrupt-practices-act-resource-guide>.

528. See, e.g., STATEMENTS OF ANTITRUST ENFORCEMENT POLICY, *supra* note 526.

529. See *Opinion Procedure Releases*, U.S. DEP'T OF JUSTICE, <https://www.justice.gov/criminal-fraud/opinion-procedure-releases> (last visited Jan. 12, 2018).

530. See Sitarchuck, *supra* note 527.

531. Press Release, U.S. Dep't of Justice, Statement of the Department of Justice's Antitrust Division on Its Decision to Close Its Investigation of Highmark's Affiliation Agreement with West Penn Allegheny Health System (Apr. 10, 2012), <https://www.justice.gov/opa/pr/statement-department-justice-s-antitrust-division-its-decision-close-its-investigation>.

532. See U.S. DEP'T OF JUSTICE, FREQUENTLY ASKED QUESTIONS ABOUT THE ANTITRUST DIVISION'S LENIENCY PROGRAM AND MODEL LENIENCY LETTERS (updated 2017), <https://www.justice.gov/atr/frequently-asked-questions-regarding-antitrust-divisions-leniency-program>.

533. Antitrust law and securities regulation present two somewhat parallel examples of regimes with broad statutes creating both civil and criminal recourse for aggrieved parties.

Pacer⁵³⁴ rates⁵³⁵ are currently cost-prohibitive for students and faculty, who, as a consequence, have (undesirably) resorted to hit-or-miss self-help remedies to gain access to legal information.⁵³⁶

b. Proposal 2: Improve security disclosure infrastructures across both the public and private sector to allow for meaningful progress tracking. At least three sets of disclosure structures should be buttressed in order to build another key component of a security vigilance infrastructure—updating the CVE system to scale effectively and address new technologies such as IoT, creating a uniform security advisory notice and repository structure, and offering a uniform data breach notification form and central data breach notification repository.

Security vulnerabilities are currently indexed by MITRE through the CVE system.⁵³⁷ However, MITRE is struggling to keep up with the volume of vulnerabilities generated by IoT.⁵³⁸ An updated structure is needed to allow for vulnerability indexing to adequately scale. Similarly, the current structures of vulnerability indexing are completely opaque to consumers. In collaboration with consumer protection agencies, a consumer-usable version of vulnerability information should be created to allow consumers to monitor their home devices for vulnerabilities and learn to ask security questions at time of purchase or new products.

Prudent companies seek to preserve customer goodwill and reputation by issuing timely security advisories—software safety notices—when vulnerabilities are discovered in their code.⁵³⁹ However, these advisories vary substantially in quality, accuracy, and

534. See PACER, <https://www.pacer.gov> (last visited Jan. 12, 2018). Meanwhile, private legal databases often lack complete indictment information. See, e.g., *Selected Criminal Law Database*, WESTLAW, <https://lawschool.westlaw.com/marketing/display/RE/82> (last visited Jan. 12, 2018) (containing “selected” criminal law materials).

535. See PACER, ELECTRONIC ACCESS FEE SCHEDULE (2013), https://www.pacer.gov/documents/epa_feesched.pdf.

536. See, e.g., *RECAP Project – Turning PACER Around*, FREE LAW PROJECT, <https://free.law/recap/> (last visited Jan. 12, 2018).

537. See, e.g., *CVE List Home*, *supra* note 473. *But see* Ragan, *supra* note 473.

538. *Id.*

539. Security advisories may also be triggered by vulnerabilities in libraries or other incorporated code used in a product’s code base.

timeliness.⁵⁴⁰ State attorneys general, directly or with the help of the National Conference of Commissioners on Uniform State Law (NCCUSL), and representatives of vulnerability database providers should work together to create a suggested uniform security advisory disclosure form and a centralized repository.⁵⁴¹ Provided that such a form is widely adopted, meaningful analysis of vulnerability information and trends would be dramatically improved and facilitated. Fraudulent, misleading, or grossly negligent information on these uniform advisories can, in turn, provide subsequent basis for suit or enforcement activity.

Data breach compliance personnel in industry consistently voice frustrations regarding two elements of state data breach notification requirements—variation across required formats for disclosure and variation in the correct point of state-level regulator notification.⁵⁴² Just as standardization happened in securities regulation with respect to the format of most blue sky filings,⁵⁴³ so too a standardized format can be drafted by NCCUSL⁵⁴⁴ or a coalition of state attorneys general to generate a suggested default data breach notification form. Provided the form is adequately robust,⁵⁴⁵ states could agree to accept this form in lieu of their current statutory disclosure requirements. Then, any one of these states could create a digital repository of all such forms, allowing citizens to search for information about the frequency of data breaches at particular companies. Federal agencies that suffer data breaches should lead by example by using the model

540. STEVE CHRISTEY & BRIAN MARTIN, BUYING INTO THE BIAS: WHY VULNERABILITY STATISTICS SUCK, <https://media.blackhat.com/us-13/US-13-Martin-Buying-Into-The-Bias-Why-Vulnerability-Statistics-Suck-Slides.pdf>.

541. See *Hearing Before the Subcomm. on Commerce, Mfg., and Trade, of the H. Comm. on Energy and Commerce*, U.S. HOUSE OF REPRESENTATIVES, 113th Cong. (2013) (statement of Dr. Andrea M. Matwyshyn), <http://docs.house.gov/meetings/IF/IF17/20130718/101152/HHRG-113-IF17-Wstate-MatwyshynA-20130718.pdf>.

542. *Id.*

543. Blue sky laws and their corresponding disclosure filings are the patchwork of state level securities regulation. For a discussion of blue sky laws see generally, Charles G. Stinner, *Estoppel and In Pari Delicto Defenses to Civil Blue Sky Law Actions*, 73 CORNELL L. REV. 448 (1988).

544. See, e.g., UNIFORM LAW COMMISSION, <http://www.uniformlaws.org/> (last visited Jan. 12, 2018).

545. For details of what this form might look like, see *Cyber Harder*, the companion essay to this article, *supra* note 29.

form and making their data breach notification disclosures available on their own websites.

2. *All Your Cyber Are Belong to Us*.⁵⁴⁶ *Defense primacy*

Having introduced the proposals aimed at building a security vigilance infrastructure, let us now turn to three proposals that aim to bolster defense primacy. These proposals involve defending supply chains, defending entrepreneurship, and defending market integrity. They each similarly mitigate the problem of reciprocal security vulnerability.

a. *Proposal 3: Defending supply chains to improve integrity.* Persistent vulnerability in both the public and private sector sometimes arises because organizations fail to keep track of the software products they use (and the components and code libraries included in those products).⁵⁴⁷ Consequently, they fail to adequately monitor a portion of the security vulnerabilities that directly impact them.⁵⁴⁸ Federal and state governments—as well as private sector entities—should conduct an annual (or more frequent) internal organization assessment of supply chain vulnerability and security integrity for all products purchased by the organization.⁵⁴⁹ Vendors that fail to patch vulnerabilities on a timely basis should be deemed in material breach of agreements and blacklisted from procurement vendor lists. Because of the purchasing power of the U.S. government and public companies in particular, this approach, which combines better vulnerability assessments and blacklists, would trigger significant security improvements in supply chain integrity in both the public and private sectors expeditiously.⁵⁵⁰

546. See, e.g., *All Your Base Are Belong to Us*, KNOW YOUR MEME, <http://knowyourmeme.com/memes/all-your-base-are-belong-to-us> (last visited Jan. 12, 2018).

547. See Andrea M. Matwyshyn, *The Big Security Mistakes Companies Make When Buying Tech*, WALL ST. J. (Mar. 13, 2017, 7:38 AM), <https://www.wsj.com/articles/the-big-security-mistakes-companies-make-when-buying-tech-1489372011>.

548. *Id.*

549. Open source products in particular present security challenges. See, e.g., Dan Geer & Joshua Corman, *Almost Too Big to Fail*, 39 USENIX, no. 4, Aug. 2014, at 66, https://www.usenix.org/system/files/login/articles/15_geer_0.pdf (explaining various vulnerabilities).

550. One such bill has been introduced in a past Congressional session. See, e.g., Cyber Supply Chain Management and Transparency Act of 2014, H.R. 5793, 113th Cong. (2014), <https://www.congress.gov/bill/113th-congress/house-bill/5793>.

b. Proposal 4: Defending entrepreneurship with security tax incentives and tools. Cash-strapped startups often struggle to learn about and implement security.⁵⁵¹ Yet, their vulnerable products may be the most likely candidates for becoming harnessed into a botnet,⁵⁵² and, consequently used in an attack on critical infrastructure or healthcare⁵⁵³ targets.

Security investment tax incentives for entrepreneurs would nudge material security improvements in much the same way that tax incentives were used to nudge environmental improvements.⁵⁵⁴ Congress should instruct the Department of Commerce and the Internal Revenue Service to construct a tax incentive structure aimed at providing phased-out tax credits to small businesses who wish to invest in their information security through hiring additional security staff, obtaining security training, or purchasing security services.⁵⁵⁵

Additionally, the FTC⁵⁵⁶ and the Defense Advanced Research Projects Agency (DARPA)⁵⁵⁷ have used contests under the America Competes Act, as renewed,⁵⁵⁸ as a way to stimulate entrepreneurship in security solutions. This type of contest approach should be

551. For a discussion of startups and security, see, for example, Luis A. Aguilar, *The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses*, U.S. SEC. & EXCHANGE COMMISSION (Oct. 19, 2015), <https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html> (explaining that small and midsize businesses “face precisely the same threat landscape that confronts larger organizations, but [they] must do so with far fewer resources”).

552. For a discussion of botnets and security risks, see, for example, *Botnets*, F-SECURE, https://www.f-secure.com/en/web/labs_global/botnets (last visited Jan. 12, 2018).

553. Hospitals currently face a ransomware problem, and threats of targeting from botnet operators are likely the next round of attack. For a discussion of hospital ransomware, see, for example, Erin Dietsche, *12 Healthcare Ransomware Attacks of 2016*, BECKER'S HEALTH IT & CIO REVIEW (Dec. 29, 2016), <http://www.beckershospitalreview.com/healthcare-information-technology/12-healthcare-ransomware-attacks-of-2016.html>.

554. See, e.g., *Tax Credits, Rebates, & Savings*, ENERGY.GOV, <https://energy.gov/savings> (last visited Jan. 12, 2018).

555. See also Jeff Kosseff, *Positive Cybersecurity Law: Creating a Consistent and Incentive-Based System*, 19 CHAP. L. REV. 401, 416 (2016) (“The government could provide companies with a tax credit for investments in qualified cybersecurity expenditures up to a certain annual amount.”).

556. See, e.g., *Contests*, FED. TRADE COMMISSION, <https://www.ftc.gov/news-events/contests> (last visited Jan. 12, 2018).

557. See, e.g., *The World's First All-Machine Hacking Tournament*, CYBER GRAND _CHALLENGE (Aug. 4, 2016), <http://archive.darpa.mil/cybergrandchallenge/>.

558. America Competes Act, H.R. 1806, 110th Cong. (2007) (renewed in substantial part by the American Innovation and Competitiveness Act, Pub. L. No. 114-329, 130 Stat. 2969 (2017)).

expanded and used by other agencies to stimulate security entrepreneurship and creation of new security tools for both the public and private sector.

c. Proposal 5: Defending market integrity. Defense primacy also involves facilitating market mechanisms. Specifically, invigorated federal agency enforcement is needed to ensure accuracy in corporate advertising and disclosures about security. Because different agencies have different missions and enforcement capabilities, a series of bilateral interagency enforcement-focused taskforces should be created to coordinate security enforcement. These various task forces should include teams across DHS, FTC, SEC, DOJ, FDA, CFPB, FCC, and any other agencies interested in participating in coordinated security enforcement or case referrals. Enforcement actions involving private sector security deficits would be either joint or coordinated, with each agency in the pair claiming portions of the enforcement activity best suited to its mission and authority but sharing resources where possible regarding basic investigation. The various task forces' dockets should include enforcement actions against entities who fail to fix known security flaws, provide inadequate security advisories, violate open source licenses' security terms, or make false claims of security about their products or operations. In this way, each agency will work on sections of the puzzle of security while maintaining a better sense of the bigger picture of security across both the government and the private sector.

V. CONCLUSION: NO CYBERS WERE HURT IN THE WRITING OF
THIS ARTICLE⁵⁵⁹

Clara: *Why would a computer need to protect itself from the people who made it?*

The Doctor: *All computers do that in the end. You wait 'til the internet starts. Oh, that was a war!*⁵⁶⁰

While Gadgetopia's fate ended unhappily, the future of the United States need not mirror it. We begin to chart a path away from Gadgetopia's fate by acknowledging that both the public and private sector face similar operational security challenges, despite legal

559. *No Animals Were Hurt in The Making of This Comic*, CHEEZBURGER, <http://cheezburger.com/8142448128> (last visited Jan. 12, 2018).

560. *Dr. Who: Hell Bent* (BBC One television broadcast Dec. 5, 2005).

differences in structure. This Article has introduced a reciprocal security paradigm. This novel paradigm has reframed the traditional security discourse away from its current focus on reactive information sharing and deterrence. Instead, it redirects attention toward a sector-neutral security approach with proactive security vigilance infrastructures and defense primacy.

May we live long and cyber.⁵⁶¹

561. *Live Long and Prosper (Vulcan Salute)*, FANLORE, [https://fanlore.org/wiki/Live_Long_and_Prospers_\(Vulcan_salute\)](https://fanlore.org/wiki/Live_Long_and_Prospers_(Vulcan_salute)) (last visited Jan. 12, 2018).

