Session 5 Optional Readings Part I: The Law of Cyber Offense: Understanding Domestic and International Frameworks | January 19, 2021

Megan Brown, Partner, Wiley Rein LLP; NSI Senior Fellow,
Adam Golodner, Former Chief of Staff, U.S. Department of Justice, Antitrust Division; NSI Visiting Fellow, &
Jamil N. Jaffer, NSI Founder and Executive Director

ESSAY

NORMS OF COMPUTER TRESPASS

*Orin S. Kerr**

This Essay develops an approach to interpreting computer trespass laws, such as the Computer Fraud and Abuse Act, that ban unauthorized access to a computer. In the last decade, courts have divided sharply on what makes access unauthorized. Some courts have interpreted computer trespass laws broadly to prohibit trivial wrongs such as violating terms of use to a website. Other courts have limited the laws to harmful examples of hacking into a computer. Courts have struggled to interpret authorization because they lack an underlying theory of how to distinguish authorized from unauthorized access.

This Essay argues that authorization to access a computer is contingent on trespass norms—shared understandings of what kind of access invades another person's private space. Judges are unsure of how to apply computer trespass laws because the Internet is young and its trespass norms are unsettled. In the interim period before norms emerge, courts should identify the best rules to apply as a matter of policy. Judicial decisions in the near term can help shape norms in the long term. The remainder of the Essay articulates an appropriate set of rules using the principle of authentication. Access is unauthorized when the computer owner requires authentication to access the computer and the access is not by the authenticated user or his agent. This principle can resolve the meaning of authorization before computer trespass norms settle and can influence the norms that eventually emerge.

---

* Fred C. Stevenson Research Professor, George Washington University Law School. Thanks to Steve Bellovin, David Cruz, Tim Edgar, Hanni Fakhoury, David Fontana, Mary Anne Franks, Ahmed Ghappour, Robert Graham, James Grimmelmann, Stephen Henderson, Marcia Hofmann, Michael Madison, Jonathan Mayer, Janice Nadler, Paul Ohm, Michael Risch, Ken Simons, Daniel Solove, Ashkan Soltani, Peter Winn, and commenters at the Privacy Law Scholars Conference and faculty workshops at Northwestern University Law School and the University of Southern California Gould School of Law for extremely helpful comments on an earlier draft.

INTRODUCTION

The federal government and all fifty states have enacted criminal laws that prohibit unauthorized access to a computer.[1] At first blush, the meaning of these statutes seems clear.[2] The laws prohibit trespass into a computer network just like traditional laws ban trespass in physical space.[3] Scratch below the surface, however, and the picture quickly turns cloudy.[4] Courts applying computer trespass laws have divided deeply over

1. The federal law is the Computer Fraud and Abuse Act (CFAA), codified at 18 U.S.C. § 1030 (2012). For a summary of state laws, see generally A. Hugh Scott, Computer and Intellectual Property Crime: Federal and State Law 639–1300 (2001); Susan W. Brenner, State Cybercrime Legislation in the United States of America: A Survey, 7 Richmond J.L. & Tech. 28, para. 15 n.37 (2001), http://jolt.richmond.edu/v7i3/article2.html [http://perma.cc/4YFP-KH8S].

2. See United States v. Morris, 928 F.2d 504, 511 (2d Cir. 1991) (concluding lower court was not required to instruct jury on meaning of "authorization" because "the word is of common usage, without any technical or ambiguous meaning").

3. See S. Rep. No. 104-357, at 11 (1996) (noting CFAA "criminalizes all computer trespass").

4. See Orin S. Kerr, Vagueness Challenges to the Computer Fraud and Abuse Act, 94 Minn. L. Rev. 1561, 1572, 1574 (2010) [hereinafter Kerr, Vagueness Challenges] (discussing uncertain application of CFAA); Note, The Vagaries of Vagueness: Rethinking the CFAA as a Problem of Private Nondelegation, 127 Harv. L. Rev. 751, 751–52 (2013) (noting scope of CFAA—chief federal computer crime law—"has been hotly litigated," and "the most substantial fight" is over meaning of authorization).

when access is authorized.[5] Circuit splits have emerged, with judges frequently expressing uncertainty and confusion over what computer trespass laws criminalize.[6]

Consider the facts of seven recent federal cases involving the federal unauthorized access law, the Computer Fraud and Abuse Act (CFAA).[7] In each case, the line between guilt and innocence hinged on a dispute over authorization:

1. An employee used his employer's computer at work for personal reasons in violation of a workplace rule that the computer could only be used for official business.[8]

2. An Internet activist logged on to a university's open network using a new guest account after his earlier guest account was blocked.[9]

3. Two men used an automated program to collect over 100,000 email addresses from a website that had posted the information at hard-to-guess addresses based on the assumption that outsiders would not find it.[10]

4. A man accessed a corporate account on a website using login credentials that he purchased from an employee in a secret side deal.[11]

5. A company collected information from Craigslist after Craigslist sent the company a cease-and-desist letter and blocked the company's IP address.[12]

---

5. See, e.g., United States v. Nosal, 676 F.3d 854, 865 (9th Cir. 2012) (en banc) (Kozinski, C.J.) (noting circuit split between Ninth Circuit and Fifth and Eleventh Circuits over whether employee who violates written restriction on employer's computer use engages in criminal unauthorized access under CFAA); NetApp, Inc. v. Nimble Storage, Inc., No. 5:13-CV-05058-LHK (HRL), 2015 WL 400251, at *11 (N.D. Cal. Jan. 29, 2015) (noting deep division in district courts on whether copying constitutes damage under CFAA); Advanced Micro Devices, Inc. v. Feldstein, 951 F. Supp. 2d 212, 217 (D. Mass. 2013) (noting two distinct schools of thought in case law on what makes access authorized).

6. See, e.g., CollegeSource, Inc. v. AcademyOne, Inc., 597 F. App'x 116, 129 (3d Cir. 2015) (noting meaning of authorization "has been the subject of robust debate"); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 n.10 (1st Cir. 2001) ("Congress did not define the phrase 'without authorization,' perhaps assuming that the words speak for themselves. The meaning, however, has proven to be elusive."); *Feldstein*, 951 F. Supp. 2d at 217 ("[T]he exact parameters of 'authorized access' remain elusive.").

7. 18 U.S.C. § 1030 (2012).

8. See *Nosal*, 676 F.3d at 863–64 (holding such acts do not violate CFAA).

9. See Indictment at 4–7, United States v. Swartz, Cr. 11-ER-10260 (D. Mass. July 14, 2011) (charging criminal defendant for such conduct).

10. See United States v. Auernheimer, 748 F.3d 525, 534–35 (3d Cir. 2014) (reversing conviction on venue grounds but not reaching whether it violated CFAA).

11. See Brief of Appellant at 10–14, United States v. Rich (4th Cir. Mar. 2, 2015) (No. 14-4774), 2015 WL 860788 (arguing such conduct does not violate CFAA).

12. See Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 968–70 (N.D. Cal. 2013) (concluding such conduct violates CFAA).

> 6. A company used an automated program to purchase tickets in bulk from Ticketmaster's website despite the website's use of a barrier designed to block bulk purchases by automated programs.[13]
>
> 7. A former employee continued to access his former employer's computer network using a backdoor account that the former employer had failed to shut down.[14]

On the surface, there are plausible arguments on both sides of these cases. The prosecution can argue that access was unwanted, at least in some sense, and therefore was unauthorized. The defense can argue that access was allowed, at least in some sense, and therefore was authorized.[15] Liability hinges on what concept of authorization applies. However, courts have not yet identified a consistent approach to authorization. Authorization is not defined under most computer trespass statutes, and the statutory definitions that exist are generally circular.[16] Violating computer trespass laws can lead to severe punishment, often including several years in prison for each violation.[17] And yet several decades after the widespread enactment of computer trespass statutes, the meaning of authorization remains remarkably unclear.

This Essay offers a framework to distinguish between authorized and unauthorized access to a computer. It argues that concepts of authorization rest on trespass norms. As used here, trespass norms are broadly shared attitudes about what conduct amounts to an uninvited entry into another person's private space.[18] Relying on the example of physical-world trespass, this Essay contends that the scope of trespass crimes follows from identifying trespass norms in three ways: first, characterizing the nature of the space; second, identifying the means of permitted access; and third,

---

13. See United States v. Lowson, Crim. No. 10-114 (KSH), 2010 WL 9552416, at *6–7 (D.N.J. Oct. 12, 2010) (discussing but not resolving CFAA liability for such facts).

14. See United States v. Steele, 595 F. App'x 208, 210–11 (4th Cir. 2014) (holding this violates CFAA).

15. See James Grimmelmann, Computer Crime Law Goes to the Casino, Concurring Opinions (May 2, 2013), http://concurringopinions.com/archives/2013/05/computer-crime-law-goes-to-the-casino.html [http://perma.cc/YYP8-A8A5] ("In any CFAA case, the defendant can argue, 'You say I shouldn't have done it, but the computer said I could!'").

16. For example, the CFAA does not define "without authorization," and the related term "exceeds authorized access" is defined circularly to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6) (2012).

17. See generally Orin S. Kerr, Computer Crime Law 328–75 (3d ed. 2013) (discussing sentencing under CFAA).

18. The word "norms" has been used to mean many different things, ranging from practices that are common and expected among members of a society to practices that are perceived as morally obligated within that group. See generally Richard H. McAdams & Eric B. Rasmusen, Norms and the Law, *in* 2 Handbook of Law and Economics 1575, 1576–78 (A. Mitchell Polinsky & Steven Shavell eds., 2007) (defining "norms"). In this Essay, I use the term "trespass norms" to focus specifically on norms that relate to perceptions of invasion of private space.

identifying the context of permitted entry. These three steps can be used to identify the norms of computer trespass and to give meaning to criminal laws on unauthorized access.

Interpreting computer trespass laws raises an important new twist. Although trespass norms in physical space are relatively settled and intuitive, computer trespass norms online are often unsettled and contested. The Internet is new and rapidly changing. No wonder courts have struggled to apply these laws: Doing so requires choosing among unsettled norms in changing technologies that judges may not fully understand. In that context, courts cannot merely identify existing norms. Instead, they must identify the best rules to apply from a policy perspective, given the state of technology and its prevailing uses. Published court decisions can then help establish norms consistent with those rules.

After first identifying the conceptual challenges of applying computer trespass laws, this Essay argues that the principle of authentication provides the most desirable basis for computer trespass norms. Authentication requires verifying that the user is the person who has access rights to the information accessed.[19] Under this principle, the open norm of the World Wide Web should render access to websites authorized unless it bypasses an authentication gate. This approach leaves Internet users free to access websites even when their owners have put in place virtual speed bumps that can complicate access, such as hidden addresses, cookies-based limits, and IP address blocks.[20] Further, when access requires authentication, whether access is authorized should hinge on whether it falls within the scope of delegated authority the authentication implies. Access to canceled accounts should be unauthorized, and access using new accounts may or may not be authorized depending on the circumstances.[21] Finally, the lawfulness of access using a shared password should depend on whether the user intentionally acts outside the agency of the account holder.

The authentication principle advocated in this Essay best captures the competing policy goals of modern Internet use in light of the blunt and severe instrument of criminal law. Norms based on this principle give users wide berth to use the Internet as the technology allows, free from the risk of arrest and prosecution, as long as they do not contravene mechanisms of authentication. On the other hand, the norms give computer owners the ability to impose an authentication requirement and then control who accesses private information online. The result establishes both public and private virtual spaces online using a relatively clear and stable technological standard.

---

19. See infra section III.C (explaining authentication).

20. See infra Part III (discussing open nature of Web and mechanisms used by site owners to restrict access).

21. See infra Part IV (discussing distinction between canceled accounts, blocked accounts, and new accounts).

This Essay contains four parts. Part I shows how trespass norms apply in physical space. Part II argues that courts should apply the same approach to computer networks but that they must identify the best trespass norms rather than simply identify existing norms. Part III considers the trespass norms that courts should identify in the many difficult cases involving the Web. Part IV explains how the norms of computer trespass should apply to the complex problems raised by canceled, blocked, and shared accounts.

I. TRESPASS IN PHYSICAL SPACE

Imagine a suspicious person is lurking around someone else's home or office. The police are called, and officers watch the suspect approach the building. Now consider: When has the suspect committed a criminal trespass that could lead to his arrest and prosecution? This section shows how the answer comes from trespass norms in physical space—shared understandings of obligations surrounding access to different physical spaces. The rules are not written down in trespass statutes. Instead, those called on to interpret physical trespass laws make intuitive conclusions based on the nature of that space and the understood purposes of different means of accessing it. From those intuitions, shared understandings emerge about whether and when access to a physical space is permitted. By unpacking our intuitions that govern physical trespass, we can then appreciate why courts have struggled to interpret computer trespass laws.

A. *Authorization and Social Norms*

The concept of trespass implies signals sent by property owners about what uses of that property are permitted. In some cases, the signals are clear and direct. Recall the childhood game "red light, green light."[22] In the game, the game master barks out orders to the players. Green light, they can run. Red light, they must stop. The control is direct and in realtime, with the game master watching the players in person. In this environment, notions of authorization are obvious. The leader monitors and maintains complete control.

The more common and interesting problems arise when control of authorization is implicit. In most cases, permission is deduced from the circumstances based on signals that draw on shared understandings about the world. A Martian who landed on Earth for the first time would find the results deeply puzzling. Having never experienced human social interaction, it would miss the signals and see the human understandings as arbitrary. From our perspective, however, the signals are intuitive and usually seem obvious.

22. See Red Light/Green Light, Games Kids Play, http://www.gameskidsplay.net/games/sensing_games/rl_gl.htm [http://perma.cc/3JVF-NZWM] (last visited Jan. 26, 2016).

Importantly, the text of criminal trespass statutes doesn't provide these answers.[23] Consider New York's trespass law, § 140.05. The language is brief: "A person is guilty of trespass when he knowingly enters or remains unlawfully in or upon premises."[24] What does "unlawfully" mean? The statutory definition tries but fails to answer that question. "A person 'enters or remains unlawfully' in or upon premises," the definition says, "when he is not licensed or privileged to do so."[25] That's no help. When are you "licensed" to enter? What gives you a "privilege"? The text doesn't say.

Criminal trespass law can retain this textual ambiguity because the real meaning of trespass law comes from trespass norms that are relatively clear in physical space.[26] The written law calls on the norms, and the norms tell us, at an intuitive level, when entry to property is forbidden and when it is permitted. Although identifying social norms is often difficult generally, the specific nature of trespass norms allows greater clarity. Trespass norms are relatively specific: They are about shared intuitions about what is a trespass, not what is appropriate or inappropriate behavior generally. And those norms provide relative clarity about what is a physical trespass.

Relative clarity doesn't mean absolute clarity, of course. Criminal trespass law is rarely litigated. Physical trespass tends to be a low-level offense,[27] and it typically extends to those who unlawfully remain in place after being told by the homeowner to leave.[28] As a practical matter, the crime may be used primarily as a way to arrest and remove someone who won't leave where he is not wanted rather than as a tool for criminal pun-

---

23. Trespass is an accordion-like concept that can mean different things in different contexts. See, e.g., 3 William Blackstone, Commentaries *208–09 (discussing variations of trespass at common law). Because computer trespass laws are primarily criminal statutes, the discussion focuses on liability under criminal trespass statutes. I am therefore excluding consideration of other kinds of trespass claims such as the scope of the common law tort of trespass to chattels. See generally eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1069–70 (N.D. Cal. 2000) (applying common law tort of trespass-to-chattels analysis in computer context).

24. N.Y. Penal Law § 140.05 (McKinney 2010).

25. Id. § 140.00(5).

26. See Richard H. McAdams, The Origin, Development, and Regulation of Norms, 96 Mich. L. Rev. 338, 340 (1997) ("Sometimes norms govern behavior irrespective of the legal rule, making the choice of a formal rule surprisingly unimportant."); see also Cass R. Sunstein, Social Norms and Social Roles, 96 Colum. L. Rev. 903, 914 (1996) (defining social norms as "social attitudes of approval and disapproval, specifying what ought to be done and what ought not to be done").

27. For example, under New York law, trespass only carries an offense level of a violation. N.Y. Penal Law § 140.05. A violation carries a maximum punishment of fifteen days. Id. § 10.00(3).

28. See, e.g., id. § 140.05 ("A person is guilty of trespass when he knowingly enters *or remains* unlawfully in or upon premises." (emphasis added)).

ishment on conviction.[29] As a result, some ambiguities may exist but remain latent in the statute.

But even if ambiguities remain, they are substantially narrowed by the three ways that trespass norms inform the meaning of criminal trespass laws. First, trespass norms provide a general set of rules that govern entrance based on the nature of the space. Second, they help resolve which means of access are permitted. And third, they explain the context in which the permitted means become authorized.

B. *The Nature of the Space*

The first way that trespass norms guide notions of license and privilege is by providing informal rules based on the nature of each space. Different spaces trigger different obligations. Private homes trigger one set of rules. Commercial stores would trigger another. A public library might trigger a third. A public park a fourth. Life experience with common social practices creates shared understandings about what kinds of entry are permitted for different kinds of spaces.

Start with the home. The home triggers a robust set of assumptions about privacy and permission.[30] A person's home is his castle, the common law tells us.[31] And the principle of the common law remains deeply and widely held today. Everyone knows that you stay out of another's home unless there is an express invitation. If you break those norms, trouble will follow. You can expect a frightened homeowner to call the police, if not to emerge with a twelve gauge pointed in your direction. And trespass case law reflects the strong default presumption of the home: The slightest overstep or intrusion into the home, or even just entry based on false pretenses, has been held to be a trespass.[32]

But what is true for the home is not true for other physical spaces. Contrast the home with a commercial store. Imagine it's a weekday afternoon and you find a flower shop in a suburban strip mall. The norms governing access to the shop are very different from those governing ac-

---

29. In general, probable cause to arrest a suspect for criminal trespassing can justify the suspect's arrest and removal so long as the offense—typically, the refusal to leave—is occurring in the officer's presence. See, e.g., N.Y. Crim. Proc. Law § 140.10 (McKinney 2004) (describing arrest powers).

30. See generally Stephanie M. Stern, The Inviolate Home: Housing Exceptionalism in the Fourth Amendment, 95 Cornell L. Rev. 905, 912 (2010) (discussing special status of home in Fourth Amendment law).

31. See Semayne's Case (1604) 77 Eng. Rep. 194, 198; 5 Co. Rep. 91 a, 93 a ("[T]he house of any one is not a castle or privilege but for himself.").

32. See, e.g., People v. Bush, 623 N.E.2d 1361, 1364 (Ill. 1993) ("If . . . the defendant gains access to the victim's residence through trickery and deceit and with the intent to commit criminal acts, his entry is unauthorized and the consent given vitiated because the true purpose for the entry exceeded the limited authorization granted."); People v. Williams, 667 N.Y.S.2d 605, 607 (Sup. Ct. 1997) (concluding "person who gains admittance to premises through intimidation or by deception, trick or artifice, does not enter with license or privilege" for purposes of criminal trespass liability).

cess to a home. You can approach the store and peer through the window. If you see no one inside, you can try to enter through the front door. If the door is unlocked, you can enter the store and walk around. The shared understanding is that shop owners are normally open to potential customers. An unlocked door during work hours ordinarily signals an invitation. That openness is not unlimited, of course. You can't go into the back of the store, marked "Employees Only," without an invitation.[33] And if the store owner tells you to leave, you have to comply.[34] But in contrast to the closed default at a private home, the default at a commercial store is openness absent special circumstances indicating closure.

Even open spaces can have trespass norms, and those norms can differ from the norms governing entry into enclosed structures such as homes or stores. In a recent Fourth Amendment case, *Florida v. Jardines*,[35] the Supreme Court considered the trespass norms that apply to a front porch. Officers suspected that Jardines might be growing marijuana in his home, so they walked a drug-sniffing dog up to his front porch and had him give the front door a good, hard sniff.[36] The dog alerted to drugs, creating probable cause for a warrant and a search.[37]

The Justices ruled that walking up to the front door with the dog was a trespass that violated the Fourth Amendment because it exceeded the implied social license governing approach to the home.[38] According to Justice Scalia, some entry onto the front porch was permitted by social custom. Any visitor could "approach the home by the front path, knock promptly, wait briefly to be received, and then (absent invitation to linger longer) leave."[39] On the other hand, bringing a drug-sniffing dog to the front door violated that customary understanding:

> To find a visitor knocking on the door is routine (even if sometimes unwelcome); to spot that same visitor exploring the front path with a metal detector, or marching his bloodhound into

33. See, e.g., State v. Cooper, 860 N.E.2d 135, 138 (Ohio Ct. App. 2006) (entering portion of store marked "Employees Only" was trespass because sign "put the defendant on notice that by entering the room, he was in violation of restriction against access that applied to him").

34. See, e.g., Model Penal Code § 221.2(2)(a) (Am. Law Inst. 2015) (punishing as "defiant trespass" a person who stays in a place when notice of trespass has been provided by "actual communication to the actor").

35. 133 S. Ct. 1409 (2013).

36. Id. at 1413.

37. Id.

38. See id. at 1417 ("[W]hether the officers had an implied license to enter the porch . . . depends upon the purpose for which they entered. Here, their behavior objectively reveals a purpose to conduct a search, which is not what anyone would think he had license to do.").

39. Id. at 1415.

> the garden before saying hello and asking permission, would inspire most of us to—well, call the police.[40]

The lesson is that different spaces have different trespass norms. Some spaces are open, others are closed, and still others are open to some but closed to others. The text of trespass laws is often misleadingly simple—just the simple prohibition against unlicensed entry. Meanwhile, the real work of distinguishing culpable invasions from nonculpable explorations comes from space-specific norms.

C. *Means of Access*

The second role of trespass norms is to identify means of permitted access. Permission to enter often is implicitly limited to specific methods of entrance. And we know which means of entry are permitted, and which are forbidden, by relying on widely understood social understandings.

Consider entrance to a commercial store. The trespass norm governing a commercial store might be that entrance is permitted when a ready means of access is available that can be read in context as an open invitation. That principle implies limits on which means of access are allowed. An open window isn't an invitation to jump through the window and go inside. If there's an open chimney or mail drop, that's not an invitation to try to enter the store. Barring explicit permission from the store owner, the only means of permitted access to a commercial store is the front door.

The source of these principles seems to be a socially shared understanding of the intended function of walls, windows, chimneys, and doors. Windows are there to let in light, not people. Chimneys exist to let out smoke, not admit guests (Santa excepted). We know from life experience that these ways in are not authorized. In contrast, entry through the unlocked front door is authorized. The front door is intended for customer entrance and exit. That's why it's there.

D. *Context of Access*

Trespass norms play a third role by governing the context in which entrance can occur. Entry through the front door might be authorized, but the front door isn't for everyone. Doors usually come with locks, and locks are designed to let some people in and keep other people out. Locks are an example of access control by which we recognize a means of access but limit it to specific people with specific rights.[41] To complete

---

40. Id. at 1416. According to Justice Scalia, the norms were readily grasped even though they were not written down: "Complying with the terms of that traditional invitation does not require fine-grained legal knowledge; it is generally managed without incident by the Nation's Girl Scouts and trick-or-treaters." Id. at 1415.

41. See Alfred J. Menezes, Paul C. van Oorschot & Scott A. Vanstone, Handbook of Applied Cryptography 3 (1996) (defining "access control" as means of "restricting access to resources to privileged entities").

the picture of how norms govern authorization to enter a home, we need to consider how those norms apply to locks and keys.

The starting point is simple enough. The property owner owns the door, lock, and keys, so the owner presumptively is in charge. If the lock breaks, the owner has to buy another one. The owner has the power to decide who gets a key and who is permitted to use it. As a result, authorization of entrance by key depends on whether that entrance was within the zone of authority delegated by the owner.

Imagine you are walking down the street and you see and pick up a lost house key. Possession of the key doesn't entitle you to use the key and enter the house. You have the key, but you lack permission to use it. And you lack permission because there's no chain of authorization coming from the owner. Picking a lock is unauthorized for the same reasons, at least unless you're a locksmith who the owner hired to open the door after being locked out.[42] If the owner grants you permission but later revokes it, your authorization expires with the revocation. If the homeowner gives someone else the key but places limits on access, those limits govern authorization.[43]

The lesson of these examples is that authorization rests on trespass norms. In a world of indirect communication, familiarity with the social signals of what entry is permitted or forbidden makes the law clear enough that most people don't fear arrest in their everyday activity. The nature of the space provides one set of messages, norms about the intended purpose of different means of access provide even more detailed guidance, and access controls within the zone of permission delegated by property owners provide an additional layer of rules.

II. THE NORMS OF COMPUTER TRESPASS

The Internet has its own kind of trespass law that closely resembles its physical-world cousin. In cyberspace, the relevant law is found in computer misuse statutes such as the CFAA.[44] The CFAA and its state equivalents ban unauthorized access to a computer.[45] At a broad level, the purpose of those statutes is easy to describe: Unauthorized access statutes are computer trespass statutes.[46] Applying the new statutes requires translat-

42. Cf. Taha v. Thompson, 463 S.E.2d 553, 557 (N.C. Ct. App. 1995) (holding evidence that individual sent locksmith onto property to change locks without homeowner's permission establishes trespass).

43. See Douglas v. Humble Oil & Ref. Co., 445 P.2d 590, 591 (Or. 1968) (en banc) (holding employee who was given key to employer's home to feed employer's pets committed trespass when employee used key to enter home for different reason).

44. 18 U.S.C. § 1030 (2012).

45. For an overview, see generally Scott, supra note 1, at 639–1300. In this Essay, I include both "access without authorization" and conduct that "exceeds authorized access" as within the general ban on unauthorized access. See infra section III.B (discussing unauthorized access).

46. See supra notes 2–5 (discussing court applications of computer trespass laws).

ing concepts of trespass from physical space to the new environment of computers and networks. But as courts have found, understanding the concept of authorization to computers ends up being surprisingly hard.[47] The courts are divided, with many courts struggling to apply this simple-seeming concept.[48]

The norms-driven nature of physical trespass law explains why courts have struggled to interpret computer trespass laws. The trespass norms of physical space are relatively clear because they are based on shared experience over time. The Internet and its technologies are new, however, and the trespass norms surrounding its usage are contested and uncertain. When faced with an authorization question under a computer trespass law, today's judges bring to mind the Martian from outer space considering how traditional trespass laws might govern trespass into a home. Without established norms to rely on, the application of a seemingly simple concept like "authorization" becomes surprisingly hard.

This section develops three lessons for interpreting authorization in computer trespass statutes that follow from the norms-based nature of trespass law. First, the meaning of authorization will inevitably rest on the identification of trespass norms, which will in turn rest on models and analogies. Second, Internet technology is sufficiently new, and the norms of computer trespass sufficiently unsettled, that judges applying computer trespass law must not just identify existing trespass norms, but must identify as a policy matter the optimal rules that should govern the Internet. And third, despite these challenges, trespass provides a sensible framework for regulating computer misuse and courts have the ability to identify and apply the norms for computer trespass within the framework of existing laws.

A. *The Inevitability of Norms in Computer Trespass Law*

The first lesson is that the meaning of authorization in computer trespass laws inevitably rests on the identification of proper trespass norms. Like their physical-world cousins, computer trespass laws feature unilluminating text. They prohibit unauthorized access to computers just like physical trespass laws prohibit unlicensed entry to physical spaces. In both contexts, the meaning of the law must draw from social understandings about access rights drawn from different signals within the relevant spaces. Courts must identify the rules of different spaces based on understandings of the relevant trespass norms.

It's no surprise that litigation over computer trespass laws often triggers a battle of physical-space analogies. The government, seeking a broad reading of the law, will push analogies to physical facts that trigger strict norms. The defense, seeking a narrow reading of the law, will push analo-

47. See supra notes 2–5.

48. See supra notes 4–5 (providing examples of disagreements among courts over concept of authorization in CFAA).

gies to physical facts that implicate loose norms. The battle of analogies happens not because it is inevitable that we analogize cyberspace to physical space,[49] but rather because authorization inevitably rests on trespass norms. Litigants will use analogies from physical spaces with the trespass norms that best aid their side.

Consider the recent litigation in *United States v. Auernheimer*.[50] Auernheimer had been convicted of unauthorized access for using a software program that collected information from an AT&T website at hard-to-guess addresses intended to be kept private.[51] On appeal to the Third Circuit, the government's brief analogized the website to a home where trespass norms are at their zenith. Use of the program was a computer trespass, the government argued, because a physical trespass occurs "when an unauthorized person enters someone else's residence, even when the front door is left open or unlocked."[52] In contrast, the defense analogized the website to a public space where trespass norms are at their nadir. Use of the program was not a trespass, the defense argued, because putting information on a website "ma[d]e the information available to everyone and thereby authorized the general public to view the information."[53] Each analogy aimed to import a set of physical-world norms.[54]

B. *Because Computer Trespass Norms Are Unsettled, Courts Should Identify the Best Norms to Apply*

The conflicting analogies found in computer trespass cases highlight the biggest difference between applying physical trespass and computer trespass laws: Computer trespass norms remain uncertain. Understandings of access rights surrounding the home are ancient, while understandings of access rights in computer networks are not. The statutes came first, and the statutory prohibition on unauthorized access has remained fixed while computer network technology has advanced at astonishing speed. In this environment, courts cannot merely identify existing norms. Instead, they should make a normative policy decision about what understandings should govern the Internet. Judicial decisions will then shape future computer trespass norms, allowing appropriate norms to emerge with the help of the courts.

---

49. See Mark Lemley, Place and Cyberspace, 91 Calif. L. Rev. 521, 523–26 (2003) ("[E]ven a moment's reflection will reveal that the analogy between the Internet and a physical place is not particularly strong.").

50. 748 F.3d 525 (3d Cir. 2014). Full disclosure: I represented Auernheimer.

51. Id. at 530–31.

52. Brief for Appellee at 34, *Auernheimer*, 748 F.3d 525 (No. 13-1816), 2013 WL 5427839.

53. Brief for Appellant at 15, *Auernheimer*, 748 F.3d 525 (No. 13-1816), 2013 WL 3488591.

54. The Third Circuit did not reach this issue, as it reversed on the ground that venue was lacking in the district where the prosecution was brought. *Auernheimer*, 738 F.3d at 541.

To appreciate the problem, consider the rapid evolution of Internet technologies. The Internet itself is less than fifty years old.[55] The World Wide Web is only about twenty years old.[56] The experience of using the Internet morphs quickly. Fifteen years ago, connecting to the Internet meant logging on from a desktop computer at work or perhaps using a dial-up connection from home. Today, connecting to the Internet is very different. Wireless connections have become the norm, allowing anyone to access the Internet from almost anywhere. And in just the last five years, the rise of the "smart phone" has brought the Internet to a light hand-held device that most adults leave on 24/7 and carry with them in their pockets and purses.[57]

The programs we use to access the Internet also change rapidly. A majority of Americans now have a Facebook account, and about seventy percent of account holders visit Facebook every day.[58] But Facebook wasn't even invented until 2004,[59] and it already has become passé among teenagers who have moved on to Instagram (launched in 2010[60]) and Snapchat (launched in 2011[61]).[62] Or consider the popular Apple iPhone introduced in 2007.[63] The iPhone popularized the phrase "there's an app for that"[64] for the new applications, or "apps," that the phone can run. Apple's

---

55. See Reno v. ACLU, 521 U.S. 844, 849–50 (1997) (tracing history of Internet from ARPANET in 1969).

56. See Tim Berners-Lee with Mark Fischetti, Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor 69 (1999) (describing February 1993 release of first popular web browser).

57. See Riley v. California, 134 S. Ct. 2473, 2484 (2014) (recognizing "modern cell phones . . . are now such a pervasive and insistent part of daily life" but were "unheard of ten years ago").

58. Elizabeth Weise, Your Mom and 58% of Americans Are on Facebook, USA Today (Jan. 9, 2015, 5:22 PM), http://www.usatoday.com/story/tech/2015/01/09/pew-survey-social-media-facebook-linkedin-twitter-instagram-pinterest/21461381/ [http://perma.cc/QNK9-N5WZ].

59. Company Info: Our History, Facebook, http://newsroom.fb.com/timeline/company-info/ [http://perma.cc/9J9R-H2BT] (last visited Jan. 26, 2016).

60. MG Siegler, Instagram Launches with the Hope of Igniting Communication Through Images, TechCrunch (Oct. 6, 2010), http://techcrunch.com/2010/10/06/instagram-launch/ [http://perma.cc/T7E2-YNU3].

61. J.J. Colao, Snapchat: The Biggest No-Revenue Mobile App Since Instagram (Nov. 27, 2012, 1:36 PM), http://www.forbes.com/sites/jjcolao/2012/11/27/snapchat-the-biggest-no-revenue-mobile-app-since-instagram/ [http://perma.cc/P6LY-7J73].

62. See Joanna Stern, Teens Are Leaving Facebook and This Is Where They Are Going, ABC News (Oct. 31, 2013), http://abcnews.go.com/Technology/teens-leaving-facebook/story?id=20739310 [http://perma.cc/4S6G-ZHYE] (noting migration of teen users from Facebook to Instagram and Snapchat).

63. See Press Release, Apple, Apple Reinvents the Phone with iPhone (Jan. 9, 2007), http://www.apple.com/pr/library/2007/01/09Apple-Reinvents-the-Phone-with-iPhone.html [http://perma.cc/L937-DHP4]; see also Steve Jobs, iPhone Introduction in 2007, YouTube (Jan. 10, 2014), http://www.youtube.com/watch?v=9hUIxyE2Ns8.

64. The phrase comes from a commercial for the iPhone 3G in 2009. Apple, There's an App for That, YouTube (Feb. 4, 2009), http://www.youtube.com/watch?v=szrsfeyLzyg.

iTunes App Store has more than 1.5 million apps available already,[65] and about 1,000 new apps are submitted for approval every day.[66] Even the specific programs we use change over time. Regular updates and improvements are the norm, with new versions often adding features that can substantially change the user experience.

The problem is not just technological. The lawyers have stepped in, too. Companies often hire counsel to write detailed terms of use that purport to say when access is permitted.[67] These written contractual limitations can be extremely restrictive,[68] often creating a clash between what the technology allows a user to do and what the language of the terms says is allowed. In that case, what governs: the technology or the language? Amidst this rapid technological change, courts cannot merely invoke existing trespass norms to interpret authorization to access a computer. It's not clear any widely shared norms exist yet.

Deferring to jury verdicts is not workable, either. Trial courts have often used jury instructions that either leave authorization undefined or else tell the jury, unhelpfully, that access is unauthorized when it is without permission.[69] A study by Matthew Kugler suggests that this leads to verdicts far beyond whatever trespass norms may emerge.[70] Kugler surveyed 593 adult Americans by asking them to review short descriptions of the facts of several CFAA cases.[71] Respondents were asked to what extent the computer user had "authorization to use the computer" in the way

---

65. Number of Available Apps in the Apple App Store from July 2008 to June 2015, Statista, http://www.statista.com/statistics/263795/number-of-available-apps-in-the-apple-app-store/ [http://perma.cc/CVH8-P4J5] (last visited Jan. 26, 2016).

66. Number of Newly Developed Applications/Games Submitted for Release to the iTunes App Store from 2012 to 2014 (Fee Based), Statista, http://www.statista.com/statistics/258160/number-of-new-apps-submitted-to-the-itunes-store-per-month/ [http://perma.cc/YN4W-7FM4] (last visited Jan. 26, 2016).

67. See Judith A. Powell & Lauren Sullins Ralls, Best Practices for Internet Marketing and Advertising, 29 Franchise L.J. 231, 235 (2010) (advising franchise operators to protect themselves by creating terms of use that allow franchisors to effectively control sites' content).

68. See United States v. Nosal, 676 F.3d 854, 860–63 (9th Cir. 2012) (providing examples of ways computer-use policies prohibit common activity).

69. See, e.g., United States v. Morris, 928 F.2d 504, 511 (2d Cir. 1991) (agreeing with lower court that "it was unnecessary to provide the jury with a definition of 'authorization' . . . [s]ince the word is of common usage"); United States v. Drew, 259 F.R.D. 449, 461 (C.D. Cal. 2009) (noting no evidence Congress intended to give specialized meaning to "authorization" and "authorized" in CFAA and citing dictionary definition); Transcript for Trial at 26–27, United States v. Auernheimer, Crim. No. 11-cr-470 (SDW), 2012 WL 5389142 (D.N.J. Oct. 26, 2012), rev'd, 748 F.3d 525 (3d Cir. 2014) ("To access without authorization is to access a computer without approval or permission.").

70. See Matthew B. Kugler, Measuring Computer Use Norms (unpublished manuscript) (manuscript at 25) (Oct. 19, 2015), http://ssrn.com/abstract=2675895 (on file with the *Columbia Law Review*) [hereinafter Kugler, Measuring Norms] (noting participants' willingness to find common behavior blameworthy and, in some cases, criminal).

71. Id. (manuscript at 6).

he did, measured on a scale of one (not at all) to six (very much).[72] The study then asked respondents to assign the proper punishment for the act, with respondents choosing among four options: no punishment at all; punishment akin to a parking ticket, punishment for a minor crime such as petty theft, and punishment for a major crime such as burglary.[73]

Kugler's survey suggests that lay opinion about when use is "authorized" differs considerably from trespass norms. In most of the scenarios, respondents viewed the computer use as unauthorized. Mean values of authorization ranged from a low of 1.43 (for an employee who used his employer's computer to sell employer trade secrets) to a high of 2.32 (for an employee who used his employer's computer to check the weather report for personal reasons).[74] But these evaluations had little connection to the respondents' evaluations of what should be criminal. For example, although checking the weather report from work was generally considered unauthorized, sixty percent thought it should not be punishable at all and another thirty-two percent concluded that it should only be punished like a parking ticket.[75] Where clear trespass norms exist, we would expect most to say that violating them should subject the trespasser to at least some criminal punishment. Kugler's results suggest that lay judgments of authorization probably do not accurately measure trespass norms, at least to the extent such norms now exist.

Courts must instead decide between competing claims for what the trespass norms should be, imposing an answer as a matter of law now rather than allowing them to develop organically. One plausible response from courts could be to refuse to go along. If the law rests on unknown norms, perhaps courts should strike down unauthorized access statutes as unconstitutionally void for vagueness—or at least construe them narrowly in light of the vagueness concerns they present.[76] I have argued that position before,[77] and it retains significant force. However, the alternative path is for courts to draw lines based on the normatively desirable rules and standards that should govern Internet use. In the interim period before norms emerge, courts can identify the best rules to apply as a matter

---

72. Email from Matthew B. Kugler to Orin Kerr, Fred C. Stevenson Research Professor, George Washington Univ. Law Sch. (Nov. 13, 2015) (on file with the *Columbia Law Review*).

73. Kugler, Measuring Norms, supra note 70 (manuscript at 6).

74. Id. (manuscript at 14).

75. Id. Seventy-seven percent thought that selling trade secrets should be a serious crime like burglary, but of course, it already is: The crime is theft of trade secrets, a separate offense from computer trespass. See 18 U.S.C. § 1832 (2012).

76. See Kerr, Vagueness Challenges, supra note 5, at 1561 (arguing "CFAA requires courts to adopt narrow interpretations of the statute in light of the void-for-vagueness doctrine").

77. See id. at 1562 ("The CFAA has become so broad, and computers so common, that expansive or uncertain interpretations of unauthorized access will render it unconstitutional.").

of policy. Judicial decisions in the near term can influence norms in the long term.

C. *Trespass Law Provides the Appropriate Framework to Resolve Computer Misuse, and Courts Can Meet the Challenge*

It is worth asking whether trespass provides the right framework to apply and if judges are up to the task. I think the answer to both questions is yes. Trespass provides an appropriate framework because it implies an essential balance. On one hand, protecting online privacy requires recognizing some boundary that individuals cannot cross. On the other hand, preserving the public value of the Internet requires identifying uses that individuals can enjoy without fear of criminal prosecution. Some cases are easy. Everyone agrees that guessing another person's password to access his private email without his permission should be considered a criminal invasion of privacy. Similarly, everyone agrees that visiting a public website with no access controls or written restrictions should be legal. The trespass structure is sensible. The real challenge is applying it.

I am optimistic that courts can identify and apply computer trespass norms using existing statutes. The very first federal appellate case on the meaning of authorization in the CFAA, *United States v. Morris*,[78] shows why. *Morris* offers an early example of how courts can identify norms of computer trespass using the same three inquiries that govern trespass in the physical world: the nature of the space, the means of entry, and the context of entry.

In the fall of 1988, Robert Tappan Morris, a computer science graduate student, crafted and released a program often called "the Internet worm."[79] Morris designed the worm to reveal the weak computer security in place on the Internet.[80] First, the program exploited what the court called a "hole or bug (an error)" in three different software programs.[81] And second, the program guessed passwords, "whereby various combinations of letters are tried out in rapid sequence in the hope that one will be an authorized user's password."[82] Morris sent the worm from a computer at MIT, and it quickly spread around the world.[83] Morris was then charged with and convicted of "intentionally access[ing] a Federal interest computer without authorization."[84]

---

78. 928 F.2d 504 (2d Cir. 1991).

79. Id. at 505.

80. Id. ("The goal of this program was to demonstrate the inadequacies of current security measures on computer networks by exploiting the security defects that Morris had discovered.").

81. Id. at 506 (internal quotation marks omitted).

82. Id.

83. Id.

84. Id. (convicting defendant under 18 U.S.C. § 1030(a)(5)(A) (1986)).

On appeal, the Second Circuit affirmed the conviction. Writing for the court, Judge Jon Newman found three reasons why the access was without authorization. First, the evidence at trial demonstrated "that the worm was designed to spread to other computers at which he had no account and no authority, express or implied, to unleash the worm program."[85] Second, the worm exploited security flaws in software commands. "Morris did not use either of those features in any way related to their intended function."[86] Instead, Morris "found holes in both programs that permitted him a special and unauthorized access route into other computers."[87] Finally, the worm also guessed passwords, rendering access to those accounts unauthorized.[88]

Judge Newman's brief explanation of why the Internet worm had accessed computers without authorization contains all of the ingredients for the proper way to think about computer trespass. First, *Morris* addressed the nature of the virtual space. Although the computers were connected to each other, access was limited to (and based on) private accounts. A user needed an officially sanctioned account to access that particular machine. Much like houses on a row in a suburban street, the computers were linked to each other but required a key or special permission to jump from the inside of one to the inside of another.

Second, *Morris* focused on the means of entry. None of the programs, used as intended, were ways of gaining access to a private account. But the Internet worm exploited security flaws by using "holes" and "bugs" in the programs that permitted "special access" in a way that was contrary to the "intended function" of the commands.[89] Instead of gaining access through the virtual front door, the worm gained access by exploiting security flaws: It broke in through an open window instead. It gained entrance through a bug, not a feature.

Third, the *Morris* opinion focused on the context of entry. When the Internet worm accessed a private account with a password, it did so only by guessing that password.[90] Here the analogy to physical entry seems intuitive. Guessing a password is like picking a physical lock. A successful guess provides access, just like a successful lock pick does. But the access is not authorized because it does not come directly or indirectly from the property owner. The trespass norm governing locks is that access is permitted only to those who have been granted the key in a delegation of permission beginning with the owner. Password guessing is outside the norm and therefore unauthorized.

---

85. Id. at 510.
86. Id.
87. Id.
88. Id.
89. Id.
90. Id.

Morris provides a helpful model for how courts can adopt sensible and clear computer trespass norms even when faced with new facts. A quarter century later, courts can follow the *Morris* example. The remaining Parts offer more specific guidance on how courts can do that for important cases that arise in the context of the Web, as well as blocked, canceled, and shared accounts.

III. NORMS OF THE WORLD WIDE WEB

Many tricky questions interpreting computer trespass statutes involve use of the World Wide Web. The Web did not exist when Congress enacted the CFAA.[91] But it has quickly become an important—if not the *most* important—way people use the Internet. Identifying the trespass norms of the Web is difficult because there are two competing narratives in play. On one hand, the World Wide Web is open: By default, anyone can go to any website. On the other hand, website owners frequently put up speed bumps, barriers, and caveats to access that range from hidden website addresses and terms of use to limiting cookies and banning IP addresses.[92] The hard question is this: When should use of the Web in the face of such efforts render the use unauthorized?

This Part argues that courts should adopt presumptively open norms for the Web. The nature of the space is inherently open. Courts should match the open technology of the Web by applying an open trespass norm. Limited efforts to regulate access such as terms of use, hidden addresses, cookies, and IP blocks should be construed as merely speed bumps rather than virtual barriers. None of these methods should overcome the basic open nature of the Web. Access that bypasses these regulations should still be authorized.

The authorization line should be deemed crossed only when access is gained by bypassing an authentication requirement. An authentication requirement, such as a password gate, is needed to create the necessary barrier that divides open spaces from closed spaces on the Web. This line achieves an appropriate balance for computer trespass law. It protects privacy when meaningful steps are taken to seal off access from the public while also creating public rights to use the Internet free from fear of prosecution.[93]

---

91. Tim Berners-Lee invented the World Wide Web in 1990, and the first browser was introduced in 1993. See Berners-Lee & Fischetti, supra note 56, at 69 (recounting history of first web browsers).

92. See infra section III.B (discussing authorized web access).

93. The CFAA sometimes distinguishes between violations of the CFAA based on "access without authorization" and violations based on acts that "exceed[] authorized access." Compare 18 U.S.C. § 1030(a)(2) (2012) (prohibiting actors from both kinds of violations when actors obtain information), with id. § 1030(a)(5)(B) (prohibiting only access without authorization when it results in damage). I agree with the conclusion of the Second and Ninth Circuits that the two forms of liability cover the same acts. See United States v. Valle, 807 F.3d 508, 524–28 (2d Cir. 2015); United States v. Nosal, 676 F.3d 854,

A. *The Inherent Openness of the Web*

The first step in applying computer trespass law to the Web is to identify the nature of the space that the Web creates. The Web is a publishing protocol for the Internet. It allows anyone in the world to publish information that can be accessed by anyone else without requiring authentication. When a computer owner decides to host a web server, making files available over the Web, the default is to enable the general public to access those files. A user who surfs the Web enters an address into the prompt at the top of the browser, directing the browser to send a request for data.[94] If the address entered is correct, the web server will respond with data that the user's browser then reassembles into a webpage.[95]

This process is open to all. The computer doesn't care who drops by. By default, all visitors get service. In the language of the computer science literature, there is no authentication requirement.[96] A visitor might be any one of the billion or so Internet users around the world. For that matter, the visitor doesn't need to be a person. It could be a "bot," a computer program running automatically. It could even be a dog, as the famous *New Yorker* cartoon reminds us.[97] Because there is no authentication requirement, the web server welcomes all, and the norm is openness to the world. Access is inherently authorized.

The open nature of the Web is no accident; it is a fundamental part of the Web's technological design. From its inception in 1969, the creators of the Internet used "Requests for Comments" (RFCs) to describe the basic workings of different Internet protocols.[98] The Internet Engineering

---

858 (9th Cir. 2012) (en banc). That is, a person who violates a trespass norm to gain access to a computer commits an access without authorization if he has no authorization to access the computer, while he exceeds authorized access if he violates a trespass norm to gain a new level of access to a computer that he has some prior authorization to access. Both prohibitions implicate the trespass norms discussed in this Essay in the same way. The only difference is whether the defendant had some prior authorization to access the computer before violating the trespass norm. See Orin S. Kerr, Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes, 78 N.Y.U. L. Rev. 1596, 1662–63 & n.283 (2003) [hereinafter Kerr, Cybercrime's Scope] (advocating such interpretation). For these reasons, my proposed approach applies equally to acts that constitute access without authorization and acts that exceed authorized access.

94. Preston Gralla, How the Internet Works 21–23, 31 (1998).

95. Id.

96. See generally William E. Burr, Donna F. Dodson & W. Timothy Polk, Nat'l Inst. of Standards & Tech., NIST Special Pub. 800-63, Version 1.0.2, Electronic Authentication Guideline (2006) (providing technical guidance to federal agencies on electronic authentication of users over open networks). Authentication requirements can be added, which changes the analysis. See infra section III.C (discussing implications of authentication requirements).

97. See Peter Steiner, Cartoon, On the Internet, Nobody Knows You're a Dog, New Yorker, July 5, 1993, at 61.

98. See Stephen D. Crocker, Opinion, How the Internet Got Its Rules, N.Y. Times (Apr. 6, 2009), http://www.nytimes.com/2009/04/07/opinion/07crocker.html (on file with the *Columbia Law Review*) (explaining history, function, and significance of RFCs).

Task Force later took over the task of crafting RFCs, and they stand as the definitive technical discussion of the intended function of different Internet applications. Think of them as computer-geek manuals for how the Internet works. The RFCs for the Web are RFC1945 and RFC2616.[99] They teach how the Web works, or more specifically, they teach how "Hypertext Transfer Protocol" (HTTP) works;[100] HTTP is one of the foundational protocols controlling data transfer between web servers and clients. And a quick review of the RFCs for the Web shows its inherently open nature.

RFC1945 and RFC2616 describe the protocol used for the Web as "a generic, stateless, object-oriented protocol"[101] for "distributed, collaborative, hypermedia information systems."[102] The means of operation are general and open. The Web works by allowing anyone to make a request for a webpage. As summarized in the RFCs, "[a] client establishes a connection with a server and sends a request to the server in the form of a request method, URI, and protocol version, followed by a MIME-like message containing request modifiers."[103] In English: Anyone can send a request without any authentication. And then, "the server responds with a status line, including the message's protocol version and a success or error code, followed by a MIME-like message containing server information, entity metainformation, and possible body content."[104] Again, in English, the server responds to anyone who has made the request.

The protocols of the Web make websites akin to a public forum. To draw an analogy, websites are the cyber-equivalent of an open public square in the physical world. A person who connects a web server to the Internet agrees to let everyone access the computer much like one who sells his wares at a public fair agrees to let everyone see what is for sale. Sellers who want to keep people out, backed by the authority of criminal trespass law, shouldn't set up shop at a public fair. Similarly, companies that want to keep people from visiting their websites shouldn't connect a web server to the Internet and configure it so that it responds to every request. By choosing to participate in the open Web, the website owner must accept the open trespass norms of the Web.

B. *Authorized Access on the Web*

Although the Web is open by default, website operators often place limits and restrictions on access to information. The challenge for courts

99. T. Berners-Lee et al., Network Working Grp., Request for Comments: 1945, Internet Engineering Task Force (2006), http://tools.ietf.org/html/rfc1945 [http://perma.cc/PS74-4C3A] [hereinafter RFC1945]; T. Berners-Lee et al., Network Working Grp., Request for Comments: 2616, Internet Engineering Task Force (1999), http://www.ietf.org/rfc/rfc2616.txt [http://perma.cc/7MJN-PWFK] [hereinafter RFC2616].

100. RFC1945, supra note 99, at 1; RFC2616, supra note 99, at 1.

101. RFC1945, supra note 99, at 1.

102. RFC2616, supra note 99, at 7.

103. RFC1945, supra note 99, at 6.

104. Id. at 6–7.

is to distinguish provider-imposed restrictions and limits that are at most speed bumps (that cannot trigger trespass liability) from the real barriers to access (that can). In my view, an authentication requirement draws the proper line. When a limit or restriction does not require authentication, access is still open to all. The limit should be construed as insufficient to overcome the open nature of the Web. On the other hand, access that bypasses an authentication gate should, under proper circumstances, be deemed an unauthorized trespass. An authentication requirement provides a clear and easy-to-apply standard that both protects privacy and carves out public-access rights online.

A decade ago, I argued that unauthorized access should be limited to access that circumvents "code-based restrictions," which I defined as ways of tricking the computer into "giving the user greater privileges" when "computer code" has been used "to create a barrier designed to block the user from exceeding his privileges on the network."[105] With the benefit of hindsight, that formulation was vague. Trying to figure out when access circumvented a code-based restriction proved harder than I predicted. I now see that the more precise way to formulate the standard is that unauthorized access requires bypassing authentication. The key point is not that some code was circumvented but rather that the computer owner conditioned access on authentication of the user and the access was outside the authentication. This section covers examples of limits and restrictions on access that do not require authentication and should not trigger trespass liability.

Begin with a relatively simple case. Access to a website should be authorized even if the webpage address is not published or is not intended to be widely known. This issue arose in *United States v. Auernheimer*, in which the federal government charged the defendant with violating the CFAA by using a webscraper that queried website addresses that the computer owner, AT&T, had not expected people to find.[106] The website addresses queried were very difficult to guess because they ended in a long serial number. The defendant helped design a program to guess the numbers and collected information from over 100,000 website addresses.[107]

Had the Third Circuit reached the question,[108] it should have held that these website visits were authorized because the website had imposed no authentication requirement. The open norm of the Web still governed. Content published on the Web is open to all. Because the Web allows anyone to visit, a website owner necessarily assumes the risk that information published on the Web will be found. A hard-to-guess URL is

105. Kerr, Cybercrime's Scope, supra note 93, at 1644–46.

106. 748 F.3d 525, 530–31 (3d Cir. 2014) (presenting facts of case and criminal charges).

107. Id. at 531.

108. The Third Circuit did not reach the authorization question, as the court reversed the conviction on venue grounds. See id. at 532.

still a URL, and the information posted at that address is still posted and accessible to the world. Accessing the URL does not violate a trespass norm because all users are implicitly invited to access a publicly accessible address.

This conclusion is bolstered by the social value and ubiquitous nature of websurfing together with the severity and chilling effect of criminal punishment. We think, and therefore we Google. Courts should not lightly conclude that visiting an unwelcome URL should subject a person to arrest by federal agents and the potential for jail time. That is a particularly sensible approach because what looks like a hard-to-guess URL to a person may not seem hard to guess for a computer. To a computer, an address is an address. Even complicated addresses are easy for computers to find. Consequently, there is no workable line between an "easy" URL that can be accessed and one so hard to guess that access is implicitly forbidden.

The open understanding of the Web should also control access that violates terms of use.[109] Many websites come with terms of use that may on their face say when users are permitted to access the website.[110] The conditions can be arbitrary. One site might say that users must be eighteen years old to visit; another might say that users must agree to be polite.[111] Such terms should not be understood as controlling authorization. Access regulated only by written terms is not authenticated access. Everyone is let in, just subject to contractual restrictions. Such written terms should be understood as contractual waivers of liability rather than barriers to access.

This understanding is backed by the understandings of most website owners and users. Lawyers draft terms of use to minimize liability.[112] Broad terms allow computer owners to take action against abusive users and show good faith efforts to stop harmful practices occurring on the site.[113] True, terms of use may be drafted by lawyers to read like limitations on access. But companies do not actually expect the many visitors to otherwise-public websites to comply with the terms by keeping themselves

---

109. This was the issue first raised in United States v. Drew, 259 F.R.D. 449, 451 (C.D. Cal. 2009) ("This case raises the issue of whether . . . violations of an Internet website's terms of service constitute a crime under the [CFAA]." (footnote omitted)). Full disclosure: I represented Drew.

110. See United States v. Nosal, 676 F.3d 854, 861–62 (9th Cir. 2012) (providing examples).

111. See id. (listing specific details of various terms of use).

112. Consider this legal advice for franchisors who create websites:

> If a franchisor does decide to operate a site where it allows others to post content, it must address a number of issues. For example, it must take steps to avoid liability for copyright infringement, defamation, violation of privacy rights, and misappropriation of "hot news" and even criminal charges associated with such postings. It should, therefore, develop and publish comprehensive terms of use that prohibit inappropriate postings . . . .

Powell & Ralls, supra note 67, at 235 (footnotes omitted).

113. Id.

out.[114] And because terms can be arbitrary, violating them implies no culpable conduct.[115] If a public website has terms prohibiting access by people who are left-handed and enjoy opera, a left-handed opera lover who visits the site anyway does not deserve arrest and jail time.

This understanding is also backed by the experience of most computer users. Studies suggest that very few Internet users read terms of use.[116] (For the record, I don't.) Few users could understand them if they tried. Terms of use are often lengthy and filled with legalese.[117] The terms can be hard to find and difficult to interpret. Such terms don't restrict access to a computer any more than a standard waiver of rights on the back of a baseball game ticket could control rights to enter the ballpark. Violating the terms on the ticket might change your legal rights to sue the ballpark if something goes wrong, but it doesn't make your entry to the ballpark a trespass. Similarly, violating terms of use while accessing a website should not render the access a computer trespass.

The same rule should apply to the use of cookies to record prior visits and prompt paywalls. Cookies are pieces of code that websites can place on a browser to customize the user's experience.[118] Websites can use cookies to prompt repeat visitors to subscribe rather than visit for

---

114. In the *Drew* prosecution, for example, the government charged Drew with having participated in the creation of a MySpace profile that was not truthful in violation of MySpace's Terms of Use. *Drew*, 259 F.R.D. at 452 (listing charges on indictment, including setting up profile of "16 year old male juvenile named 'Josh Evans'"). Although the government presented the use of MySpace in violation of the terms as a trespass, it turned out that the co-founder of MySpace, Tom Anderson, whose MySpace profile greeted every new user, lied about his age in his own profile in violation of MySpace's Terms of Use. See Jessica Bennett, MySpace: How Old Is Tom?, Newsweek (Oct. 27, 2007, 11:22 AM), http://www.newsweek.com/myspace-how-old-tom-103043 [http://perma.cc/8FZS-28ZD] (reporting on Anderson's false age on his profile).

115. See Kerr, Cybercrime's Scope, supra note 93, at 1657–58 ("[A] qualitative difference exists between the culpability and threat to privacy and security raised by breach of a computer use contract on one hand, and circumvention of a code-based restriction on the other.").

116. According to one study, only 1.4% of users fully read end user license agreements (EULAs) for software programs, even though they require explicit agreement and generally require the user to claim she read the agreement. See Jens Grossklags & Nathan Good, Empirical Studies on Software Notices to Inform Policy Makers and Usability Designers, http://people.ischool.berkeley.edu/~jensg/research/paper/Grossklags07-USEC.pdf [http://perma.cc/VP8S-RGVF] (last visited Jan. 26, 2016). The readership of terms of use on a website is likely much lower, as readers ordinarily are not prompted to do so and are less likely to see visiting a website as a significant occasion.

117. See Aleecia M. McDonald & Lorrie Faith Cranor, The Cost of Reading Privacy Policies, 4 I/S: J.L. & Pol'y for Info. Soc'y 543, 565 (2008) (concluding it would take hundreds of hours for typical consumer to actually read privacy policies encountered in one year of typical Internet use).

118. See In re Google Inc. Cookie Placement Consumer Privacy Litig., 988 F. Supp. 2d 434, 439–40 (D. Del. 2013) ("Cookies are used in internet advertising to store website preferences, retain the contents of shopping carts between visits, and keep browsers logged into social networking services and web mail as individuals surf the internet.").

free. Consider the popular *New York Times* website, nytimes.com. When you visit the *Times* website, it places a cookie on your browser that records the visit.[119] The cookie allows the *Times* to meter access: If a browser is used to visit more than ten stories on the site in a month, the website brings up a screen blocking the reading of additional articles.[120] The point of the block is to pressure frequent readers to buy a subscription. But what if a reader regularly clears out his browser, which erases the cookie and enables unlimited access?[121] Is accessing the site after clearing out the browser unauthorized?

The answer should be that access enabled by erasing cookies is still authorized. Browsers are designed to give users control over what cookies are stored on their browsers.[122] Such cookies do not authenticate users: They merely allow users to customize their browsing experience. Users can accept cookies, reject cookies, or clear out the cookies kept in their browsers as often as they like.[123] They can use different browsers or different computers. As a result, user control of cookies is an expected and common way to use the Internet. They do not really limit access to computers; they only complicate access to the text of particular stories. Access limitations based on cookies are at most speed bumps rather than barriers. Instead of keeping people out, cookies-based barriers only impose enough of a hassle to encourage some users to buy a subscription.[124] Only the most unsophisticated users will see cookies as a barrier, and it will only be because they don't yet understand how cookies work.[125]

A more difficult case is raised by IP address blocking, which was the issue in *Craigslist v. 3Taps*.[126] Every device connected to the Internet has

---

119. Amit Agarwal, How to Bypass the *New York Times* Paywall (July 15, 2013), http://www.labnol.org/internet/nyt-paywall/18992 [http://perma.cc/R6XH-2GKD].

120. Id.

121. See id. (describing how to bypass *New York Times* paywall by deleting cookies).

122. This is the case with traditional browser cookies, at least. Different kinds of cookies may present different issues. See, e.g., Paul Lanois, Privacy in the Age of the Cloud, 15 J. Internet L. 3, 5 (2011) (discussing flash cookies).

123. For example, in the popular Chrome browser, users can go into "incognito" mode, which will not store cookies. Alternatively, they can delete all of the cookies stored on their browsers. See Laura, Google, Manage Your Cookies and Site Data, Chrome Help, http://support.google.com/chrome/answer/95647?hl=en [http://perma.cc/W262-45MU] (last visited Jan. 26, 2016) (describing how to delete cookies). Each step takes only seconds and is a common and expected part of surfing the Web.

124. See Danny Sullivan, The Leaky *New York Times* Paywall & How "Google Limits" Led to "Search Engine Limits," Search Engine Land (Mar. 22, 2011, 4:45 AM), http://searchengineland.com/leaky-new-york-times-paywall-google-limits-69302 [http://perma.cc/DW9Y-8KVZ] (describing shortcoming of *New York Times* paywall system).

125. The same principle also applies to browser restrictions based on "user agents," an issue that arose but was not resolved in the *Auernheimer* case. See Appellant's Amended Reply Brief at 13–14, United States v. Auernheimer, 748 F.3d 525 (3d Cir. 2014) (No. 13-1816), 2013 WL 6825411 ("Changing the user agent does not make a person guilty of trespass, whether that trespass is a physical trespass or the cyber trespass of the CFAA.").

126. 964 F. Supp. 2d 1178 (N.D. Cal. 2013).

an IP address, which is a number that represents the Internet address of that device.[127] Web servers communicate with users on the Internet by receiving requests and sending data to them at their IP addresses. In *3Taps*, the defendant business scraped ads from Craigslist and republished them on its own website.[128] Craigslist responded by sending 3Taps a cease-and-desist letter and by blocking the IP addresses associated with 3Taps's computers.[129] 3Taps changed its IP addresses to circumvent the IP block. Judge Charles Breyer ruled that 3Taps's access was an unauthorized access under the CFAA because "[a] person of ordinary intelligence would understand Craigslist's actions to be a revocation of authorization to access the website."[130] Judge Breyer explained:

> IP blocking may be an imperfect barrier to screening out a human being who can change his IP address, but it is a real barrier, and a clear signal from the computer owner to the person using the IP address that he is no longer authorized to access the website.[131]

Judge Breyer is wrong. Understood in the context of the open Web, an IP block is not a real barrier. A user's IP address is not fixed. For many users, the IP addresses of their devices will change periodically during normal use.[132] Using multiple computers often means using multiple IP addresses. A person might surf the Web from his phone (using his cell phone's IP address), from his laptop at home (using his home connection's IP address), and from work (using the company's IP address). Users also can easily change their IP addresses if they wish. For some users, turning on and off their modems at home will lead their IP addresses to change.[133] For more sophisticated users, accessing the Web using Tor or a virtual private network allows them to change their IP addresses with the click of a button.[134] There is nothing untoward or blameworthy about using different IP addresses. It is a routine part of using the Internet.

Because of these technical realities, bypassing an IP block is no more culpable than bending your neck to see around someone who has temporarily blocked your view. To be sure, an IP block indicates that the com-

---

127. E.g., id. at 1181 n.2.

128. Id. at 1180.

129. Id. at 1180–81.

130. Id. at 1186.

131. Id. at 1186 n.7.

132. Why Does Your IP Address Change Now and Then?, What Is My IP Address, http://whatismyipaddress.com/keeps-changing [http://perma.cc/QE8N-KDLB] (last visited Jan. 26, 2016).

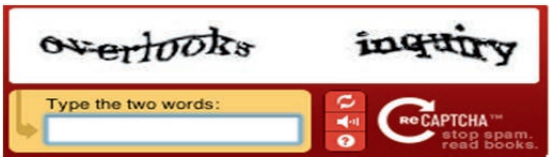
133. See How to Change Your IP Address, What Is My IP Address, http://whatismyipaddress.com/change-ip [http://perma.cc/9GLE-73RK] (last visited Jan. 26, 2016) (noting turning modem off and then back on will sometimes change IP address).

134. See Quentin Hardy, VPNs Dissolve National Boundaries Online, for Work and Movie-Watching, N.Y. Times: Bits Blog (Feb. 8, 2015, 5:30 AM), http://bits.blogs.nytimes.com/2015/02/08/in-ways-legal-and-illegal-vpn-technology-is-erasing-international-borders/ (on file with the *Columbia Law Review*) ("Millions of people around the world now pay for virtual private computer networks . . . to hook into a server in the United States.").

puter owner does not want at least someone at that IP address to visit the website. But that subjective desire is not enough to establish a criminal trespass in light of the open nature of the Web. A computer owner cannot both publish data to the world and yet keep specific users out just by expressing that intent. It is something like publishing a newspaper but then forbidding someone to read it. Publishing on the Web means publishing to all, and IP blocking cannot keep anyone out. Merely circumventing an IP block does not violate trespass norms.

A particularly tricky case is access that circumvents a CAPTCHA, an issue that arose in *United States v. Lowson*.[135] CAPTCHA is an acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart."[136] You have probably seen CAPTCHAs when buying tickets online or posting online comments. The website presents you with an image like this requiring you to type in the words before you can proceed:[137]

FIGURE 1: CAPTCHA EXAMPLE



The purpose of the CAPTCHA, as the full name suggests, is to allow humans in but to block computer "bots" that can make thousands of automated requests at once.[138]

The interesting question is whether use of an automated program to bypass the CAPTCHA by guessing or reading the words is an unauthorized access. The question is difficult because the technology shares some characteristics of a traditional authentication gate but not others. Like a password gate, it requires a code to be entered; but unlike a password gate, it presents the code to the user. Although it's a close case, I think the better answer is that automated bypassing of a CAPTCHA is not itself an unauthorized access. Although the CAPTCHA *looks* like a password gate, it does not operate like one. The site tells everyone the password. It invites all to enter.

---

135. No. 10-114 (KSH), 2010 WL 9552416 (D.N.J. Oct. 12, 2010).

136. E.g., Craigslist, Inc. v. Naturemarket, Inc., 694 F. Supp. 2d 1039, 1048 (N.D. Cal. 2010).

137. See CAPTCHA: Telling Humans and Computers Apart Automatically, CAPTCHA, http://www.captcha.net/ [http://perma.cc/9FHM-C62D] (last visited Jan. 26, 2016) (using this image as sample).

138. See id. (explaining usefulness of CAPTCHAs).

It is tempting to think that a CAPTCHA authenticates users as people instead of bots. But a "bot" request is still ultimately a request from a person. It is merely an automated request, with the person who used the software still responsible. That person could gain access and bypass the CAPTCHA manually by visiting the page and typing in the string of numbers that appear. As a result, a CAPTCHA is best understood as a way to slows a user's access rather than as a way to deny authorization to access. The CAPTCHA is a speed bump instead of a real barrier to access. Courts should hold that automated access is not a trespass merely because it bypasses a CAPTCHA.

Finally, it is worth considering the business implications of my proposed trespass rules. The examples in this section mostly involve businesses that might try to control customer use of their computers for business reasons. A ticket seller might use a CAPTCHA to limit scalpers, for example, just like the *New York Times* might use cookies to encourage readers to purchase subscriptions. That raises a fair question: If courts hold that these methods do not constitute a trespass, would that prevent businesses from using these methods—and if so, is that a policy reason to adopt different trespass norms?

The answer is that criminal trespass liability is unlikely to impact business strategies. Companies can already use civil contract law, based on terms of use, to set legal limits on how visitors use their websites.[139] Companies may not want to enforce those limits for a range of reasons.[140] But at least as a matter of law, often they can.[141] The scope of computer trespass laws implicates a different question: not just what user conduct is legal but what user acts are *criminal*. As a practical matter, it's hard to imagine a company using a business model that depends substantially on the prospect of the police arresting and prosecuting customers who circumvent speed bumps designed to regulate website use. Jailing customers for using a website isn't likely to be a good business strategy. It is telling that when the government has pursued aggressive criminal charges under the CFAA for use of websites, it has often been without the support of the companies claimed as victims.[142]

---

139. See, e.g., Ward v. TheLadders.com, Inc., 3 F. Supp. 3d 151, 162 (S.D.N.Y. 2014) (denying motion to dismiss in contract claim brought under website terms of use); Cvent, Inc. v. Eventbrite, Inc., 739 F. Supp. 2d 927, 937–38 (E.D. Va. 2010) (evaluating contract claim based on website terms of use).

140. Suing customers is costly and can trigger negative press attention, making such suits rare even if website misuse is common.

141. See, e.g., *Ward*, 3 F. Supp. 3d at 162 (denying motion to dismiss claim based on violation of website's terms of use).

142. For example, in the Lori Drew case, which involved a CFAA prosecution for violating MySpace's Terms of Use, MySpace remained curiously silent throughout the case. See, e.g., Scott Glover & P.J. Huffstutter, 'Cyber Bully' Fraud Charges Filed in L.A., L.A. Times (May 16, 2008), http://articles.latimes.com/2008/may/16/local/me-myspace16 [http://perma.cc/6QY3-M9DX] (reporting on Drew's indictment and noting MySpace had not responded to request for comment). In the *Auernheimer* case, the victim, AT&T, was

C. *Unauthorized Access on the Web and the Authentication Requirement*

In contrast to the examples above, bypassing an authentication requirement should trigger liability for computer trespass. Even open spaces often have closed subspaces. Like a store open to the public in the front but for employees only in the back, the Web can have real barriers through which access violates trespass norms and is unauthorized. This moves the norms question from the first inquiry of the nature of the space to the second inquiry of the types of permitted entry. What counts as a real barrier on the Web, and what ways of overcoming those barriers are authorized? When a user bypasses an authentication requirement, either by using stolen credentials or bypassing security flaws to circumvent authentication, access should be considered an unauthorized trespass. This standard harnesses criminal law to protect privacy when network owners use technical means to enable access only to specific authenticated users.

The basic principle of authentication is probably intuitive to most Internet users. Every Internet user is familiar with the notion of an account that limits access. The requirement of credentials to identify the user is an authentication requirement.[143] When access to a computer requires an account, the user must register and obtain login credentials such as a username and password. Before allowing the user to access specific information, the user must establish that he is someone with special rights to access the account. A user who cannot satisfy the authentication requirement is blocked from access. The account structure imposes an access control that separates the insiders with accounts from outsiders without them. Because only the account holder should be able to satisfy the authentication requirement, the world—minus one user—is blocked. An authentication requirement creates a technical barrier to access by others. It carves out a virtual private space within the website or service that requires proper authentication to gain access.

Authentication requirements should be understood as the basic requirement of a trespass-triggering barrier on the Web. By limiting access to a specific person or group, the authentication requirement imposes a barrier that overrides the Web default of open access. The norm shifts from open to closed. At that stage, the emphasis shifts to means of access.

---

also quiet: At sentencing, when the probation office asked AT&T to detail its losses at sentencing, AT&T declined to respond. Brief of Defendant-Appellant at 52, United States v. Auernheimer, 748 F.3d 525 (3rd Cir. 2014) (No. 13-1816), 2013 WL 3488591. In the Aaron Swartz case, the victim, JSTOR, actively opposed the prosecution. See, e.g., Zach Carter et al., Aaron Swartz, Internet Pioneer, Found Dead Amid Prosecutor 'Bullying' in Unconventional Case, Huffington Post (Jan. 13, 2013), http://www.huffingtonpost.com/2013/01/12/aaron-swartz_n_2463726.html [http://perma.cc/VXS8-W4LM] ("JSTOR opposed prosecuting Swartz . . . .").

143. See generally William E. Burr, Donna F. Dodson & W. Timothy Polk, Nat'l Inst. of Standards & Tech., Electronic Authentication Guideline 12–13 (2006), http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf [http://perma.cc/VXS8-W4LM] (noting credentials are required part of e-authentication process).

Much like with a physical key to a door, access is authorized to the person who was given the password. On the other hand, as the *Morris* court noted, gaining access by guessing a password is just like picking a lock; both lack authorization.[144]

Exploits that circumvent authentication mechanisms or otherwise "break in" to systems are similarly unauthorized. *Morris* is again instructive. Access enabled by an exploit that uses a command in a way contrary to its intended function is unauthorized, much like entering through a window or a chimney in the physical world. For example, hacking techniques such as SQL injection attacks are unauthorized and illegal.[145] A Structural Query Language (SQL) injection attack is executed by attaching special extra language to the end of a web request.[146] Some web servers are misconfigured so that this extra language will execute a command on the web server rather than return a webpage.[147] The special command can provide access to the private database on the web server rather than just the pages to be published, providing the attacker with means to retrieve, alter, or delete the data.[148] Although a hacker using an SQL injection attack executes the injection by entering a command into a web browser—just like one would enter a username or password—the act exploits a security bug or hole just like the SENDMAIL flaw used in *Morris*. Access using an SQL injection is unauthorized for the same reason. An SQL injection attack is contrary to the intended function of the web browser: It violates the trespass norms surrounding the proper means of access to information on the server.

Importantly, the application of trespass norms can be technologically arbitrary even if they are socially meaningful. Consider the role of session cookies and persistent login cookies, which are browser cookies generated on a user's web browser during a typical login process to a website.[149] The website generates a long number associated with that login and passes the information back to the user's browser, with instructions for the browser to store it as a cookie.[150] When the user subsequently visits the website, the browser passes along the unique session-cookie value back to the website. Websites then use this information to automatically log in the user. You have likely benefited from these cookies when using web-based email, Amazon, or Facebook. After not visiting the page

144. United States v. Morris, 928 F.2d 504, 509 (2d Cir. 1991).

145. Claridge v. RockYou, Inc., 785 F. Supp. 2d 855, 858 (N.D. Cal. 2011).

146. E.g., Josh Shaul, Why Do SQL Injection Attacks Continue to Succeed?, SC Mag. (May 24, 2011), http://www.scmagazine.com/why-do-sqlinjectionattacks-continue-to-succeed/article/203679/ [http://perma.cc/PM4C-TECV].

147. Id.

148. Id.

149. Michael R. Siebecker, Cookies and the Common Law: Are Internet Advertisers Trespassing on Our Computers?, 76 S. Cal. L. Rev. 893, 897 (2003).

150. See id. at 897–90 (outlining process by which cookies are placed on computers, how they work once deposited, and purposes they serve).

for a few minutes or even a few days, you can go back to the website and it will automatically log you in. The website does this by reading your stored login or session cookie and matching it to an ongoing known login session.[151]

Now consider how computer trespass principles might apply to access made by hijacking such information. Imagine a third party intercepts a login cookie sent over the Web, loads it into his own browser, and visits the website. Use of the cookie will automatically log the third party into the user's email or Facebook account without the user's permission or knowledge. Is the third-party access authorized because it was obtained merely by sending on a specific cookie value as part of the browser's web request? Or is it unauthorized because it does so in a way that bypasses an authentication gate?

Unauthorized use of a persistent login cookie should be considered a violation of trespass norms. The cookie acts as a temporary password, tied to the user's permanent password, that identifies the account and provides access to it. It circumvents the password gate in exactly the same way that entering the permanent username and password would. The fact that the cookie is sent by the browser, which is normally an environment controlled by the user for the user's benefit, should not lead to a different result. This kind of cookie is an exception to the usual rule because it is a password; the embedding of the password in the browser does not change its function as a password.

The lines here are subtle, to be clear. Recall the *Auernheimer* case, where the information posted on a website was available only at a hard-to-guess website address.[152] The difference between a hard-to-guess website address, which should not act as an authentication gate, and a hard-to-guess session cookie, which should, is a matter of social understanding rather than technology. We can draw plausible lines about what acts as a password, but at some level the differences will boil down to shared understandings that some information is part of a public address while other information is a unique identifier. In close cases the technological arbitrariness is inevitable, as trespass norms are ultimately shared views about what invades another's private space and what doesn't. Technology alone cannot provide the answer.[153]

---

151. After a period of inactivity, the session may expire and the session cookie no longer works. At that point, the user must enter in the username and password to log in.

152. See supra notes 50–53 (discussing *Auernheimer* facts and issues).

153. Good security practices can help avoid the murkiest cases, however. For example, imagine a website required users to enter a secret password to enter the site but announced that the password was either "red" or "green." Such an example blurs the line between speed bump and authentication gate. But it is easy for website owners to avoid the blurry lines simply by having better authentication practices.

IV. CANCELED, BLOCKED, AND SHARED ACCOUNTS

The next set of questions asks how computer trespass statutes should apply to canceled, blocked, and shared accounts. These questions implicate the third way that norms control trespass, the identification of norms governing the context of permitted access. At this stage, authentication clearly implicates trespass liability. If a stranger guesses a victim's username and password and enters those credentials to access her account without permission, that access is plainly unauthorized.[154] On the other hand, if the user enters her own credentials to access her own private account, that access is authorized. The hard cases lie between these two poles.

The gray area involves three basic problems. First, a computer owner might revoke the user's right to access an account but not close the account. If the credentials still work, and the user continues to access the account using them, is that access authorized or unauthorized? Second, a computer owner might cancel access to a user's account, and the user might then respond by creating a new account on the same system unbeknownst to the owner. Is use of the new account authorized or unauthorized? Third, an account holder might share her username and password with a third party who accesses the account. Is the third-party access authorized because it was by permission of the account holder, or is it unauthorized because it was not actually accessed by the account holder? In these cases, the law must grapple with how authorization norms apply when account rights are terminated, modified, or shared with others.

This Part attempts to answer all three questions using the principle of authentication. As explained in Part III, authentication of a user authorizes the user to access the account but makes access by others unauthorized. The trespass norm should aim to preserve that delegation of authority. Again, the goal is to achieve an optimal balance. Overly restricting delegations would prevent beneficial uses of networks by authenticated users. On the other hand, permitting authenticated users to further delegate authority, or to ignore withdrawals of delegation, would nullify the owner's power to designate who can access the network. Applying this approach suggests three rules. First, suspending an account withdraws authorization to access the account. Second, a suspension may or may not signal that access to additional accounts is prohibited. Finally, use of shared passwords should be permitted only when the third party access is within the scope of agency of the authenticated user.

This Part concludes by discussing the role of mental states, or mens rea, on computer trespass liability. When authorization hinges on the context of access, the user often will not know the facts that determine whether access was authorized. In that context, the statutory requirement

---

154. See United States v. Morris, 928 F.2d 504, 511 (2d Cir. 1991) (discussing "unauthorized access" requirement).

that unauthorized access must be intentional or knowing plays an important role in narrowing criminal liability.

A. *Canceled Accounts*

The first issue is how trespass laws should apply when the authority to use an account has been revoked but the user accesses the account anyway. The answer should come from an understanding of what authentication means. By permitting an account that requires authentication, the computer owner should be understood to have delegated access rights to the authenticated user. The authenticated user has permission to access the account so long as the computer owner grants the account. The trespass norm should be to preserve that delegation. Preserving the delegation achieves the same dual goals as the authentication requirement provided in Part III. It enables use of computers (here, accounts held by authorized users) while affording them appropriate space to use their delegated accounts without fear of criminal prosecution for trespass.

Under this standard, the owner's revocation of the right to use an authenticated account revokes authorization. When the computer owner communicates the revocation to the user, the delegated authority ends. Subsequent account access violates trespass norms; it should be understood as entering a space where the user is no longer welcome. Because authority to use an authenticated account should exist only inside the zone of delegated power, ending the right to access the account should end the delegated right and end the authorization.

Courts have so far adopted this approach, as the Fourth Circuit's decision in *United States v. Steele*[155] demonstrates. Robert Steele worked as a backup system administrator at a business named SRA, and for work purposes he created a backdoor account that gave him access to SRA's network files.[156] After he resigned, Steele continued to use the account to access SRA's network. The Fourth Circuit ruled that "the fact that Steele no longer worked for SRA when he accessed its server logically suggests that the authorization he enjoyed during his employment no longer existed."[157] Having left the company, Steele's rights to access the account were revoked: "Just because SRA neglected to change a password on Steele's backdoor account does not mean SRA intended for Steele to have continued access to its information."[158]

---

155. 595 F. App'x 208 (4th Cir. 2014).

156. Id. at 209–10.

157. Id. at 211.

158. Id. For a similar case reaching the same result, see United States v. Shahulhameed, No. 14-5718, 2015 WL 6219237, at *2 (6th Cir. Oct. 22, 2015) (holding employee's authorization to access his work account ended when he was informed by telephone and email that he was fired). The point was assumed by the parties and apparently accepted by the court in LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1136 (9th Cir. 2009) (noting

This approach implies a distinction between the rules that should apply to a user who violates terms of use and a user whose account is suspended for violating terms of use. Recall that a user who violates terms of use is not committing an unauthorized access.[159] On the other hand, I argue here that a user whose account is revoked for violating terms of use but uses the banned account anyway is guilty of trespass. The distinction is justified because violating terms of use merely provides legal justification for revocation if the website owner chooses to do so. When a website owner authorizes an account for a user, the user has access rights unless the account is actually revoked. The authority is delegated by the issuing of the account and withdrawn by its revocation, so the act of revocation is needed to undo the act of granting the account.

B. *New Accounts Following the Banning of an Old Account*

Next imagine that the computer owner cancels or blocks the account but the user can readily sign up for a new one. Imagine Gmail suspended your email account for violating Gmail's terms of use and you want to open another Gmail account the next day or the next year. Does the company's blocking the first account deny authorization to set up a second account? Or is the user free to start again after having been blocked once—or twice, or three times, or even hundreds of times?

This problem arose in the controversial case of *United States v. Swartz*.[160] The Internet activist Aaron Swartz created a guest account on MIT's network and used it to download a massive number of academic articles to his laptop.[161] Network administrators canceled the guest account in response; Swartz created a new guest account.[162] When system administrators blocked access through the new guest account, Swartz then figured out a way to circumvent guest-account registration: He found a closet in the basement of one of MIT's buildings that stored the server, entered it, and hard-wired his computer to the network.[163] He then assigned himself two new IP addresses from which he could con-

---

"[t]here is no dispute" that if employee accessed company computer after leaving company then employee "would have accessed a protected computer 'without authorization' for purposes of the CFAA").

159. See *Morris*, 928 F.2d at 511 (discussing meaning of "unauthorized access").

160. Indictment, United States v. Swartz, Cr. 11-ER-10260 (D. Mass. July 14, 2011). Swartz committed suicide before his case went to trial. John Schwartz, Internet Activist, a Creator of RSS, Is Dead at 26, Apparently a Suicide, N.Y. Times (Jan. 12, 2013), http://www.nytimes.com/2013/01/13/technology/aaron-swartz-internet-activist-dies-at-26.html (on file with the *Columbia Law Review*). I will assume the facts in the indictment are true.

161. Indictment at 4–5, United States v. Swartz, Cr. 11-ER-10260 (D. Mass. July 14, 2011).

162. See id. at 4 (noting computer was registered under "fictitious guest name 'Gary Host'").

163. See id. at 8–9 (describing observation of Swartz "entering the restricted basement network wiring closet" and "attempt[ing] to evade identification").

tinue his access.[164] The question was, did having been blocked with an account once mean that subsequent efforts to obtain access were unauthorized?

As before, the legal line should track the delegation of authority implied by authentication. The application of that principle is trickier, however, because the revocation of delegated authority is less obvious. When anyone can open an account, there is an implicit delegation to anyone who registers for a new account. In some contexts, a single act of blocking does not imply a total and permanent revocation. In other contexts, it does. For example, a user who has an account suspended for misconduct may be perfectly welcome to start again with a new account on the understanding that no further misconduct continues. On the other hand, users who are repeatedly banned eventually must get the message that they are not welcome.

The key question should be the objective signal sent by the banning or suspension, which will in some contexts allow the user to create a new account but in other contexts won't. When the ban would be reasonably interpreted as "don't do *that*," creating a new account and using it properly is authorized. When the ban would be reasonably interpreted as "go away and never come back," creating another account is unauthorized. In the *Swartz* case, for example, access would have been unauthorized by the time Swartz entered the closet to circumvent IP registration. Having had his accounts blocked multiple times by MIT's system administrators for violating the rules on MIT's network, Swartz had received clear signals that he was no longer welcome to create another account to continue the same conduct.

This approach once again ends up drawing a subtle distinction. Recall my earlier conclusion that an IP block is insufficient to trigger trespass liability.[165] Circumventing an IP address ban is permitted and authorized. At the same time, I am arguing here that if the computer owner requires an account to access a computer and then bans the account, circumventing that ban might not be authorized if the context can be interpreted as a complete ban. Is there really a difference? I think there is. Everyone can visit a public website, while not everyone can have the privilege of an account. By creating the access control of an account regime, the computer owner takes control of who can access it by making individualized decisions about specific accounts. A suspended account is not just a speed bump. It's a block to using that account and a potential signal about opening another one. The rules governing the two cases should be different.

---

164. Id. at 7–8.

165. See supra notes 126–134 and accompanying text (discussing trespass liability for circumventing IP blocks).

C. *Password Sharing*

The last and most difficult issue is identifying trespass norms that should govern shared passwords. Consider the facts of *United States v. Rich*.[166] A financial-services company, LendingTree, sold valuable access to financial information on its website to customers who paid a fee and received a username and password to access the site.[167] The defendant, Brian Rich, made a side deal with an employee at one of LendingTree's customers; he agreed to pay the employee to get the company username and password.[168] Rich then used the credentials to access the LendingTree website without paying LendingTree.[169] The question is: Does using a shared password constitute an unauthorized access in violation of trespass norms?

The starting point should again be that the computer owner's granting of an authenticated account delegated access rights to the account holder. The account holder is authorized but others are not. To preserve this principle, the trespass norm should be that access by the account holder or his agent is authorized while other access to the account is not.[170] When the account holder gives login credentials to a third party, access by the third party is authorized only when the third party acts as the agent of the account holder.

This approach mirrors the analogous rule in the physical world. When access is limited by a physical lock and key, whether entry is a physical trespass law depends on whether it falls within the zone of permission granted by the owner.[171] For example, in *Douglas v. Humble Oil & Refining Co.*, a business owner gave an employee the key to his home so the employee could feed his pets when he was away.[172] The employee later used the key to enter the home for a different reason. According to the court, this entry for reasons outside the scope of permission was a trespass.[173]

This approach allows computer account holders to share usernames and passwords with an agent. If the agent accesses the account on the account holder's behalf, the agent is acting in the place of the account holder and is authorized. The agent then has the same authorization

---

166. 610 F. App'x 334 (4th Cir. 2015).

167. Brief of Appellant at 3, *Rich*, 610 F. App'x 334 (No. 14-4774), 2015 WL 860788, at *9.

168. Id. at 4.

169. Id.

170. See generally Restatement (Third) of Agency § 1.01 (Am. Law Inst. 2006) (defining agent).

171. See, e.g., Rich v. Tite-Knot Pine Mill, 421 P.2d 370, 374 (Or. 1966) (noting "one who originally enters the premises as a licensee may forfeit his license and become a trespasser if he exceeds its scope").

172. 445 P.2d 590, 591 (Or. 1968) (en banc).

173. See id. ("The undisputed evidence was that the only purpose for which Douglas had authorized his employee to use the house key was to attend to the feeding of the Douglas's household pets.").

rights as the account holder. For example, I recently set up a Gmail account for my students to email class assignments. I gave my assistant the account password and asked her go into the email inbox and collect them for me. When she did so, she was acting as my agent. Legally speaking, she was me.[174] She was fully authorized to access the account in her capacity as my agent. Her conduct was authorized and legal, much like employee access to an employer's account for work purposes.

On the other hand, a third party who uses a password in pursuit of her own ends stands in the same place as a third party who has guessed or stolen the password. Consider the facts of *Rich*.[175] When Rich accessed the LendingTree website using a password, he was not acting as an agent of a legitimate customer. Rich paid for access to the password, but he did not pay LendingTree. Instead, he paid an employee of a legitimate customer. Rich accessed the account to help himself get richer, not to help the employee. From the perspective of LendingTree, Rich's access was no different from access using a guessed or stolen password. Rich was not a legitimate customer or an agent of a legitimate customer. Whether he obtained the password by stealing it from the employee or by paying for it makes no difference to LendingTree. For that reason, Rich's access was unauthorized.

Two wrinkles need to be ironed out. First, what is the impact of terms of use to the delegated authority of the computer owner? Recall my use of a Gmail account for class. What if Gmail's Terms of Use forbid password sharing and my secretary's access violates those Terms?[176] In my view, terms of use barring shared access should be irrelevant for the same reason they are irrelevant to access more generally. As explained earlier, terms of use create rights for the computer owner rather than the account holder.[177] When terms are violated, the computer owner can suspend or restrict the account. But violating the terms does not render access an unauthorized trespass either in the context of public access websites or of specific accounts. By granting a user an account, the computer owner necessarily grants the user authorization to access the account for any reason.

Second, note that my treatment of the delegation from the computer owner to an account holder is different from my treatment of the delegation from the account holder to a third party. When authorized by the computer owner, the account holder has full access rights. When au-

---

174. See State ex rel. Coffelt v. Hartford Accident & Indem. Co., 314 S.W.2d 161, 163 (Tenn. Ct. App. 1958) ("The basis for holding the principal for the acts of his agent is that the agent acts as the principal's *alter ego* or other self.").

175. United States v. Rich, 610 F. App'x 334, 335–36 (4th Cir. 2015).

176. They don't, at least right now. See Google Terms of Service, Google (Apr. 14, 2014), http://www.google.com/intl/en/policies/terms/ [http://perma.cc/7T2J-PEQL] (including warning to "keep your password confidential" but refraining from enacting formal requirement).

177. See supra section III.B (discussing legal implications of terms of use).

thorized by the account holder, on the other hand, the third party has narrower rights only to act as the account holder's agent. This distinction is justified by the underlying role of an authentication requirement. Setting up the authentication gate and granting a user account confers rights on the account holder and her agents. An account holder should have only a narrower power to confer access rights because otherwise that delegation would interfere with the original authentication. If computer owner A can confer access rights to account holder B, an unlimited power of B to confer access rights to C, D, and E would nullify A's judgment to confer access rights to only account holder B. The rule should be that third-party access outside the agency relationship is unauthorized access.

D. *The Critical Role of Mens Rea*

The problem of canceled, blocked, and shared accounts is not complete without understanding the associated mental state, or mens rea, that accompanies computer trespass statutes.[178] The problem here is with the fact-sensitive context of permitted entry. The facts relevant to authorization may not be known to the user. In this context, the mental state of authorization plays a critical role. Computer trespass statutes generally require that the user commit an intentional or knowing unauthorized access.[179] The government's burden to prove that an unauthorized access was intentional or knowing plays a crucial role in establishing a limit on liability when authorization is lacking due to the context of entry.

Courts have not explored the role of mental state in establishing liability for computer trespass, so it is important to understand what a mental state or knowledge or intent might mean in this context. Consider the broadest section of the CFAA, which prohibits "intentionally access[ing] a computer without authorization" or intentionally "exceeding authorized access."[180] The intent requirement plainly applies to the element that authorization is lacking. But does the requirement of intent with respect to lack of authorization require intent as to the legal conclusion that access is unauthorized, or does it merely mean intent as to the facts that make access legally unauthorized?

---

178. For an introduction to mens rea, see generally Joshua Dressler, Understanding Criminal Law 117–36 (6th ed. 2012).

179. See, e.g., 18 U.S.C. § 1030(a)(2) (2012) (prohibiting intentional access without authorization or exceeding authorized access); Cal. Penal Code § 502(c)(7) (West 2010) (prohibiting "access[] to "any computer, computer system, or computer network" that is "[k]nowing[] and without permission"); Colo. Rev. Stat. Ann. § 18-5.5-102 (West 2013) (prohibiting knowing access without authorization or exceeding authorized access).

180. 18 U.S.C. § 1030(a)(2).

Courts have not addressed the question, and it is surprisingly complex.[181] The usual rule, however, is that a knowledge or intent requirement for a criminal element requires knowledge or intent about the facts that are legally relevant to the element rather than to a legal status the element implies.[182] It is not entirely free from doubt that this rule applies to computer trespass statutes,[183] although it is often enough the default rule in federal criminal law that it seems likely to apply at least to the CFAA.[184] Applying the usual rule to computer trespass statutes, proving intentional unauthorized access likely requires the government to show that the defendant knew of or hoped for the facts legally relevant to authorization and intentionally accessed the computer anyway. The prosecution need not prove that the defendant knew or intended his conduct

---

181. See generally Kenneth W. Simons, Ignorance and Mistake of Criminal Law, Noncriminal Law, and Fact, 9 Ohio St. J. Crim. L. 487 (2012) (exploring difficulty raised by mental states with respect to criminal elements having aspects of both law and fact).

182. See, e.g., McFadden v. United States, 135 S. Ct. 2298, 2304 (2015) (holding, in prosecutions for knowingly distributing a controlled substance, government must prove either that defendant knew substance he distributed was on list of controlled substances or that defendant "knew the identity of the substance he possessed" and it was on the controlled-substances list); Elonis v. United States, 135 S. Ct. 2001, 2009 (2015) ("[A] defendant generally must know the facts that make his conduct fit the definition of the offense even if he does not know that those facts give rise to a crime." (citations omitted) (internal quotation marks omitted) (quoting Staples v. United States, 511 U.S. 600, 607 n.3 (1994))); Morissette v. United States, 342 U.S. 246, 271 (1952) ("He must have had knowledge of the facts, though not necessarily the law, that made the taking a conversion."); United States v. Brown, 669 F.3d 10, 19–20 (1st Cir. 2012) (ruling, in prosecution for intentionally thwarting officers in course of their official duties, it was irrelevant that defendant believed officers were enforcing unconstitutional law and that therefore officers were not acting in course of their official duties).

183. For example, in *Liparota v. United States*, the Court construed a statute that punished knowingly using or possessing food stamps in a way unauthorized by law as requiring knowledge that the use or possession was legally unauthorized. 471 U.S. 419, 433 (1985). Applying *Liparota*, it could be argued that intentional unauthorized access also requires intent—here, awareness or hope—about the act being legally unauthorized. This might be bolstered by the text of physical trespass statutes, which often plainly requires knowledge that presence is legally unauthorized. See, e.g., Model Penal Code § 221.2(2) (Am. Law Inst. 2015) ("A person commits an offense if, knowing that he is not licensed or privileged to do so, he enters or remains in any place as to which notice against trespass is given . . . ."). *Liparota* is potentially distinguishable, however, because the lack of authorization in the computer trespass statute concerns lack of authorization with respect to the relevant norms, not the relevant law. Further, not all physical-trespass statutes have required knowledge as to the absence of legal privilege. See, e.g., N.J. Stat. Ann. § 2A:170-31 (repealed 1979).

184. See supra notes 160–164 (discussing defendant's knowledge of facts in *United States v. Swartz*). This is bolstered by the common use of "willfulness" in federal criminal statutes to indicate knowing violation of a legal duty, see, e.g., Cheek v. United States, 498 U.S. 192, 193 (1991) (applying willfulness standard to failure to file federal income tax return), a use that does not appear in the CFAA. A 1986 Senate report has a brief discussion of the purpose of changing the mental state for unauthorized access from knowing to intentional. S. Rep. No. 99-432, at 5–6 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2483–84. The discussion is unclear and can be read as supporting either position.

to be legally unauthorized. Instead, the key question is the defendant's state of mind about the facts that, once the law is understood, made the access unauthorized.

So construed, the mental state requirement of computer trespass has a significant narrowing effect on liability for using canceled, blocked, and shared accounts. The individual must not only take steps that are contrary to the delegated authority; he must know or hope that his steps are contrary to that delegated authority. Recall the *Steele* case, in which the ex-employee used the backdoor account after he had resigned.[185] Steele obviously knew that the authority to access the account had been revoked: As the Fourth Circuit explained, the company had taken his work laptop, denied him physical access to the building, and made him sign a letter that he would not try to access the employer's network in the future.[186] In other cases, however, the revocation might not be so clear. The ex-employee might not know that her access rights to the account had been revoked. In such a case, she would not be guilty of criminal computer trespass.

The mental state requirement is particularly important in cases that involve shared passwords. If B shares a password with C, C's access is without authorization when C is acting outside the agency of B. At the same time, C's access is intentionally without authorization only if C knows or hopes of facts that would bring C*'s* access outside the agency of B. In many cases, C may not know how B uses the account, how often, or for what. C's state of mind about whether C is outside the agency relationship element may sharply limit C*'s* liability.

For example, imagine Ann gives Bob her Netflix username and password and tells Bob to feel free to use her account. Bob then uses Ann's account as if it were his own. Whether Bob's use of Ann's account is outside the agency relationship is itself a murky question: General permission to use the account whenever Bob likes implies a broad or even perhaps limitless authorization. But that murkiness aside, Bob can't be criminally liable for accessing Ann's account unless he knows or hopes that his acts are outside Ann's authorization. In the usual case, Bob would lack intent to access the account without authorization.[187]

CONCLUSION

Applying law to the Internet often rests on analogies. In litigation, each side will offer analogies that push the decisionmaker in a particular direction. Courts faced with competing analogies must know how to de-

185. United States v. Steele, 595 F. App'x 208 (4th Cir. 2014).

186. Id. at 211.

187. If courts construe the intent requirement as going to the legal conclusion that authorization is lacking, then the mental state requirement has an even more dramatic effect. It would prohibit liability unless the government can prove beyond a reasonable doubt that the defendant knew or hoped that his conduct was unlawful.

cide between them: How do you know whether Internet facts are more like one set of facts from the physical world or another?

This Essay can be understood as a conceptual guide to choosing analogies in the interpretation of computer trespass statutes. By appreciating the role of norms in the interpretation of physical trespass laws, courts can adopt sensible rules based on technological realities and their social construction. Because computer-network norms remain largely unsettled, the task is normative rather than descriptive. Judicial identification of the best norms to apply can help bring public acceptance of those norms, or at least provide a temporary set of answers until real norms emerge.

This approach helps avoid analogies that mislead rather than inform by missing the underlying norms that make analogies fit. Applying physical-world trespass cases to the Internet without first considering the difference between the physical and network worlds risks applying precedents from an environment with one norm to an environment that merits a very different one.

18 U.S. Code § 1030 - Fraud and related activity in connection with computers

U.S. Code Notes

(a) Whoever—

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) [1] of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5)

(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.[2]

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States; [3]

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—

(A) threat to cause damage to a protected computer;

(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;

shall be punished as provided in subsection (c) of this section.

(b) Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is—

(1)

(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2)

(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or

an attempt to commit an offense punishable under this subparagraph, if—

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds $5,000; and

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3)

(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4),[4] or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(4)

(A) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 5 years, or both, in the case of—

(i) an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)—

(I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other

proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(III) physical injury to any person;

(IV) a threat to public health or safety;

(V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

(VI) damage affecting 10 or more protected computers during any 1-year period; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(B) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 10 years, or both, in the case of—

(i) an offense under subsection (a)(5)(A), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) a harm provided in subclauses (I) through (VI) of subparagraph (A)(i); or

(ii) an attempt to commit an offense punishable under this subparagraph;

(C) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 20 years, or both, in the case of—

(i) an offense or an attempt to commit an offense under subparagraphs (A) or (B) of subsection (a)(5) that occurs after a conviction for another offense under this section; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(D) a fine under this title, imprisonment for not more than 10 years, or both, in the case of—

(i) an offense or an attempt to commit an offense under subsection (a)(5)(C) that occurs after a conviction for another offense under this section; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(E) if the offender attempts to cause or knowingly or recklessly causes serious bodily injury from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for not more than 20 years, or both;

(F) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both; or

(G) a fine under this title, imprisonment for not more than 1 year, or both, for—

(i) any other offense under subsection (a)(5); or

(ii) an attempt to commit an offense punishable under this subparagraph.

(d)

(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for

offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.

(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section—

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "protected computer" means a computer—

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government;

(B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States; or

(C) that—

(i) is part of a voting system; and

(ii)

(I) is used for the management, support, or administration of a Federal election; or

(II) has moved in or otherwise affects interstate or foreign commerce;

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term "financial institution" means—

(A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

(I) an organization operating under section 25 or section 25(a) [1] of the Federal Reserve Act;

(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;

(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;

(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;

(10) the term "conviction" shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service;

(12) the term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity;

(13) the term "Federal election" means any election (as defined in section 301(1) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30101(1))) for Federal office (as defined in section 301(3) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30101(3))); and

(14) the term "voting system" has the meaning given the term in section 301(b) of the Help America Vote Act of 2002 (52 U.S.C. 21081(b)).

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses [5] (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection

unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

(i)

(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

(A) such person's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation; and

(B) any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation.

(2) The criminal forfeiture of property under this subsection, any seizure and disposition thereof, and any judicial proceeding in relation thereto, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

(j) For purposes of subsection (i), the following shall be subject to forfeiture to the United States and no property right shall exist in them:

(1) Any personal property used or intended to be used to commit or to facilitate the commission of any violation of this section, or a conspiracy to violate this section.

(2) Any property, real or personal, which constitutes or is derived from proceeds traceable to any violation of this section, or a conspiracy to violate this section [6]

(Added Pub. L. 98–473, title II, § 2102(a), Oct. 12, 1984, 98 Stat. 2190; amended Pub. L. 99–474, § 2, Oct. 16, 1986, 100 Stat. 1213; Pub. L. 100–690, title VII, § 7065, Nov. 18, 1988, 102 Stat. 4404; Pub. L. 101–73, title IX, § 962(a)(5), Aug. 9, 1989, 103 Stat. 502; Pub. L. 101–647, title XII, § 1205(e), title XXV, § 2597(j), title XXXV, § 3533, Nov. 29, 1990, 104 Stat. 4831, 4910, 4925; Pub. L. 103–322, title XXIX, § 290001(b)–(f), Sept. 13, 1994, 108 Stat. 2097–2099; Pub. L. 104–294, title II, § 201, title VI, § 604(b)(36), Oct. 11, 1996, 110 Stat. 3491, 3508; Pub. L. 107–56, title V, § 506(a), title VIII, § 814(a)–(e), Oct. 26, 2001, 115 Stat. 366, 382–384; Pub. L. 107–273, div. B, title IV, §§ 4002(b)(1), (12), 4005(a)(3), (d)(3), Nov. 2, 2002, 116 Stat. 1807, 1808, 1812, 1813; Pub. L. 107–296, title XXII, § 2207(g), formerly title II, § 225(g), Nov. 25, 2002, 116 Stat. 2158, renumbered § 2207(g), Pub. L. 115–278, § 2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178; Pub. L. 110–326, title II, §§ 203, 204(a), 205–208, Sept. 26, 2008, 122 Stat. 3561, 3563; Pub. L. 116–179, § 2, Oct. 20, 2020, 134 Stat. 855.)

U.S. Code Toolbox

Law about... Articles from Wex
Table of Popular Names
Parallel Table of Authorities
How current is this?

515

ACCESSIBILITY

ABOUT LII

CONTACT US

ADVERTISE HERE

HELP

TERMS OF USE

PRIVACY

[LII]

17 U.S. Code § 1201 - Circumvention of copyright protection systems

U.S. Code Notes

(a) Violations Regarding Circumvention of Technological Measures.—

(1)

(A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter.

(B) The prohibition contained in subparagraph (A) shall not apply to persons who are users of a copyrighted work which is in a particular class of works, if such persons are, or are likely to be in the succeeding 3-year period, adversely affected by virtue of such prohibition in their ability to make noninfringing uses of that particular class of works under this title, as determined under subparagraph (C).

(C) During the 2-year period described in subparagraph (A), and during each succeeding 3-year period, the Librarian of Congress, upon the recommendation of the Register of Copyrights, who shall consult with the Assistant Secretary for Communications and Information of the Department of Commerce and report and comment on his or her views in making such recommendation, shall make the determination in a rulemaking proceeding for purposes of subparagraph (B) of whether persons who are users of a copyrighted work are, or are likely to be in the succeeding 3-year period, adversely affected by the prohibition under subparagraph (A) in their ability to make noninfringing uses under this title of a

particular class of copyrighted works. In conducting such rulemaking, the Librarian shall examine—

(i) the availability for use of copyrighted works;

(ii) the availability for use of works for nonprofit archival, preservation, and educational purposes;

(iii) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research;

(iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and

(v) such other factors as the Librarian considers appropriate.

(D) The Librarian shall publish any class of copyrighted works for which the Librarian has determined, pursuant to the rulemaking conducted under subparagraph (C), that noninfringing uses by persons who are users of a copyrighted work are, or are likely to be, adversely affected, and the prohibition contained in subparagraph (A) shall not apply to such users with respect to such class of works for the ensuing 3-year period.

(E) Neither the exception under subparagraph (B) from the applicability of the prohibition contained in subparagraph (A), nor any determination made in a rulemaking conducted under subparagraph (C), may be used as a defense in any action to enforce any provision of this title other than this paragraph.

(2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—

(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;

(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

(3) As used in this subsection—

(A) to "circumvent a technological measure" means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner; and

(B) a technological measure "effectively controls access to a work" if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.

(b) Additional Violations.—

(1) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—

(A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;

(B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.

(2) As used in this subsection—

(A) to "circumvent protection afforded by a technological measure" means avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure; and

(B) a technological measure "effectively protects a right of a copyright owner under this title" if the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title.

(c) Other Rights, Etc., Not Affected.—

(1) Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title.

(2) Nothing in this section shall enlarge or diminish vicarious or contributory liability for copyright infringement in connection with any technology, product, service, device, component, or part thereof.

(3) Nothing in this section shall require that the design of, or design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure, so long as such part or component, or the product in which such part or component is integrated, does not otherwise fall within the prohibitions of subsection (a)(2) or (b)(1).

(4) Nothing in this section shall enlarge or diminish any rights of free speech or the press for activities using consumer electronics, telecommunications, or computing products.

(d) Exemption for Nonprofit Libraries, Archives, and Educational Institutions.—

(1) A nonprofit library, archives, or educational institution which gains access to a commercially exploited copyrighted work solely in order to make a good faith determination of whether to acquire a copy of that work for the sole purpose of engaging in conduct permitted under this title shall not be in violation of subsection (a)(1)(A). A copy of a work to which access has been gained under this paragraph—

(A) may not be retained longer than necessary to make such good faith determination; and

(B) may not be used for any other purpose.

(2) The exemption made available under paragraph (1) shall only apply with respect to a work when an identical copy of that work is not

reasonably available in another form.

(3) A nonprofit library, archives, or educational institution that willfully for the purpose of commercial advantage or financial gain violates paragraph (1)—

(A) shall, for the first offense, be subject to the civil remedies under section 1203; and

(B) shall, for repeated or subsequent offenses, in addition to the civil remedies under section 1203, forfeit the exemption provided under paragraph (1).

(4) This subsection may not be used as a defense to a claim under subsection (a)(2) or (b), nor may this subsection permit a nonprofit library, archives, or educational institution to manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, component, or part thereof, which circumvents a technological measure.

(5) In order for a library or archives to qualify for the exemption under this subsection, the collections of that library or archives shall be—

(A) open to the public; or

(B) available not only to researchers affiliated with the library or archives or with the institution of which it is a part, but also to other persons doing research in a specialized field.

(e) Law Enforcement, Intelligence, and Other Government Activities.— This section does not prohibit any lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee of the United States, a State, or a political subdivision of a State, or a person acting pursuant to a contract with the United States, a State, or a political subdivision of a State. For purposes of this subsection, the term "information security" means activities carried out in order to identify and address the vulnerabilities of a government computer, computer system, or computer network.

(f) Reverse Engineering.—

(1) Notwithstanding the provisions of subsection (a)(1)(A), a person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively

controls access to a particular portion of that program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to the person engaging in the circumvention, to the extent any such acts of identification and analysis do not constitute infringement under this title.

(2) Notwithstanding the provisions of subsections (a)(2) and (b), a person may develop and employ technological means to circumvent a technological measure, or to circumvent protection afforded by a technological measure, in order to enable the identification and analysis under paragraph (1), or for the purpose of enabling interoperability of an independently created computer program with other programs, if such means are necessary to achieve such interoperability, to the extent that doing so does not constitute infringement under this title.

(3) The information acquired through the acts permitted under paragraph (1), and the means permitted under paragraph (2), may be made available to others if the person referred to in paragraph (1) or (2), as the case may be, provides such information or means solely for the purpose of enabling interoperability of an independently created computer program with other programs, and to the extent that doing so does not constitute infringement under this title or violate applicable law other than this section.

(4) For purposes of this subsection, the term "interoperability" means the ability of computer programs to exchange information, and of such programs mutually to use the information which has been exchanged.

(g) Encryption Research.—

(1) Definitions.—For purposes of this subsection—

(A) the term "encryption research" means activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products; and

(B) the term "encryption technology" means the scrambling and descrambling of information using mathematical formulas or

algorithms.

(2) Permissible acts of encryption research.—Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure as applied to a copy, phonorecord, performance, or display of a published work in the course of an act of good faith encryption research if—

(A) the person lawfully obtained the encrypted copy, phonorecord, performance, or display of the published work;

(B) such act is necessary to conduct such encryption research;

(C) the person made a good faith effort to obtain authorization before the circumvention; and

(D) such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.

(3) Factors in determining exemption.—In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include—

(A) whether the information derived from the encryption research was disseminated, and if so, whether it was disseminated in a manner reasonably calculated to advance the state of knowledge or development of encryption technology, versus whether it was disseminated in a manner that facilitates infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security;

(B) whether the person is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology; and

(C) whether the person provides the copyright owner of the work to which the technological measure is applied with notice of the findings and documentation of the research, and the time when such notice is provided.

(4) Use of technological means for research activities.—Notwithstanding the provisions of subsection (a)(2), it is not a violation of that

subsection for a person to—

(A) develop and employ technological means to circumvent a technological measure for the sole purpose of that person performing the acts of good faith encryption research described in paragraph (2); and

(B) provide the technological means to another person with whom he or she is working collaboratively for the purpose of conducting the acts of good faith encryption research described in paragraph (2) or for the purpose of having that other person verify his or her acts of good faith encryption research described in paragraph (2).

(5) Report to congress.—Not later than 1 year after the date of the enactment of this chapter, the Register of Copyrights and the Assistant Secretary for Communications and Information of the Department of Commerce shall jointly report to the Congress on the effect this subsection has had on—

(A) encryption research and the development of encryption technology;

(B) the adequacy and effectiveness of technological measures designed to protect copyrighted works; and

(C) protection of copyright owners against the unauthorized access to their encrypted copyrighted works.

The report shall include legislative recommendations, if any.

(h) Exceptions Regarding Minors.—In applying subsection (a) to a component or part, the court may consider the necessity for its intended and actual incorporation in a technology, product, service, or device, which—

(1) does not itself violate the provisions of this title; and

(2) has the sole purpose to prevent the access of minors to material on the Internet.

(i) Protection of Personally Identifying Information.—

(1) Circumvention permitted.—Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person

to circumvent a technological measure that effectively controls access to a work protected under this title, if—

(A) the technological measure, or the work it protects, contains the capability of collecting or disseminating personally identifying information reflecting the online activities of a natural person who seeks to gain access to the work protected;

(B) in the normal course of its operation, the technological measure, or the work it protects, collects or disseminates personally identifying information about the person who seeks to gain access to the work protected, without providing conspicuous notice of such collection or dissemination to such person, and without providing such person with the capability to prevent or restrict such collection or dissemination;

(C) the act of circumvention has the sole effect of identifying and disabling the capability described in subparagraph (A), and has no other effect on the ability of any person to gain access to any work; and

(D) the act of circumvention is carried out solely for the purpose of preventing the collection or dissemination of personally identifying information about a natural person who seeks to gain access to the work protected, and is not in violation of any other law.

(2) Inapplicability to certain technological measures.—
This subsection does not apply to a technological measure, or a work it protects, that does not collect or disseminate personally identifying information and that is disclosed to a user as not having or using such capability.

(j) Security Testing.—

(1) Definition.—
For purposes of this subsection, the term "security testing" means accessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network.

(2) Permissible acts of security testing.—
Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to engage in an act of security

testing, if such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.

(3) Factors in determining exemption.—In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include—

(A) whether the information derived from the security testing was used solely to promote the security of the owner or operator of such computer, computer system or computer network, or shared directly with the developer of such computer, computer system, or computer network; and

(B) whether the information derived from the security testing was used or maintained in a manner that does not facilitate infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security.

(4) Use of technological means for security testing.—
Notwithstanding the provisions of subsection (a)(2), it is not a violation of that subsection for a person to develop, produce, distribute or employ technological means for the sole purpose of performing the acts of security testing described in subsection (2),[1] provided such technological means does not otherwise violate section[2] (a)(2).

(k) Certain Analog Devices and Certain Technological Measures.—

(1) Certain analog devices.—

(A) Effective 18 months after the date of the enactment of this chapter, no person shall manufacture, import, offer to the public, provide or otherwise traffic in any—

(i) VHS format analog video cassette recorder unless such recorder conforms to the automatic gain control copy control technology;

(ii) 8mm format analog video cassette camcorder unless such camcorder conforms to the automatic gain control technology;

(iii) Beta format analog video cassette recorder, unless such recorder conforms to the automatic gain control copy control technology, except that this requirement shall not apply until

there are 1,000 Beta format analog video cassette recorders sold in the United States in any one calendar year after the date of the enactment of this chapter;

(iv) 8mm format analog video cassette recorder that is not an analog video cassette camcorder, unless such recorder conforms to the automatic gain control copy control technology, except that this requirement shall not apply until there are 20,000 such recorders sold in the United States in any one calendar year after the date of the enactment of this chapter; or

(v) analog video cassette recorder that records using an NTSC format video input and that is not otherwise covered under clauses (i) through (iv), unless such device conforms to the automatic gain control copy control technology.

(B) Effective on the date of the enactment of this chapter, no person shall manufacture, import, offer to the public, provide or otherwise traffic in—

(i) any VHS format analog video cassette recorder or any 8mm format analog video cassette recorder if the design of the model of such recorder has been modified after such date of enactment so that a model of recorder that previously conformed to the automatic gain control copy control technology no longer conforms to such technology; or

(ii) any VHS format analog video cassette recorder, or any 8mm format analog video cassette recorder that is not an 8mm analog video cassette camcorder, if the design of the model of such recorder has been modified after such date of enactment so that a model of recorder that previously conformed to the four-line colorstripe copy control technology no longer conforms to such technology.

Manufacturers that have not previously manufactured or sold a VHS format analog video cassette recorder, or an 8mm format analog cassette recorder, shall be required to conform to the four-line colorstripe copy control technology in the initial model of any such recorder manufactured after the date of the enactment of this chapter, and thereafter to continue conforming to the four-line colorstripe copy control technology. For purposes of this subparagraph, an analog video cassette

recorder "conforms to" the four-line colorstripe copy control technology if it records a signal that, when played back by the playback function of that recorder in the normal viewing mode, exhibits, on a reference display device, a display containing distracting visible lines through portions of the viewable picture.

(2) Certain encoding restrictions.—No person shall apply the automatic gain control copy control technology or colorstripe copy control technology to prevent or limit consumer copying except such copying—

(A) of a single transmission, or specified group of transmissions, of live events or of audiovisual works for which a member of the public has exercised choice in selecting the transmissions, including the content of the transmissions or the time of receipt of such transmissions, or both, and as to which such member is charged a separate fee for each such transmission or specified group of transmissions;

(B) from a copy of a transmission of a live event or an audiovisual work if such transmission is provided by a channel or service where payment is made by a member of the public for such channel or service in the form of a subscription fee that entitles the member of the public to receive all of the programming contained in such channel or service;

(C) from a physical medium containing one or more prerecorded audiovisual works; or

(D) from a copy of a transmission described in subparagraph (A) or from a copy made from a physical medium described in subparagraph (C).

In the event that a transmission meets both the conditions set forth in subparagraph (A) and those set forth in subparagraph (B), the transmission shall be treated as a transmission described in subparagraph (A).

(3) Inapplicability.—This subsection shall not—

(A) require any analog video cassette camcorder to conform to the automatic gain control copy control technology with respect to any video signal received through a camera lens;

(B) apply to the manufacture, importation, offer for sale, provision of, or other trafficking in, any professional analog video cassette recorder; or

(C) apply to the offer for sale or provision of, or other trafficking in, any previously owned analog video cassette recorder, if such recorder was legally manufactured and sold when new and not subsequently modified in violation of paragraph (1)(B).

(4) Definitions.—For purposes of this subsection:

(A) An "analog video cassette recorder" means a device that records, or a device that includes a function that records, on electromagnetic tape in an analog format the electronic impulses produced by the video and audio portions of a television program, motion picture, or other form of audiovisual work.

(B) An "analog video cassette camcorder" means an analog video cassette recorder that contains a recording function that operates through a camera lens and through a video input that may be connected with a television or other video playback device.

(C) An analog video cassette recorder "conforms" to the automatic gain control copy control technology if it—

(i) detects one or more of the elements of such technology and does not record the motion picture or transmission protected by such technology; or

(ii) records a signal that, when played back, exhibits a meaningfully distorted or degraded display.

(D) The term "professional analog video cassette recorder" means an analog video cassette recorder that is designed, manufactured, marketed, and intended for use by a person who regularly employs such a device for a lawful business or industrial use, including making, performing, displaying, distributing, or transmitting copies of motion pictures on a commercial scale.

(E) The terms "VHS format", "8mm format", "Beta format", "automatic gain control copy control technology", "colorstripe copy control technology", "four-line version of the colorstripe copy control technology", and "NTSC" have the meanings that are

commonly understood in the consumer electronics and motion picture industries as of the date of the enactment of this chapter.

(5) VIOLATIONS.—

Any violation of paragraph (1) of this subsection shall be treated as a violation of subsection (b)(1) of this section. Any violation of paragraph (2) of this subsection shall be deemed an "act of circumvention" for the purposes of section 1203(c)(3)(A) of this chapter.

(Added Pub. L. 105–304, title I, § 103(a), Oct. 28, 1998, 112 Stat. 2863; amended Pub. L. 106–113, div. B, § 1000(a)(9) [title V, § 5006], Nov. 29, 1999, 113 Stat. 1536, 1501A–594.)

U.S. Code Toolbox

Law about... Articles from Wex
Table of Popular Names
Parallel Table of Authorities
How current is this?

40

CYBER SECURITY ACTIVE DEFENSE: PLAYING WITH FIRE OR SOUND RISK MANAGEMENT?

Sean L. Harrington*

Trying to change its program
Trying to change the mode . . . crack the code
Images conflicting into data overload[1]

Cite as: Sean L. Harrington, *Cyber Security Active Defense: Playing with Fire or Sound Risk Management?*, 20 RICH. J.L. & TECH. 12 (2014), http://jolt.richmond.edu/v20i4/article12.pdf.

I. INTRODUCTION

[1] "Banks Remain the Top Target for Hackers, Report Says," is the title of an April 2013 *American Banker* article.[2] Yet, no new

* The author is a cyber-security policy analyst in the banking industry and a digital forensics examiner in private practice. Mr. Harrington is a graduate with honors from Taft Law School, and holds the CCFP, MCSE, CISSP, CHFI, and CSOXP certifications. He has served on the board of the Minnesota Chapter of the High Technology Crime Investigation Association, is a current member of Infragard, the Financial Services Roundtable's legislative and regulatory working groups, FS-ISAC, the U.S. Chamber of Commerce "Cyber Working Group," the Fourth District Ethics Committee in Minnesota, and is a council member of the Minnesota State Bar Association's Computer & Technology Law Section. Mr. Harrington teaches computer forensics for Century College in Minnesota, and recently contributed a chapter on the Code of Ethics for the forthcoming Official (ISC)²® Guide to the Cyber Forensics Certified Professional CBK®. He is also an instructor for the CCFP certification.

[1] RUSH, *The Body Electric*, *on* GRACE UNDER PRESSURE (Mercury Records 1984).

[2] Sean Sposito, *Banks Remain the Top Target for Hackers, Report Says*, AM. BANKER (April 23, 2013, 10:04 AM), http://www.americanbanker.com/issues/178_78/banks-remain-the-top-target-for-hackers-report-says-1058543-1.html.

comprehensive U.S. cyber legislation has been enacted since 2002,[3] and neither legislative history nor the statutory language of the Computer Fraud and Abuse Act (CFAA) or Electronic Communications Privacy Act (ECPA) make reference to the Internet.[4] Courts have nevertheless filled in the gaps—sometimes with surprising results.

[2] Because state law, federal legislative proposals, and case law all are in a continuing state of flux, practitioners have found it necessary to follow these developments carefully, forecast, and adapt to them, all of which has proved quite challenging. As the title of this Comment suggests, deploying sound cyber security practices is not only equally as

[3] ERIC A. FISHER, CONG. RESEARCH SERV., R 42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW AND DISCUSSION OF PROPOSED REVISIONS 3 (2013), *available at* http://fas.org/sgp/crs/natsec/R42114.pdf (discussing, for example, the Federal Information Security Management Act).

[4] *See* Yonatan Lupu, *The Wiretap Act and Web Monitoring: A Breakthrough for Privacy Rights?*, 9 VA. J.L. & TECH. 3, ¶¶ 7, 9 (2004) (discussing the use of the ECPA and the lack of words such as "Internet," "World Wide Web," and "e-commerce" in the text or legislative history); *see also* Eric C. Bosset et al., *Private Actions Challenging Online Data Collection Practices Are Increasing: Assessing the Legal Landscape*, INTELL. PROP. & TECH. L.J., Feb. 2011, at 3 ("[F]ederal statutes such as the Electronic Communications Privacy Act (ECPA) and the Computer Fraud and Abuse Act (CFAA) . . . were drafted long before today's online environment could be envisioned . . . ."); Miguel Helft & Claire Cain Miller, *1986 Privacy Law Is Outrun by the Web*, N.Y. TIMES (Jan. 9, 2011), http://www.nytimes.com/2011/01/10/technology/10privacy.html?pagewanted=all&_r=1 & (noting that Congress enacted the ECPA before the World Wide Web or widespread use of e-mail); Orin S. Kerr, *The Future of Internet Surveillance Law: A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208, 1213-14, 1229-30 (2004); *see generally The Electronic Communications Privacy Act: Government Perspectives on Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 1-2 (2011) (statement of Sen. Patrick Leahy, Chairman, S. Comm. on the Judiciary), *available at* http://fas.org/irp/congress/2011_hr/ecpa.pdf ("[D]etermining how best to bring this privacy law into the Digital Age will be one of Congress's greatest challenges. . . . [The] ECPA is a law that is hampered by conflicting standards that cause confusion for law enforcement, the business community, and American consumers alike.").

challenging, but also "risky," which may seem counterintuitive in light of the fact that intent of cyber security programs is to manage risk, not create it.[5]

[3] Cyber security risks concern exploits made possible by technological advances, some of which are styled with familiar catch-phrases: "e-Discovery," "social media," "cloud computing," "Crowdsourcing," and "big data," to name a few. Yet, long before the term "cloud computing" became part of contemporary parlance, Picasa used to store photos in the cloud (where the "cloud" is a metaphor for the Internet).[6] This author has been using Hotmail since 1997 (another form of cloud computing). As the foregoing examples illustrate, the neologisms were long predated by their underlying concepts.

[4] One of the latest techno-phrases du jour is "hack back."[7] The concept isn't new, and the term has been "common" parlance at least as far back as 2003.[8] "Hack back"—sometimes termed "active defense," "back hacking," "retaliatory hacking," or "offensive countermeasures" ("OCM")—has been defined as the

[5] *See generally* NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 4 (Version 1.0, 2014) *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf (describing The Framework as "a risk-based approach to managing cybersecurity risk").

[6] *See*, Eric Griffith, *What is Cloud Computing?*, PC MAGAZINE (May 13, 2013) http://www.pcmag.com/article2/0,2817,2372163,00.asp.

[7] *See, e.g.*, Ken Dilanian, *A New Brand of Cyber Security: Hacking the Hackers*, L.A. TIMES (Dec. 4, 2012), http://articles.latimes.com/2012/dec/04/business/la-fi-cyber-defense-20121204/2 (proposing that "companies should be able to 'hack back' by, for example, disabling servers that host cyber attacks").

[8] *See, e.g.*, Scott Carle, *Crossing the Line: Ethics for the Security Professional*, SANS INST. (2003), http://www.sans.org/reading-room/whitepapers/hackers/crossing-line-ethics-security-professional-890. Readers, doubtless, will know of earlier references.

> "process of identifying attacks on a system and, if possible, identifying the origin of the attacks." Back hacking can be thought of as a kind of reverse engineering of hacking efforts, where security consultants and other professionals try to anticipate attacks and work on adequate responses."[9]

A more accurate and concise definition might be "turning the tables on a cyberhacking assailant: thwarting or stopping the crime, or perhaps even trying to steal back what was taken."[10] One private security firm, renowned for its relevant specialization, defines active defense, in pertinent part, as "deception, containment, tying up adversary resources, and creating doubt and confusion while denying them the benefits of their operations."[11] Some have proposed—or carried out—additional measures, such as "photographing the hacker using his own system's camera, implanting malware in the hacker's network, or even physically disabling or destroying the hacker's own computer or network."[12]

---

[9] TECHOPEDIA, http://www.techopedia.com/definition/23172/back-hack (last visited June 28, 2014); *see also* NETLINGO, http://www.netlingo.com/word/back-hack.php (last visited June 28, 2014) ("[Back-hack is t]he reverse process of finding out who is hacking into a system. Attacks can usually be traced back to a computer or pieced together from 'electronic bread crumbs' unknowingly left behind by a cracker.").

[10] Melissa Riofrio, *Hacking Back: Digital Revenge Is Sweet but Risky*, PCWORLD (May 9, 2013, 3:00 AM), http://www.pcworld.com/article/2038226/hacking-back-digital-revenge-is-sweet-but-risky.html.

[11] Dmitri Alperovitch, *Active Defense: Time for a New Security Strategy*, CROWDSTRIKE (Feb. 25, 2013), http://www.crowdstrike.com/blog/active-defense-time-new-security-strategy/.

[12] COMM'N ON THE THEFT OF AM. INTELLECTUAL PROP., THE IP COMMISSION REPORT 81 (2013) [hereinafter THE IP COMMISSION REPORT], *available at* http://ipcommission.org/report/IP_Commission_Report_052213.pdf; s*ee also* Sam Cook, *Georgia Outs Russian Hacker, Takes Photo with His Own Webcam*, GEEK (Oct. 31, 2012, 4:28 PM), http://www.geek.com/news/georgia-outs-russian-hacker-takes-photo-with-his-own-webcam-1525485/. *See* Jay P. Kesan & Carol M. Hayes, *Thinking*

[5] Back hacking has been a top-trending technology topic over the past year, prompted in part by the controversial Report of the Commission on the Theft of American Intellectual Property ("IP Commission Report"),[13] and has been debated on blogs, symposium panels, editorials, and news media forums by information security professionals and lawyers alike. One with the potential to grab practitioners' attention was a panel of attorneys David Navetta and Ron Raether—both well regarded in the information security community—discussing the utility and propriety of such practices. One opined that, if the circumstance is exigent enough, a company may take "measures into [its] own hands," and that it would, "not likely be prosecuted under the CFAA, depending on the exigency of the circumstances."[14] The other reasoned that hack back "technically violates the law, but is anyone going to prosecute you for that? Unlikely."[15] He noted, "[i]t provides a treasure trove of forensic information that you can use," and continued, "[w]ith respect to the more extreme end of hack back, where you are actually going to shut down servers, I think there is a necessity element to it—an exigency: if someone's life is threatened, if it appears that there is going to be a monumental effect on the company, then it might be justified."[16] In 2014

Through Active Defense in Cyberspace, in Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy 327, 328 (The National Academies Press ed., 2010) ("Counterstrikes of this nature have already been occurring on the Internet over the last decade, by both government and private actors, and full software packages designed to enable counterstriking have also been made commercially available, even though such counterstrikes are of questionable legality").

[13] *See* THE IP COMMISSION REPORT, *supra* note 12.

[14] Tom Fields, *To 'Hack Back' or Not?*, BANKINFOSECURITY (Feb. 27, 2013), http://www.bankinfosecurity.com/to-hack-back-or-not-a-5545.

[15] *Id.*

[16] *Id.*

at the most recent RSA conference, where the "hackback" debate continued, the presentation was billed, in part, with the proposition, "[a]ctive defense should be viewed as a diverse set of techniques along a spectrum of varying risk and legality."[17] And, other commentators have urged that "offensive operations must be considered as a possible device in the cyber toolkit." [18]

[6] Most commentators and scholars, however, seem to agree that "hack back" is not only "risky," but is also not a viable option for a variety of reasons.[19] Hack backs and other surreptitious cyber acts incur the risks of criminal liability, civil liability, regulatory liability, professional discipline, compromise of corporate ethics, injury to brand image, and escalation. One practitioner quoted by the LA Times exclaimed, "[i]t's not only legally wrong, it's morally wrong."[20] James Andrew Lewis, a senior

[17] *Hackback? Claptrap!—An Active Defense Continuum for the Private Sector*, RSA CONF. (Feb. 27, 2014, 9:20 AM), http://www.rsaconference.com/events/us14/agenda/sessions/1146/hackback-claptrap-an-active-defense-continuum-for.

[18] Shane McGee, Randy V. Sabett, & Anand Shah, *Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense*, 8 J. BUS. & TECH. L. 1 (2013) Available at: http://digitalcommons.law.umaryland.edu/jbtl/vol8/iss1/3

[19] *See, e.g.*, Rafal Los, *Another Reason Hacking Back Is Probably a Bad Idea*, INFOSECISLAND (June 20, 2013), http://www.infosecisland.com/blogview/23228-Another-Reason-Hacking-Back-is-Probably-a-Bad-Idea.html; Riofrio, *supra* note 10.

[20] Dilanian, *supra* note 7; *see also* William Jackson, *The Hack-Back vs. The Rule of Law: Who Wins?*, CYBEREYE, (May 31, 2013, 9:39 AM) http://gcn.com/blogs/cybereye/2013/00/hacking-back-vs-the-rule-of-law.aspx (stating "[i]n the face of increasing cyber threats there is an understandable pent-up desire for an active response, but this response should not cross legal thresholds. In the end, we either have the rule of law or we don't. That others do not respect this rule does not excuse us from observing it. Admittedly this puts public- and private-sector organizations and individuals at a short-term disadvantage while correcting the situation, but it's a pill we will have to swallow.").

fellow at the Center for Strategic and International Studies, characterized hacking back as "a remarkably bad idea that would harm the national interest."[21] The Cyber Intelligence Sharing and Protection Act, a major cybersecurity bill passed by the House in April 2013, contained an amendment that specifically provided that the bill did not permit hacking back.[22] Representative Jim Langevin (RI-D), who authored the amendment, explained, "[w]ithout this clear restriction, there is simply too much risk of potentially dangerous misattribution or misunderstanding of any hack-back actions."[23] Further, the private security firm renowned for its active defense strategies, mentioned *ante*, has attempted to distance itself from the phrases such as "hack back" and "retaliatory hacking," preferring instead the broader phrase "active defense."[24] Another example of the importance of subtleties in word choice may be "Countermeasure," where some appear to have conflated the word with the concept of active defense.[25]

---

[21] James Andrew Lewis, *Private Retaliation in Cyberspace*, CENTER FOR STRATEGIC & INT'L STUDIES (May 22, 2013), http://csis.org/publication/private-retaliation-cyberspace.

[22] *See* Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. (2013).

[23] Christopher M. Matthews, *Support Grows to Let Cybertheft Victims 'Hack Back'*, WALL ST. J. (June 2, 2013, 9:33 PM), http://online.wsj.com/news/articles/SB10001424127887324682204578517374103394466.

[24] *See* Alperovitch, *supra* note 11. The firm's online marketing literature includes the following: "Active Defense is NOT about 'hack-back,' retaliation, or vigilantism . . . we are fundamentally against these tactics and believe they can be counterproductive, as well as potentially illegal." *Id.*; *see also* Paul Roberts, *Don't Call It a Hack Back: Crowdstrike Unveils Falcon Platform*, SECURITY LEDGER (June 19, 2013, 11:47 AM), https://securityledger.com/2013/06/dont-call-it-a-hack-back-crowdstrike-unveils-falcon-platform/.

[25] Charlie Mitchell, *Senate Judiciary Panel Will Examine Stronger Penalties for Cyber Crimes and Espionage*, INSIDE CYBERSECURITY (May 9, 2014) http://insidecybersecurity.com/Cyber-Daily-News/Daily-News/senate-judiciary-panel-will-examine-stronger-penalties-for-cyber-crimes-and-espionage/menu-id-1075.html

II. ACTIVE DEFENSE APPROACHES

[7] Self-defense is not an abstraction created by civilization, but a law spawned by nature itself, and has been justified since antiquity.[26] It has been regarded since the early modern period as available to redress injuries against a state's sovereign rights.[27] There is little question cyber-attacks against a designated critical infrastructure are attacks against a state's sovereign rights,[28] because much of civilian infrastructure is both a military and national asset.[29] Accordingly, the focus of 2014 NATO

(stating "[a]uthorization for so-called countermeasures is included in the draft cyber information-sharing and liability protection bill . . . White House and Department of Homeland Security officials . . . declined to discuss the administration's view of deterrence issues such as active defense."). To be distinguished from OCM, "countermeasure" is defined in the draft Cybersecurity Information-Sharing Act of 2014 as "an action, device, procedure, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that prevents or mitigates a known or suspected cybersecurity threat or security vulnerability." *See* H.R. 624.

[26] *See, e.g.*, Marcus Tullius Cicero, The Speech of M.T. Cicero in Defence of Titus Annius Milo, *in* THE ORATIONS OF MARCUS TULLIUS CICERO 390, 392-393 (C.D. Yonge trans., 1913).

[27] Sheng Li, Note, *When Does Internet Denial Trigger the Right of Armed Self-Defense?*, 38 YALE J. INT'L L. 179, 182 (2013).

[28] *See, e.g.*, WALTER GARY SHARP SR., CYBERSPACE AND THE USE OF FORCE 129-31 (1999).

[29] *See* U.S. DEP'T. OF DEF., CONDUCT OF THE PERSIAN GULF WAR: FINAL REPORT TO CONGRESS PURSUANT TO TITLE V OF THE PERSIAN GULF CONFLICT SUPPLEMENTAL AUTHORIZATION AND PERSONNEL BENEFITS ACT OF 1991 (PUBLIC LAW 102-25) N-1 (1992) ("Civilian employees, despite seemingly insurmountable logistical problems, unrelenting pressure, and severe time constraints, successfully accomplished what this nation asked of them in a manner consistent with the highest standards of excellence and professionalism.").

International Conference on Cyber Conflict ("CyCon") is active cyber defense, including implications for critical infrastructure.[30] Likewise, a project sponsored by NATO's Cooperative Cyber Defense Centre of Excellence is set to publish a report in 2016 that establishes acceptable responses to pedestrian or quotidian cyber-attacks against nations, whereas its predecessor, regarded as an academic text, focused on cyber-attacks against a country that are physically disruptive or injurious to people and possible responses under the UN charter and military rules.[31] Both works are based on the concepts of self-defense and, under certain circumstances, preemptive "anticipatory self-defense."[32]

[8] The questions that scholars, policymakers, information security experts, and corporate executives have struggled with, however, is at what threshold do such attacks warrant the protection of the state,[33] whether a private corporation may respond in lieu of or in concert with protection by the state, and to what extent such collusion constitutes excessive entanglement between the private and public sector. Implicit in these questions is whether the government is willing and able to develop a

[30] *See* CYCON, http://ccdcoe.org/cycon/index.html (last visited July 16, 2014).

[31] *See* NATO COOP. CYBER DEFENCE CTR. OF EXCELLENCE, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 4 (Michael N. Schmitt ed., 2013); *see also* U.N. Charter art. 2, para. 4 & art. 51 (governing the modern law of self-defense).

[32] *See, e.g.*, Keiko Kono, *Briefing Memo: Cyber Security and the Tallinn Manual*, NAT'L INST. FOR DEF. STUDIES NEWS, Oct. 2013, at 2, *available at* www.nids.go.jp/english/publication/briefing/pdf/2013/briefing_e180.pdf.

[33] *See, e.g.*, Siobhan Gorman & Danny Yadron, *Banks Seek U.S. Help on Iran Cyberattacks*, WALL ST. J. (June 16, 2013, 12:01 AM), http://online.wsj.com/news/articles/SB10001424127887324734904578244302923178548 ; Christopher J. Castelli, *DOJ Official Urges Public-Private Cybersecurity Partnership Amid Legal Questions*, INSIDE CYBERSECURITY (April 1, 2014), http://insidecybersecurity.com/Cyber-Daily-News/Daily-News/doj-official-urges-public-private-cybersecurity-partnership-amid-legal-questions/menu-id-1075.html.

modern and adaptable regulatory and criminal law framework and to allocate adequate law enforcement resources to confront the problem.[34] Because, at the time of this writing, it is widely perceived that the government is not yet willing and able,[35] victims often do not report suspected or actual cyber-attacks, and have resorted to inappropriate self-help, deploying their own means of investigating and punishing transgressors.[36] As one commentator posits,

> With regard to computer crime, some might argue that the *entire* investigative process be outsourced to the business community. Historically, the privatization of investigations has assisted public law enforcement by allowing them to concentrate on other responsibilities, and has prevented

[34] One such example is the "Computer Trespasser" exception added by Congress to the Wiretap Act, which allows law enforcement officials to monitor the activities of hackers when (1) the owner or operator of the network authorizes the interception; (2) law enforcement is engaged in a lawful investigation; (3) law enforcement has reasonable grounds to believe the contents of the communications will be relevant to that investigation; and (4) such interception does not acquire communications other than those transmitted to or from the hacker. *See* 18 U.S.C. § 2511(2)(i)(I)-(IV) (2012); *see also* Bradley J. Schaufenbuel, *The Legality of Honeypots*, ISSA J., April 2008, at 16, 19, *available at* http://www.jdsupra.com/legalnews/the-legality-of-honeypots-50070/.

[35] *See, e.g.*, David E. Sanger, *White House Details Thinking on Cybersecurity Flaws*, New York Times, (April 28, 2014) (discussing the Government's admission that it refrains from disclosing major computer sercurity vulnerabilities that could be useful to "thwart a terrorist attack, stop the theft of our nation's intellectual property, or even discover more dangerous vulnerabilities that are being used by hackers or other adversaries to exploit our networks.")

[36] *See* Sameer Hinduja, *Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future*, 1 INT'L J. CYBER CRIMINOLOGY 1, 16 (2007) (citation omitted).

> their resources from being allocated in too sparse a manner to be useful." [37]

Awaiting the ultimate resolution of these questions, American corporations have developed an array of active defense tactics. Below are a few of the more common examples of those, and the corresponding challenges:

A. Beaconing

[9] Beaconing is one of the most cited active defense techniques, and one mentioned in the IP Commission Report (along with "meta-tagging," and "watermarking") as a way to enhance electronic files to "allow for awareness of whether protected information has left an authorized network and can potentially identify the location of files in the event that they are stolen."[38] A benign version of beaconing is the use of so-called Web bugs.[39] A Web bug is a link—a surreptitious file object—commonly used by spammers and placed in an e-mail message or e-mail attachment, which, when opened, will cause the e-mail client or program will attempt to retrieve an image file object from a remote Web server and, in the

[37] *Id.* at 19. *But see* Kesan & Hayes, *supra*, note 12 at 33 ("there is a more significant downside of entrusting active defense to private firms. Our model addressing the optimal use of active defense emphasizes that there are threshold points where permitting counterstrikes would be the socially optimal solution. However, it does not define these thresholds, and determining these thresholds requires some sort of standardization. It would be unwise to allow individual companies to make these decisions on a case by case basis.")

[38] THE IP COMMISSION REPORT, *supra* note 12, at 81. *See also* Joseph Menn, *Hacked Companies Fight Back With Controversial Steps*, REUTERS, June 18, 2012, available at http://www.reuters.com/article/2012/06/18/us-media-tech-summit-cyber-strikeback-idUSBRE85G07S20120618

[39] *See* Stephanie Olsen, *Nearly Undetectable Tracking Device Raises Concerns*, CNET (July 12, 2000), http://news.cnet.com/2100-1017-243077.html.

process, transmit information that includes the user's IP address and other information.[40] This transmission is not possible "if the user did not preconfigure the e-mail client or program to refrain from retrieving images or HTML content from the Internet," or if the user's e-mail client blocks externally-hosted images by default.[41] "This information becomes available to the sender either through an automated report service (*e.g.*, ReadNotify.com) or simply by monitoring traffic to the Web server."[42] In one project demonstrating the use advocated by the IP Commission Report, researchers employed such technology in decoy documents to track possible misuse of confidential documents.[43] So, is beaconing legal?

[10] *The Wall Street Journal* (the "*Journal*") quoted Drexel University law professor Harvey Rishikof—who also is co-chairman of the American Bar Association's Cybersecurity Legal Task Force—as saying the legality of beaconing is not entirely clear.[44] Rishikof is quoted as saying, "'[t]here's the black-letter law, and there's the gray area. . . . Can you put a beacon on your data? Another level is, could you put something on your data that would perform a more aggressive action if the data was

[40] *See id. See also* John Gilroy, *Ask The Computer Guy*, WASH. POST, Jan. 27, 2002, at H07 (describing web bugs in lay parlance).

[41] Sean L. Harrington, *Collaborating with a Digital Forensics Expert: Ultimate Tag Team or Disastrous Duo?*, 38 WM. MITCHELL L. REV. 353, 363 (2011), *available at* http://www.wmitchell.edu/lawreview/Volume38/documents/7.Harrington.pdf.

[42] *Id.*

[43] *See generally* Brian M. Bowen et al., *Baiting Inside Attackers Using Decoy Documents*, COLUM. UNIV. DEP'T OF COMPUTER SCI. (2009), *available at* http://www.cs.columbia.edu/~angelos/Papers/2009/DecoyDocumentsSECCOM09.pdf (last visited May 13, 2014) (introducing and discussing properties of decoys as a guide to design "trap-based defenses" to better detect the likelihood of insider attacks).

[44] *See* Matthews, *supra* note 23.

taken?'"[45] The article went on to suggest more aggressive strategies such as "inserting code that would cause stolen data to self-destruct or inserting a program in the data that would allow a company to seize control of any cameras on the computers where the data were being stored."[46] The *Journal*, citing an anonymous Justice Department source, further reported that, "[i]n certain circumstances beaconing could be legal, as long as the concealed software wouldn't do other things like allow a company to access information on the system where the stolen data were stored."[47]

[11] Another important consideration is the fact that beaconing may fall within one of the active defense definitions (*supra*) as "deception."[48] Although deception is recognized as both a common and effective investigative technique,[49] the problem is the possibility that the activities of the investigator could be imputed under Model Rule of Professional Conduct 5.3 to one or more attorneys responsible for directing or approving of those activities.[50] Under Model Rule 8.4(c), neither an attorney nor an attorney's agent under his or her direction or control may "engage in conduct involving dishonesty, fraud, deceit, or

[45] *Id.*

[46] *Id.*

[47] *Id.*

[48] *See* Harrington, *supra* note 41, at 362-64.

[49] The Supreme Court has tacitly approved deception as a valid law enforcement technique in investigations and interrogations. *See* Illinois v. Perkins, 496 U.S. 292, 297 (1990) ("*Miranda* forbids coercion, not mere strategic deception . . ."); United States v. Russell, 411 U.S. 423, 434 (1973) ("Criminal activity is such that stealth and strategy are necessary weapons in the arsenal of the police officer."); Allan Lengel, *Fed Agents Going Undercover on Social Networks Like Facebook*, AOLNEWS (Mar. 28, 2010, 5:55 PM), http://www.ticklethewire.com/2010/03/28/fed-agents-going-undercover-on-social-networks-like-facebook/.

[50] *See* MODEL RULES OF PROF'L CONDUCT R. 5.3 (2013).

misrepresentation."[51] Although the question of whether deception, as contemplated in Rule 8.4, exists in the context of incident response or network forensics investigations is not well settled,[52] most states have held "[t]here are circumstances where failure to make a disclosure is the equivalent of an affirmative misrepresentation."[53] A few state bar associations have already addressed similar technology-related ethical pitfalls. The Philadelphia Bar Association Professional Guidance Committee advised in Opinion 2009–02 that an attorney who asks an agent (such as an investigator) to "friend" a party in Facebook in order to obtain access to that party's non-public information, would violate, among others, Rule 5.3 of the Pennsylvania Rules of Professional Conduct.[54] Likewise, the Association of the Bar of the City of New York Committee on Professional and Judicial Ethics issued Formal Opinion 2010–2, which provides that a lawyer violates, among others, New York Rules of

[51] MODEL RULES OF PROF'L CONDUCT R. 8.4(c); *see, e.g.*, *In re* Disciplinary Action Against Carlson, No. A13-1091 (Minn. July 11, 2013) (public reprimand for "falsely posing as a former client of opposing counsel and posting a negative review about opposing counsel on a website, in violation of Minn. R. Prof. Conduct 4.4(a) and 8.4(c)"); *In re* Pautler, 47 P.3d 1175, 1176 (Colo. 2002) (disciplining a prosecutor, who impersonated a public defender in an attempt to induce the surrender of a murder suspect, for an act of deception that violated the Rules of Professional Conduct).

[52] *See* Sharon D. Nelson & John W. Simek, *Muddy Waters: Spyware's Legal and Ethical Implications*, GPSOLO MAG., Jan.-Feb. 2006, http://www.americanbar.org/newsletter/publications/gp_solo_magazine_home/gp_solo_magazine_index/spywarelegalethicalimplications.html ("The legality of spyware is murky, at best. The courts have spoken of it only infrequently, so there is precious little guidance.").

[53] *In re* Disciplinary Action Against Zotaley, 546 N.W.2d 16, 19 (Minn. 1996) (quoting MINN. R. PROF'L CONDUCT 3.3 cmt. 3 (2005)).

[54] *See* PHILA. BAR ASS'N PROF'L GUIDANCE COMM., Op. 2009-02, at 1-2 (2009), *available at* http://www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf.

Professional Conduct Rule 5.3, if an attorney employs an agent to engage in the deception of "friending" a party under false pretenses to obtain evidence from a social networking website.[55]

B. Threat Counter-Intelligence Gathering

[12] One of the most seemingly-innocuous active defense activities is intelligence gathering. Security analyst David Bianco defines threat intelligence as "[c]onsuming information about adversaries, tools or techniques and applying this to incoming data to identify malicious activity."[56] Threat intelligence gathering ranges from everything from reverse malware analysis and attribution to monitoring inbound and outbound corporate e-mail to more risky endeavors.[57] Some security

[55] *See* N.Y.C. BAR ASS'N PROF'L & JUDICIAL ETHICS COMM., Formal Op. 2010-2 (2010), *available at* http://www2.nycbar.org/Publications/reports/show_html.php?rid=1134; *cf.* Justin P. Murphy & Adrian Fontecilla, *Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues*, 19 RICH. J.L. & TECH. 11, ¶ 21 n.76 (2013) (citing similar ethics opinions rendered by bar committees in New York State and San Diego County).

[56] David Bianco, *Use of the Term "Intelligence" in the RSA 2014 Expo*, ENTERPRISE DETECTION & RESPONSE (Feb. 28, 2014) http://detect-respond.blogspot.com/#!/2014/03/use-of-term-intelligence-at-rsa.html.

[57] *See* Sameer, *supra* note 36, at 15 (citing A. Meehan, G. Manes, L. Davis, J. Hale & S. Shenoi, *Packet Sniffing for Automated Chat Room Monitoring and Evidence Preservation*, *in* PROCEEDINGS OF THE 2001 IEEE WORKSHOP ON INFORMATION ASSURANCE AND SECURITY 285, 285 (2001)) ("[T]he monitoring of bulletin-boards and chat-rooms by investigators has led to the detection and apprehension of those who participate in sex crimes against children."), *available at* http://index-of.es/Sniffers/Sniffers_pdf/52463601-packet-sniffing-for-automated-chat-room-74909.pdf; *see, e.g.*, Kimberly J. Mitchell, Janis Wolak & David Finkelhor, *Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?*, 17 SEXUAL ABUSE: J. RES. & TREATMENT 241 (2005); Lyta Penna, Andrew Clark & George Mohay, *Challenges of Automating the Detection of Paedophile Activity on the Internet*, *in Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering* (2005), *available at* http://eprints.qut.edu.au/20860/1/penna2005sadfe.pdf.

experts claim to frequent "Internet store fronts" for malware, "after carefully cloaking [their] identity to remain anonymous."[58] The reality, however, is that gaining access to and remaining on these black market fora requires the surreptitious visitor either to: (1) participate ("pay to play"); (2) to have developed a reputation over months or years, or founded the underground forum *ab initio*; or (3) to have befriended or been extended a personal invitation by an established member. The first two of these three activities implies that the participant would have co-conspirator or accomplice liability in the underlying crimes. Another risk is, if the site is reputed to also purvey child pornography, a court may find that the site visitor acquired possession (even as temporary Internet cache) of the contraband knowingly, even if the true intent of lurking was to gather intelligence.[59] Another obvious risk is that surreptitious monitoring of hacker sites using false credentials or representations is an act of deception which, for the reasons more fully set forth above, could create disciplinary liability for any attorneys who are involved or acquiesce to the activity.

[58] Martin Moylan, *Target's Data Breach Link to 'the Amazon of Stolen Credit Card Information'*, MPRNEWS (February 3, 2014), http://www.mprnews.org/story/2014/02/02/stolen-credit-and-debit-card-numbers-are-just-a-few-clicks-away.

[59] *See* "Investigating the Dark Web — The Challenges of Online Anonymity for Digital Forensics Examiners," FORENSIC FOCUS (July 28, 2014) ("It is certainly easier to access indecent images of children and similar content on the dark net.") Available at http://articles.forensicfocus.com/2014/07/28/investigating-the-dark-web-the-challenges-of-online-anonymity-for-digital-forensics-examiners/. *And see, e.g.*, MINN. STAT. § 617.247 subd. 4(a) (2013) (criminalizing possession of "a pornographic work [involving minors] or a computer disk or computer or other electronic, magnetic, or optical storage system or a storage system of any other type, containing a pornographic work, knowing or with reason to know its content and character").

C. Sinkholing

[13] Sinkholing is the impersonation of a botnet command-and-control server in order to intercept and receive malicious traffic from its clients.[60] To accomplish this, either the domain registrar must redirect the domain name to the investigator's machine (which only works when the connection is based on a DNS name), or the Internet Service Provider (ISP) must redirect an existing IP address to the investigator's machine (possible only if the investigator's machine is located in the IP range of the same provider), or the ISP must redirect all traffic destined for an IP address to the investigator's machine, instead (the "walled garden" approach).[61]

[14] Sinkholing involves the same issues of deception discussed *ante*, but also relies on the domain registrar's willingness and legal ability to assist. As Link and Sancho point out in their paper *Lessons Learned While Sinkholing Botnets—Not as Easy as it Looks!*, "[u]nless there is a court order that compels them to comply with such a request, without the explicit consent of the owner/end-user of the domain, the registrar is unable to grant such requests."[62] Doubtless they were referring to the Wiretap Act (Title 1 of the Electronic Communications Privacy Act), which generally prohibits unconsented interception (contemporaneous with transmission), disclosure, or use of electronic communications.[63]

---

[60] *See* Rainer Link & David Sancho, *Lessons Learned While Sinkholing Botnets—Not As Easy As It Looks!*, *in* PROCEEDINGS OF THE VIRUS BULLETIN CONFERENCE 106, 106 (2011), *available at* http://www.trendmicro.com/media/misc/lessons-learned-virusbulletin-conf-en.pdf.

[61] *Id.*

[62] *Id.* at 107.

[63] "[C]onsent may be demonstrated through evidence of appropriate notice to users through service terms, privacy policies or similar disclosures that inform users of the potential for monitoring." Bosset et.al, *supra* note 4 (citing Mortensen v. Bresnan

Further, a federal district court recently ruled that intentionally circumventing an IP address blacklist in order to crawl an otherwise-publicly available website constitutes "access without authorization" under the CFAA.[64] Link and Sancho continue that registrars have little incentive to assist because it does not generate revenue, and note that sinkholing invites distributed denial of service ("DDoS") retaliation which could affect other customers of a cloud-provided broadband connection.[65] Finally, sinkholing is likely to collect significant amounts of data, including personally identifiable information ("PII"). The entity collecting PII is likely to be subject to the data privacy, handling, and disclosure laws of all the jurisdictions whence the data came.

D. Honeypots

[15] A honeypot is defined as "a computer system on the Internet that is expressly set up to attract and 'trap' people who attempt to penetrate other people's computer systems."[66] It may be best thought of as "an information system resource whose value lies in unauthorized or illicit use of that resource."[67] Honeypots do arguably involve deception, but have been in use for a comparatively long time, and are generally accepted as a valid information security tactic (therefore, relatively free from controversy). The legal risks, historically, have been identified as: (1)

Commc'ns, LLC, No. CV 10-13-BLG-RFC, 2010 WL 5140454, at *3-5 (D. Mont. Dec. 13, 2010)).

[64] *See* Craigslist Inc. v. 3Taps Inc., 964 F. Supp. 2d 1178, 1182-83 (N.D. Cal. 2013).

[65] *See* Link & Sancho, *supra* note 60, at 107-08.

[66] *Honeypot*, SEARCHSECURITY, http://searchsecurity.techtarget.com/definition/honey-pot (last visited June 29, 2014).

[67] Eric Cole & Stephen Northcutt, *Honeypots: A Security Manager's Guide to Honeypots*, SANS INST., http://www.sans.edu/research/security-laboratory/article/honeypots-guide (last visited May 13, 2014).

potential violations of the ECPA;[68] and (2) possibly creating an entrapment defense for the intruder.[69] Neither of these is applicable here, because, respectively: (1) the context of the deployment discussed herein is the corporate entity as the honeypot owner (thus, a party to the wire communication); and (2) the corporate entity is not an agent of law enforcement, and, further, the entrapment defense is only available when defendant was not predisposed to commit the crime (here, a hacker intruding into a honeypot is predisposed).[70] Nevertheless, Justice Department attorney Richard Salgado, speaking at the Black Hat Briefings, did reportedly warn that the law regarding honeypots is "untested" and that entities implementing devices or networks designed to attract hackers could face such legal issues as liability for an attack launched from a compromised honeypot.[71] This possibility was discussed six years ago:

> If a hacker compromises a system in which the owner has not taken reasonable care to secure and uses it to launch an attack against a third party, the owner of that system may be liable to the third party for negligence. Experts refer to this scenario as "downstream liability." Although a case has yet to arise in the courts, honeypot operators may be especially vulnerable to downstream liability claims since it

[68] *See, e.g.*, JEROME RADCLIFFE, CYBERLAW 101: A PRIMER ON US LAWS RELATED TO HONEYPOT DEPLOYMENTS 6-9 (2007), *available at* http://www.sans.org/reading-room/whitepapers/legal/cyberlaw-101-primer-laws-related-honeypot-deployments-1746.

[69] *See id.* at 14-17.

[70] *See* Schaufenbuel, *supra* note 34, at 16-17 ("Because a hacker finds a honeypot by actively searching the Internet for vulnerable hosts, and then attacks it without active encouragement by law enforcement officials, the defense of entrapment is not likely to be helpful to a hacker.").

[71] *See* Cole & Northcutt, *supra* note 67.

> is highly foreseeable that such a system be misused in this manner.[72]

Another honeypot risk is the unintended consequence of becoming a directed target because the honeypot provoked or attracted hackers to the company that deployed it, which hackers might otherwise have moved on to easier targets. Another is that an improperly configured honeypot could ensnare an innocent third party or customer and collect legally-protected information (such as PII). If that information is not handled according to applicable law, the owner of the honeypot could incur statutory liabilities therefor.[73] And yet another scenario is one that, perhaps, only a lawyer would recognize as a risk: "[i]f you have a honeypot and do learn a lot from it but don't remedy or correct it, then there's a record that is discoverable and that you knew you had a problem and didn't [timely] fix it."[74]

[16] Finally, there are uses for honeypots which, when regarded as a source of revenue by its owners, have the potential to cause substantial injury to brand image and reputation, and possibly court sanctions: one law firm has been accused of seeding the very copyrighted content it was retained to protect, which the firm used as evidence in copyright suits it prosecuted.[75] Because of these alleged activities, the firm has been

[72] Schaufenbuel, *supra* note 34, at 19.

[73] *See generally id.* (stating that the best way for a honeypot owner to avoid downstream liability is to configure the honeypot to prohibit or limit outbound connections to third parties).

[74] Scott L. Vernick, *To Catch a Hacker, Companies Start to Think Like One*, FOX ROTHSCHILD, LLP (Feb. 15, 2013), http://www.foxrothschild.com/print/convertToPDF.aspx?path=/newspubs/newspubsprint.aspx&parms=id|15032388757.

[75] *See* Kevin Parrish, *Copyright Troll Busted for Seeding on The Pirate Bay*, TOM'S GUIDE (Aug. 19, 2013, 2:00 PM), http://www.tomsguide.com/us/torrent-pirate-bay-copyright-troll-prenda-law-honeypot,news-17391.html#torrent-pirate-bay-copyright-troll-

labelled a "copyright troll."[76] The allegations, if proved true, also appear to involve acts of deception, discussed *ante*, which may subject the firm's attorneys to attorney disciplinary proceedings.[77] Further, the firm's attorneys may incur other possible liabilities, such as vexatious and frivolous filing sanctions, abuse of process, barratry, or champerty.[78]

E. Retaliatory Hacking

[17] A common belief for why corporations have little to fear in the way of prosecution for retaliatory hacking is, "criminals don't call the cops."[79] Nevertheless, there is little debate that affirmative retaliatory hacking is unlawful,[80] even if done in the interests of national security.[81]

---

prenda-law-honeypot%2Cnews-17391.html?&_suid=139637099057702274079508184874 7.

[76] *Id.*

[77] *See id.*

[78] *See, e.g.*, Sean L. Harrington, *Rule 11, Barratry, Champerty, and "Inline Links*", MINN. ST. BAR ASS'N COMPUTER & TECH. L. SEC. (Jan. 27, 2011, 11:42 PM), http://mntech.typepad.com/msba/2011/01/rule-11-barratry-champerty-and-inline-links.html (discussing the vexatious litigation tactics of Righthaven, LLC).

[79] *See* Scott Cohn, *Companies Battle Cyberattacks Using 'Hack Back'*, CNBC (June 04, 2013, 1:00 PM), http://www.cnbc.com/id/100788881 ("[L]aw enforcement is unlikely to detect or prosecute a hack back. 'If the only organization that gets harmed is a number of criminals' computers, I don't think it would be of great interest to law enforcement."); Aarti Shahani, *Tech Debate: Can Companies Hack Back?*, AL JAZEERA AM. (Sept. 18, 2013, 5:57 PM), http://america.aljazeera.com/articles/2013/9/18/tech-debate-can-companieshackback.html ("The Justice Department has not prosecuted any firm for hacking back and, as a matter of policy, will not say if any criminal investigations are pending").

[80] *See* Cohn, *supra* note 79 (statement of Professor Joel Reidenberg) ("'Reverse hacking is a felony in the United States, just as the initial hacking was. It's sort of like, if someone steals your phone, it doesn't mean you're allowed to break into their house and take it back.'"); Shahani, *supra* note 79 (statement of David Wilson) ("'No, it's not legal, not

Although there may be "little debate," there is debate.[82] The views of many passionate information security analysts could be summed up by authors John Strand and Paul Asadoorian, who argue, "[c]urrently, our only defense tools are the same tools we have had for the past 10+ years, and they are failing."[83] David Willson, the owner and president of Titan Info Security Group, and a retired Army JAG, contends that using "automated tools outside of your own network to defend against attacks by innocent but compromised machines" is not gaining unauthorized access or a computer trespass, and he asks, "[i]f it is, how is it different from the adware, spam, cookies, or others that load on your machine without your knowledge, or at least with passive consent?"[84] Willson provides a typical scenario and then examines the statutory language of the CFAA and offers some possible arguments—but notes his arguments bear stretch marks

unless the blackmailer gave permission. . . . But who's going to report it? Not the bad guy.'").

[81] *See, e.g.*, Nathan Thornburgh, *The Invasion of the Chinese Cyberspies (and the Man Who Tried to Stop Them)*, TIME (Sept. 5, 2005), http://courses.cs.washington.edu/courses/csep590/05au/readings/titan.rain.htm (discussing the "rogue" counter-hacking activities of Shawn Carpenter, who was working with the FBI and for whose activities Carpenter claimed the FBI considered prosecuting him).

[82] *See* Dilanian, *supra* note 7 ("Others, including Stewart Baker, former NSA general counsel, said the law does allow hacking back in self-defense. A company that saw its stolen data on a foreign server was allowed to retrieve it, Baker argued.") (In preparation for this comment, the author asked Mr. Baker about the interview, and he replied, "[T]he *LA Times* interview didn't involve me talking about a particular case where retrieving data was legal. I was arguing that it should be legal.").

[83] JOHN STRAND ET AL., OFFENSIVE COUNTERMEASURES: THE ART OF ACTIVE DEFENSE 207 (2013).

[84] David Willson, *Hacking Back in Self Defense: Is It Legal; Should It Be?*, GLOBAL KNOWLEDGE (Jan. 6, 2012), http://blog.globalknowledge.com/technology/security/hacking-cybercrime/hacking-back-in-self-defense-is-it-legal-should-it-be/.

(and he makes no offer of indemnification should practitioners decide to use them).[85]

[18] Willson is not alone in searching for leeway within the CFAA. Stewart Baker, former NSA general counsel, argues on his blog,

> Does the CFAA, prohibit counterhacking? The use of the words "may be illegal," and "should not" are a clue that the law is at best ambiguous. . . . [V]iolations of the CFAA depend on "authorization." If you have authorization, it's nearly impossible to violate the CFAA . . . [b]ut the CFAA doesn't define "authorization." . . . The more difficult question is whether you're "authorized" to hack into the attacker's machine to extract information about him and to trace your files. As far as I know, that question has never been litigated, and Congress's silence on the meaning of "authorization" allows both sides to make very different arguments. . . . [C]omputer hackers won't be bringing many lawsuits against their victims. The real question is whether victims can be criminally prosecuted for breaking into their attacker's machine.[86]

Other theories —and assorted arguments bearing stretch marks— analogize retaliatory hacking as subject to the recapture of chattels privilege,[87] entry upon land to remove chattels,[88] private necessity,[89] or

[85] *See id.*

[86] Stewart Baker, *The Hack Back Debate* (Nov. 02, 2012) http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/.

[87] *See* W. PAGE KEETON ET AL., PROSSER & KEETON ON THE LAW OF TORTS § 22 (5th ed. 1984).

[88] *See id.*

even the castle doctrine.[90] Jassandra K. Nanini, a cybersecurity law specialist, suggests applying the "security guard doctrine" as an analogy.[91] She posits that, if private actors act independently of law enforcement and have a valid purpose for their security activities that remains separate from law enforcement, then incidental use of evidence gained through those activities by law enforcement is permissible, even if the security guard acted unreasonably (as long as he remained within the confines of the purpose of his employer's interests).[92] As applied, Nanini explains the analogy as follows:

> If digital property were considered the same as physical, cyber security guards could "patrol" client networks in search of intruder footprints, and based on sufficient evidence of a breach by a particular hacker, perhaps indicated by the user's ISP, initiate a breach of the invader's network in order to search for compromised data and disable its further use. Even more aggressive attacks designed to plant malware in hacker networks could be considered seizure of an offensive weapon, comparable to a school security guard seizing a handgun from a malicious party. Such proactive defense could use the hacker's own malware to corrupt his systems when he attempts to retrieve the data from the company's system. Certainly all

[89] *See id.* at § 24.

[90] *See id.* at § 21. *And see* McGee, Sabett, & Shah, *supra,* note 18 ("Reaching consensus on applying the concepts of self-defense to the cyber domain has proven to be a difficult task, though not for the lack of trying").

[91] *See* Jassandra Nanini, *China, Google, and Private Security: Can Hack-Backs Provide the Missing Defense in Cybersecurity*, (forthcoming 2015) (manuscript at 14-15) (on file with author).

[92] *See id.* (manuscript at 14).

> of these activities are within the scope of the company's valid interest, which include maintaining data integrity, preventing use of stolen data, and disabling further attack. . . . Similarly, companies may wholly lack any consideration of collecting evidence for legal recourse, keeping in step with the private interest requirement of the private security guard doctrine in general. All hack-backs could be executed without any support or direction from law enforcement, opening the door to utilization of evidence in a future prosecution against the hacker. [93]

The foregoing theories notwithstanding, what is clear is that obtaining evidence by use of a keylogger, spyware, or persistent cookies likely is violative of state and federal laws, such as the CFAA or ECPA.[94] The CFAA, last amended in 2008, criminalizes anyone who commits, attempts to commit, or conspires to commit an offense under the Act, including offenses such as knowingly accessing without authorization a protected computer (for delineated purposes) or intentionally accessing a computer without authorization (for separately delineated purposes).[95] Relevant statutory phrases, such as "without authorization" and "access," have been the continuing subject of appellate review.[96] One federal court, referring

[93] *Id.* (manuscript at 15-16).

[94] *See* Sean Harrington, *Why Divorce Lawyers Should Get Up to Speed on CyberCrime Law*, MINN. ST. B. ASS'N COMPUTER & TECH. L. SEC. (Mar. 24, 2010, 9:40 PM), http://mntech.typepad.com/msba/2010/03/why-divorce-lawyers-should-get-up-to-speed-on-cybercrime-law.html (collecting cases regarding unauthorized computer access).

[95] 18 U.S.C. § 1030 (2012); *see* Clements-Jeffrey v. Springfield, 810 F. Supp. 2d 857, 874 (S.D. Ohio 2011) ("It is one thing to cause a stolen computer to report its IP address or its geographical location in an effort to track it down. It is something entirely different to violate federal wiretapping laws by intercepting the electronic communications of the person using the stolen laptop.").

[96] *See generally* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1624–42 (2003)

to both the ECPA and CFAA, pointed out that "the histories of these statutes reveal specific Congressional goals—*punishing destructive hacking*, preventing wiretapping for criminal or tortious purposes, securing the operations of electronic communication service providers—that are carefully embodied in these criminal statutes and their corresponding civil rights of action."[97] At least one court has held that the use of persistent tracking cookies is a violation of the Electronic Communications Privacy Act.[98] Congress is currently considering reform to the CFAA, as well as comprehensive privacy legislation that would, in some circumstances, afford a private right of action to consumers whose personal information is collected without their consent. [99]

[19] Regardless of the frequency with which retaliatory hacking charges have been brought, one issue that has not yet been included in the debate involves illegally obtained evidence that is inadmissible. This matters because bringing suit under the CFAA or ECPA is a remedy that corporate victims have recently invoked increasingly.[100]

(showing how and why courts have construed unauthorized access statutes in an overly broad manner that threatens to criminalize a surprising range of innocuous conduct involving computers).

[97] In re DoubleClick Privacy Litig., 154 F. Supp. 2d 497, 526 (S.D.N.Y. 2001) (emphasis added).

[98] *See* In re Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 13 & 21-22 (1st Cir. 2003) (holding use of tracking cookies to intercept electronic communications was within the meaning of the ECPA, because the acquisition occurred simultaneously with the communication).

[99] *See* Peter J. Toren, *Amending the Computer Fraud and Abuse Act*, BNA (Apr. 9, 2013), http://about.bloomberglaw.com/practitioner-contributions/amending-the-computer-fraud-and-abuse-act/.

[100] *See, e.g.*, Holly R. Rogers & Katharine V. Hartman, *The Computer Fraud and Abuse Act: A Weapon Against Employees Who Steal Trade Secrets*, BNA (June 21, 2011) ("[E]mployers are increasingly using this cause of action to go after former employees who steal trade secrets from their company-issued computers.").

[20] Another liability —the one most frequently cited— is that of misattribution and collateral damage:

> [E]ncouraging digital vigilantes will only make the mayhem worse. Hackers like to cover their tracks by routing attacks through other people's computers, without the owners' knowledge. That raises the alarming prospect of collateral damage to an innocent bystander's systems: imagine the possible consequences if the unwitting host of a battle between hackers and counter-hackers were a hospital's computer.[101]

Likewise, Representative Mike Rogers (R-MI), sponsor for the Cyber Intelligence Sharing and Protection Act (CISPA) and Chair of the House Permanent Select Committee on Intelligence, warned private corporations against going on the offensive as part of their cyber security programs: "You don't want to attack the wrong place or disrupt the wrong place for somebody who didn't perpetrate a crime."[102] Contemplate the civil

[101] *A Byte for a Byte*, ECONOMIST (Aug. 10, 2013), *available at* http://www.economist.com/node/21583268/; *see also* Lewis, *supra* note 21 ("There is also considerable risk that amateur cyber warriors will lack the skills or the judgment to avoid collateral damage. A careless attack could put more than the intended target at risk. A nation has sovereign privileges in the use of force. Companies do not."); John Reed, *The Cyber Security Recommendations of Blair and Huntsman's Report on Chinese IP Theft*, COMPLEX FOREIGN POL'Y (May 22, 2012), http://complex.foreignpolicy.com/posts/2013/05/22/the_cyber_security_recomendations_of_blair_and huntsman_report_on_chinese_ip_theft ("While it may be nice to punch back at a hacker and take down his or her networks or even computers, there's a big potential for collateral damage, especially if the hackers are using hijacked computers belonging to innocent bystanders.").

[102] John Reed, *Mike Rogers: Cool It with Offensive Cyber Ops*, COMPLEX FOREIGN POL'Y (Dec. 14, 2012, 5:07 PM), http:/complex.foreignpolicy.com/posts/2012/12/14/mike_rogers_cool_it_with_offensive_cyber_ops (audio recording of full speech *available at* http://www.c-

liabilities that one could incur if, in an effort to take down a botnet through self-help and vigilantism, the damaged computers belonged to customers, competitors, or competitors' customers. Aside from the financial losses and injury to brand reputation and goodwill, implicated financial institutions could expect increased regulatory scrutiny and could compromise government contracts subject to FISMA.

[21] Yet another frequently discussed liability is that of escalation: cybercrime is perpetrated by many different attacker profiles of persons and entities, including cyber-terrorists, cyber-spies, cyber-thieves, cyber-warriors, and cyber-hactivists.[103] Because the purported motivation of a cyber-hactivist is *principle,* retaliation by the corporate victim may be received as an invitation to return fire and escalate. Similarly, "[e]ncouraging corporations to compete with the Russian mafia or Chinese military hackers to see who can go further in violating the law . . . is not a contest American companies can win."[104] Conversely, the motivation of a cyber-thief is *principal and interest,* so retaliation by the target might be taken as a suggestion to move on to an easier target. Because the perpetrators are usually anonymous, the corporate victim has no way to make a risk-based and proportional response premised upon the classification of the attacker as nation-state, thief, or hactivist.

---

span.org/video?314114-1/rep-rogers-rmi-addresses-cyber-threats-economy). *But see See* McGee, Sabett, & Shah, *supra,* note 18 (urging the adoption of a "Framework for 'good enough' attribution").

[103] For definitions and discussion of these terms, see ERIC A. FISCHER ET AL., CONG. RESEARCH SERV., R42984, THE 2013 CYBERSECURITY EXECUTIVE ORDER: OVERVIEW AND CONSIDERATIONS FOR CONGRESS 2-4, (2013), *available at* http://www.fas.org/sgp/crs/misc/R42984.pdf.

[104] Max Fisher, *Should the U.S. Allow Companies to 'Hack Back' Against Foreign Cyber Spies?,* WASH. POST (May 23, 2013, 10:43 AM), http://www.washingtonpost.com/blogs/worldviews/wp/2013/05/23/should-the-u-s-allow-companies-to-hack-back-against-foreign-cyber-spies/ (quoting Lewis, *supra,* note 21).

> [I]n cyberspace attribution is a little harder. On the playground you can see the person who hit you . . . well, almost always[,] . . . in cyberspace we can track IP addresses and TTPs from specific threat actors, which smart analysts and researchers tell us is a viable way to perform attribution. I agree with them, largely, but there's a fault there. An IP address belonging to China SQL injecting your enterprise applications is hardly a smoking gun that Chinese APTs are after you. Attackers have been using others' modus operandi to mask their identities for as long as spy games have been played. Attackers have been known to use compromised machines and proxies in hostile countries for as long as I can remember caring—to "bounce through" to attack you. Heck, many of the attacks that appear to be originating from nation-states that we suspect are hacking us may very well be coming from a hacker at the coffee house next door to your office, using multiple proxies to mask their true origin. This is just good OpSec, and attackers use this method all the time, let's not kid ourselves.[105]

If, without conclusive attribution and intelligence, the corporate victim is unable to make a risk-based and proportional response, it may be reasonable to question whether retaliatory hacking is abandoning the risk-based approach to business problems exhorted by FFIEC,[106] PCI,[107] and

[105] Los, *supra* note 19.

[106] *See* Fahmida Y. Rashid, *Layered Security Essential Tactic of Latest FFIEC Banking Guidelines*, EWEEK (June 30, 2011), http://www.eweek.com/c/a/IT-Infrastructure/Layered-Security-Essential-Tactic-of-Latest-FFIEC-Banking-Guidelines-557743/ ("Banks must adopt a layered approach to security in order to combat highly sophisticated cyber-attacks, the Federal Financial Institutions Examination Council said in a supplement released June 28. The new rules update the 2005 'Authentication in an Internet Banking Environment' guidance to reflect new security measures banks need to

the NIST Cybersecurity Framework?[108] "If we start using those sort of [cyber weapons], it doesn't take much to turn them against us, and we are tremendously vulnerable," said Howard Schmidt, a former White House cyber security coordinator.[109]

[22] Then there is the often overlooked issue of professional ethics—not for the attorney—but for the information security professional. "Ethics," a term derived from the ancient Greek *ethikos* (ἠθικός), has been defined as "a custom or usage."[110] Modernly, ethics is understood to be "[professional] norms shared by a group on a basis of mutual and usually reciprocal recognition."[111] The codes of ethics provide articulable principles against which one's decision-making is objectively measured, and serve other important interests, including presenting an image of

fend off increasingly sophisticated attacks. . . . The guidance . . . emphasized a risk-based approach in which controls are strengthened as risks increase.").

[107] *See PCI 2.0 Encourages Risk-Based Process: Three Things You Need to Know*, ITGRC (Aug. 23, 2010), http://itgrcblog.com/2010/08/23/pci-2-0-encourages-risk-based-process-three-things-you-need-to-know/.

[108] *See* Lee Vorthman, *IT Security: NIST's Cybersecurity Framework*, NETAPP (July 16, 2013, 6:01 AM), https://communities.netapp.com/community/netapp-blogs/government-gurus/blog/2013/07/16/it-security-nists-cybersecurity-framework) ("It is widely anticipated that the Cybersecurity Framework will improve upon the current shortcomings of FISMA by adopting several controls for continuous monitoring and by allowing agencies to move away from compliance-based assessments towards a real-time risk-based approach.").

[109] Reed, *supra* note 102.

[110] Geoffrey C. Hazard, Jr., *Law, Morals, and Ethics*, 19 S. ILL. U. L.J. 447, 453 (1995), *available at* http://repository.uchastings.edu/faculty_scholarship/252.

[111] *Id.*

prestige and credibility for the organization and the profession,[112] eliminating unfair competition,[113] and fostering cooperation among professionals.[114]

[23] Many information security professionals are certified by the International Information Systems Security Certification Consortium ((ISC)$^{2®}$). The (ISC)$^{2®}$ Committee has recognized its responsibility to provide guidance for "resolving good versus good, and bad versus bad, dilemmas," and "to encourage right behavior."[115] The Committee also has the responsibility to discourage certain behaviors, such as raising unnecessary alarm, fear, uncertainty, or doubt; giving unwarranted

---

[112] *See generally* HEINZ C. LUEGENBIEHL & MICHAEL DAVIS, ENGINEERING CODES OF ETHICS: ANALYSIS AND APPLICATIONS 10 (1986) (referring to the "Contract with society" theory on the relation between professions and codes of ethics).

> According to this approach, a code of ethics is one of those things a group must have before society will recognize it as a profession. The contents of the code are settled by considering what society would accept in exchange for such benefits of professionalism as high income and high prestige. A code is a way to win the advantages society grants only to those imposing certain restraints on themselves.

Id.

[113] *See, e.g.*, OFFICIAL (ISC)^2 GUIDE TO THE CISSP CBK 1214 (Steven Hernandez ed., 3d ed. 2013) ("The code helps to protect professionals from certain stresses and pressures (such as the pressure to cut corners with information security to save money) by making it reasonably likely that most other members of the profession will not take advantage of the resulting conduct of such pressures. An ethics code also protects members of a profession from certain consequences of competition, and encourages cooperation and support among the professionals.").

[114] *See id.*

[115] (ISC)^2, (ISC)^2 OVERVIEW: EVOLVING IN TODAY'S COMPLEX SECURITY LANDSCAPE 4 (2013), *available at* www.infosec.co.uk/_novadocuments/47180?v=635294483175930000.

comfort or reassurance; consenting to bad practice; attaching weak systems to the public network; professional association with non-professionals; professional recognition of, or association with, amateurs; or associating or appearing to associate with criminals or criminal behavior.[116] Therefore, an information security professional bound by this code who undertakes active defense activities that he or she knows or should know are unlawful, or proceeds where the legality of such behavior not clear, may be in violation the Code.

[24] It would stand to reason that, an organization that empowers, directs, or acquiesces to conduct by its employees that violates the (ISC) Code of Ethics may violate its own corporate ethics or otherwise compromise its ethical standing in the corporate community—or not: when Google launched a "secret counter-offensive" and "managed to gain access to a computer in Taiwan that it suspected of being the source of the attacks,"[117] tech sources praised Google's bold action.[118]

[25] Nevertheless, corporate ethics is an indispensable consideration in the hack back debate. The code of ethics and business conduct for financial institutions should reflect and reinforce corporate values, including uncompromising integrity, respect, responsibility and good citizenship. As noted above, retaliatory hacking is deceptive and has been characterized as reckless, and even Web bugs are commonly associated with spammers. Corporate management must consider whether resorting to techniques pioneered by and associated with criminals or spammers has

[116] *See id.*

[117] David E. Sanger & John Markoff, *After Google's Stand on China, U.S. Treads Lightly*, N.Y. TIMES (Jan. 15, 2010), http://www.nytimes.com/2010/01/15/world/asia/15diplo.html?_r=0.

[118] *See, e.g.*, Skipper Eye, *Google Gives Chinese Hackers a Tit for Tat*, REDMOND PIE (Jan. 16, 2010), *available at* http://www.redmondpie.com/google-gives-chinese-hackers-a-tit-for-tat-9140352/.

the potential to compromise brand image in the eyes of existing and prospective customers. Similarly, to the extent that financial corporations are engaging in active defense covertly,[119] corporate management must consider whether customers' confidence in the security of their data and investments could be shaken when such activities are uncovered. Will customers wonder whether their data has been placed at risk because of escalation? Will shareholders question whether such practices are within the scope of good corporate stewardship?

III. ALTERNATIVES TO RETALIATORY HACKING

[26] The obvious argument in support of active defense is that the law and governments are doing little to protect private corporations and persons from cybercrime, which has inexorably resulted in resort to self-help,[120] and those who vociferously counsel to refrain from active defense often have little advice on alternatives. At the risk of pointing out the obvious, one counsels, "'when you look at active defense, we need to focus on reducing our vulnerabilities.'"[121]

[27] Alternatives to hacking back are evolving, and one of the more promising is the pioneering threat intelligence gathering and sharing from the Financial Services Information Sharing and Analysis Center ("FS-

[119] *See* Shelley Boose, *Black Hat Survey: 36% of Information Security Professionals Have Engaged in Retaliatory Hacking*, BUSINESSWIRE (June 26, 2012, 11:00 AM), http://www.businesswire.com/news/home/20120726006045/en/Black-Hat-Survey-36-Information-Security-Professionals ("When asked 'Have you ever engaged in retaliatory hacking?' 64% said 'never,' 23% said 'once,' and 13% said 'frequently". . . . [W]e should take these survey results with a grain of salt . . . . It's safe to assume some respondents don't want to admit they use retaliatory tactics.").

[120] Lewis, *supra* note 21 ("Another argument is that governments are not taking action, and therefore private actors must step in.").

[121] Reed, *supra* note 102.

ISAC"), which collects information about threats and vulnerabilities from its 4,400 FI members, government partners, and special relationships with Microsoft®, iSIGHT Partners℠, Secunia, *et al.*, anonymizes the data, and distributes it back to members.[122] In addition to e-mail alerts and a Web portal, FS-ISAC holds regular tele-conferences during which vulnerability and threat information is discussed, and during which presentations on current topics are given.[123] The FS-ISAC recently launched a security automation project to eliminate manual processes to collect and distribute cyber threat information, according to Bill Nelson, the Center's director.[124] The objective of the project is to significantly reduce operating costs and lower fraud losses for financial institutions, by consuming threat information on a real-time basis.[125]

[28] Although, as *American Banker* wryly observes, "[b]ankers have never been too keen on sharing secrets with one another," [126] dire

[122] *See About FS-ISAC*, FIN. SERV.: INFO. SHARING & ANALYSIS CENTER, https://www.fsisac.com/about (last visited June 9, 2014). Launched in 1999, FS-ISAC was established by the financial services sector in response to 1998's Presidential Directive 63. That directive — later updated by 2003's Homeland Security Presidential Directive 7 — mandated that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the U.S. critical infrastructure. *See id.*

[123] *See id.*

[124] *FS-ISAC Security Automation Working Group Continues to Mature Automated Threat Intelligence Strategy, Deliver on Multi-Year Roadmap*, FIN. SERV.: INFO. SHARING & ANALYSIS CENTER (Feb. 26, 2014), https://www.fsisac.com/sites/default/files/news/FSISAC_PR_SAWG_Feb19-2014v1AH%20-%20DHE-ALL-EDITS-FINAL2%20EG.pdf.

[125] *See id.*

[126] Sean Sposito, *In Cyber Security Fight, Collaboration Is Key: Guardian Analytics*, AM. BANKER (Oct. 08. 2013, 2:01 PM), http://www.americanbanker.com/issues/178_195/in-cyber-security-fight-collaboration-is-key-guardian-analytics-1062688-1.html.

circumstances have catalyzed a new era of cooperation, paving the way for the success of the cooperative model developed by the FS-ISAC—even before its current ambitious automation project, which has resulted in successful botnet takedown operations.[127] An illustrative example is the Citadel malware botnet takedown, where Microsoft's Digital Crimes Unit, in collaboration with the FS-ISAC, the Federal Bureau of Investigation, the American Bankers Association, NACHA—The Electronic Payments Association, and others, executed a simultaneous operation to disrupt more than 1,400 Citadel botnets reportedly responsible for over half a billion dollars in losses worldwide.[128] With the assistance of U.S. Marshals, data and evidence, including servers, were seized from data hosting facilities in New Jersey and Pennsylvania, and was made possible by a court ordered civil seizure warrant from a U.S. federal court.[129] Microsoft also reported that it shared information about the botnets' operations with international Computer Emergency Response Teams, which can deal with elements of the botnets outside U.S. jurisdiction, and the FBI informed enforcement agencies in those countries.[130] Similar, more recent, operations include one characterized as "major takedown of the Shylock Trojan botnet," which botnet is described as "an advanced cybercriminal infrastructure attacking online banking systems around the world," that reportedly was coordinated by the UK National Crime Agency (NCA), and included Europol, the FBI, BAE Systems Applied

[127] *See generally, Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks: Hearing Before the S. Comm. on the Judiciary*, 113th Cong. (July 15, 2014) http://www.judiciary.senate.gov/meetings/taking-down-botnets_public-and-private-efforts-to-disrupt-and-dismantle-cybercriminal-networks (providing access to testimony from the hearing).

[128] *See* Tracy Kitten, *Microsoft, FBI Take Down Citadel Botnets*, BANK INFO SECURITY (June 6, 2013), http://www.bankinfosecurity.com/microsoft-fbi-takedown-citadel-botnets-a-5819/op-1.

[129] *See id.*

[130] *See id.*

Intelligence, Dell SecureWorks, Kaspersky Lab and the UK's GCHQ,[131] and another takedown operation that targeted the much-feared Cryptolocker.[132] Following the FS-ISAC model, the retail sector has taken the "historic decision" to share data on cyber-threats for the first time through a newly-formed Retail Cyber Intelligence Sharing Center (R-CISC),[133] and the financial services and retail sectors formed a cross-partnership.[134]

[29] Finally, at the time of this publication, a draft Cybersecurity Information-Sharing Act of 2014, advanced by Chairman Dianne Feinstein (D-CA) and ranking member Saxby Chambliss (R-GA), was passed out of the Senate Intelligence on a 12-3 vote, and is expected to be put to a vote in the full Senate.[135] The bill is designed to enhance and

[131] *See NCA Leads Global Shylock Malware Takedown*, INFOSECURITY (July 12, 2014) http://www.infosecurity-magazine.com/view/39289/nca-leads-global-shylock-malware-takedown/.

[132] *See* Gregg Keizer, *Massive Botnet Takedown Stops Spread of Cryptolocker Ransomware*, COMPUTERWORLD (June 5, 2014 02:15 PM), http://www.computerworld.com/s/article/9248872/Massive_botnet_takedown_stops_spread_of_Cryptolocker_ransomware.

[133] John E. Dunn, *Worried US Retailers Battle Cyber-attacks Through New Intelligence-Sharing Body*, TECHWORLD (May 16, 2014, 6:29 PM), http://news.techworld.com/security/3517094/worried-us-retailers-battle-cyber-attacks-through-new-inte/.

[134] *See, e.g.*, Dan Dupont Retail, *Financial Sectors Form Cybersecurity Partnership in Wake of Data Breaches* (March 13, 2014), http://insidecybersecurity.com/Cyber-Daily-News/Daily-News/retail-financial-sectors-form-cybersecurity-partnership-in-wake-of-data-breaches/menu-id-1075.html.

[135] *See* Press Release, Dianne Feinstein, *Senate Intelligence Committee Approves Cyber Security Bill* (July 8, 2014) *available at* http://www.feinstein.senate.gov/public/index.cfm/2014/7/senate-intelligence-committee-approves-cybersecurity-bill.

provide liability protections for information sharing between private corporate entities, between private corporate entities and the Government, and between Government agencies.

[30] Yet another promising option is the partnership that critical infrastructure institutions have formed, or should investigate forming, with ISPs. For example, ISPs currently provide DDoS mitigation services that, although not particularly effective in application vulnerability (OSI model layer 7) attacks, are very capable in responding to volume-based attacks.[136] One senior ISP executive proposed to this author, under the Chatham House Rule,[137] the possibility that ISPs may be able to provide aggregated threat intelligence information, including attribution, based upon monitoring of the entirety of its networks (not merely the network traffic to and from an individual corporate client).

[31] ISPs' capabilities are, however, subject both to statutory and regulatory limitations, including, for example, the Cable Act,[138] and

[136] *See* BRENT ROWE ET AL., THE ROLE OF INTERNET SERVICE PROVIDERS IN CYBER SECURITY 7 (2011), *available at* http://sites.duke.edu/ihss/files/2011/12/ISP-Provided_Security-Research-Brief_Rowe.pdf.

[137] *See, generally, Chatham House Rule*, CHATHAM HOUSE; THE ROYAL INSTITUTE OF INTERNATIONAL AFFAIRS http://www.chathamhouse.org/about/chatham-house-rule (explaining the Chatham House Rule).

[138] Section 631 of the Cable Communications Policy Act of 1984, 47 U.S.C. §§ 521, *et seq.* The Cable Act prohibits cable systems' disclosure of personally identifiable subscriber information without the subscriber's prior consent; requires the operator to destroy information that is no longer necessary for the purpose it was collected, to notify subscribers of system data collection, retention and disclosure practices and to afford subscribers access to information pertaining to them; provides certain exceptions to the disclosure restrictions, such as permission for the cable operator to disclose "if necessary to conduct a legitimate business activity related to a cable service or other service" provided to the subscriber, and disclosure of subscriber names and addresses (but not phone numbers), subject to an "opt out" right for the subscriber. Congress expanded, as part of the Cable Television Consumer Protection and Competition Act of 1992, the

proposed rules that would restrict the blocking of "lawful content, applications, services, or non-harmful devices," that may appear to implicate liability-incurring discretion.[139]

[32] Nevertheless, several researchers urge that ISPs should assume a "larger security role," and are in a good position "to cost-effectively prevent certain types of malicious cyber behavior, such as the operation of botnets on home users' and small businesses' computers."[140] Likewise, the Federal Communications Commission has defined "legitimate network management" as including "ensuring network security and integrity" and managing traffic unwanted by end users:

> In the context of broadband Internet access services, techniques to ensure network security and integrity are designed to protect the access network and the Internet against actions by malicious or compromised end systems. Examples include spam, botnets, and distributed denial of service attacks. Unwanted traffic includes worms, malware, and virus that exploit end-user system vulnerabilities; denial of service attacks; and spam.[141]

N.B., a 2010 study found that just ten ISPs accounted for 30 percent of IP addresses sending out spam worldwide.[142] And, in 2011, it was reported

---

privacy provision of the Communications Act to cover interactive services provided by cable operators. *Id.*

[139] *Protecting and Promoting the Open Internet*, GN Docket No. 14-28, at App'x A, §§ 8.5, 8.11 (May 15, 2015).

[140] *Id.* at 1-2.

[141] Preserving the Open Internet, 76 Fed. Reg. 59192, 59209 n.102 (Sept. 23, 2011).

[142] MICHEL VAN EETEN ET AL., THE ROLE OF INTERNET SERVICE PROVIDERS IN BOTNET MITIGATION: AN EMPIRICAL ANALYSIS BASED ON SPAM DATA 1 (2010), *available at* http://weis2010.econinfosec.org/papers/session4/weis2010_vaneeten.pdf.

that over 80% of infected machines were located within networks of ISPs, and that fifty ISPs control about 50% of all botnet infected machines worldwide.[143]

[33] Other options that some companies have pursued as alternatives to the pitfalls of inherently risky threat counter-intelligence gathering discussed above include risk transfer or automated monitoring, both of which rely on outside vendors or subscription services.

[34] Under the risk transfer approach, a corporate entity may choose to rely on the findings of a private contractor or company without undue concern for how the contractor or firm acquired the information. U.S. companies already outsource threat intelligence gathering to firms who employ operatives in Israel, such as IBM-Trusteer and RSA,[144] ostensibly because these operatives are able to effectively obtain information without running afoul of U.S. law. For legal scholars, perhaps a case to help justify this approach might be that of the famous Pentagon Papers (*New York Times v. United States*), in which the Supreme Court held that the public's right to know was superior to the Government's need to maintain secrecy of the information, notwithstanding that the leaked documents were obtained unlawfully (*i.e.*, in alleged violation of § 793 of the Espionage Act).[145] Yet, a corporate entity that knowingly—or with blissful ignorance—retains the services resulting from unethical conduct or conduct that would be criminal if undertaken in the U.S. may nevertheless suffer injury to the brand resulting from revelations of the vendor's actions.

[143] Rowe et al., *supra* note 136.

[144] *See, e.g.*, Meir Orbach, *Israeli Cyber Tech Companies on Rise in US Market*, AL MONITOR (Jan. 23, 2014) http://www.al-monitor.com/pulse/business/2014/01/us-cyber-security-market-israeli-companies.html.

[145] *See* New York Times Co. v. United States, 403 U.S. 713, 714 (1971).

[35] Under the automated monitoring approach, corporate entities rely on vendor subscription services, such as Internet Identity (IID™), that use automated software to monitor various fora or social media sites for the occurrence of keywords, concepts, or sentiment, and then alert the customer. Variations of these technologies are in use for high frequency stock trading and e-Discovery. An example might be detecting the offering for sale on a site of primary account numbers and related information by a cyberthief, and providing real-time notification to the merchant so that the accounts can be disabled.

[36] Other promising options include "big data" approach, which is to employ data scientists and software and hardware automation in-house to draw more meaningful inferences from the data and evidence already legally within the company's custody and control. For example, David Bianco, a "network hunter" for security firm FireEye, suggests allocating resources for detecting, evaluating, and treating threat indicators according to their value *to the attacker*, which he represents in his so-called "Pyramid of Pain."[146] Under this model, remediation efforts are directed toward those indicators that are costly (in time or resources) to the attacker, requiring the attacker to change strategy or incur more costs.[147] Bianco proposed this model after concluding that organizations seem to blindly collect and aggregate indicators, without making the best use of them.[148] Vendors, such as Guardian Analytics,[149] FireEye's Threat Analytics Program,[150] CrowdStrike's Falcon platform,[151] and HP's

[146] *See* David Bianco, *The Pyramid of Pain*, ENTERPRISE DETECTION & RESPONSE BLOG (Mar. 1, 2014), http://detect-respond.blogspot.com/#!/2013/03/the-pyramid-of-pain.html.

[147] *See id.*

[148] *See id.*

[149] *See* Sposito, *supra* note 126.

[150] *See FireEye Threat Analytics Platform*, FIREEYE, http://www.fireeye.com/products-and-solutions/threat-analytics-platform.htm (last visited June 9, 2014).

Autonomy IDOL[152] (intelligent data operating layer) are endeavoring to bring real-time threat intelligence parsing or information sharing tools and services to the marketplace.

IV. CONCLUSION

[37] Hack back or active defense, depending on how one defines each—and everything in between—consists of activities that are both lawful and unlawful, and which carry all the business and professional risks associated with deceptive practices, misattribution, and escalation. To urge a risk-based approach to using even lawful active defense tactics would be to state the obvious, and the use of certain types of active defense where misattribution is possible, may be to entirely abandon the risk-based approach to problem solving. Moreover, at the time of this writing, a qualified privilege to hack back through legislative reform seems unlikely, and would be difficult because the holder of such a privilege would not only have to establish proper intent, but also attribution. However, the tools, technologies, partnerships, and information sharing between corporations, governments, vendors, and trade associations are promising; they have already proven effective, and are steadily improving.

[151] *See* Tim Wilson, *CrowdStrike Turns Security Fight Toward Attacker*, DARK READING (June 25, 2013, 9:18 AM), http://www.darkreading.com/analytics/threat-intelligence/crowdstrike-turns-security-fight-toward-attacker/d/d-id/1139998?.

[152] *See HP IDOL*, HP AUTONOMY, www.autonomy.com/products/idol (last visited June 9, 2014).

Hacking Back against Cyber Attacks

Alice Tang - July 21st, 2015

Back hacking is the process of reverse engineering of hacking efforts, which attempts to stop cyber crimes by identifying attacks on a system and their origin.

The rapid advancement of information technology facilitates an increasing demand for information transmission, processing, and storage. However, it also creates substantial data security risks, which have provoked wide, public concern. Apart from implementing new defense technology to upgrade the traditional cyber protection system, some American corporations have developed a more aggressive strategy to fight against cyber attacks. One such example is the practice of active defense, which is often referred to as "hack back." Back hacking is the process of reverse engineering of hacking efforts, which attempts to stop cyber crimes by identifying attacks on a system and their origin. Some definitions also include aggressive active defense actions, such as stealing back what was stolen. The publication of the controversial "IP Commission Report [http://ipcommission.org/report/IP_Commission_Report_052213.pdf]" in 2013 provoked hot public debate over back hacking, making it a trending technology topic over the past two years. Although this approach seems to be more effective intuitively, it remains a controversial topic whether back hacking is legal and whether it can be clearly defined.

In "Cyber Security Active Defense: Playing with Fire or Sound Risk Management? [http://jolt.richmond.edu/v20i4/article12.pdf]," Sean L. Harrington discusses the legality and risks of active defense against cyber attacks in various aspects. By exploring the risks associated with the most popular active defense tactics used by private organizations, including Beaconing [http://www.reuters.com/article/2012/06/18/us-media-tech-summit-cyber-strikeback-%20idUSBRE85G07S20120618], Threat Counter-Intelligence Gathering [http://detect-respond.blogspot.com/#!/2014/03/use-of-term-intelligence-at-rsa.html.], Sinkholing [http://www.trendmicro.com/media/misc/lessons-learned-virusbulletin-conf-en.pdf], Honeypots [http://searchsecurity.techtarget.com/definition/honey-pot], and Retaliatory Hacking [http://www.cnbc.com/id/100788881], Harrington argues that it seems both difficult and unlikely for the government to legalize active defense without being able to establish what is or is not misattribution. In other words, it is difficult to distinguish between hacking and back hacking, meaning that hackers could potentially use active defense as a means to conduct cyber attacks. Without clear restrictions, it's likely that an actual hacking action could be disguised as active defense.

In this context, alternatives to back hacking, including approaches that involve new technologies and those based on collaboration among corporations, governments, Internet Service Providers (ISPs), and trade associations, are evolving rapidly and are widely implemented by private corporations to reduce their cyber vulnerabilities.

Since back hacking is also "hacking" by nature, the public has not yet reached a consensus on its legality.

Since back hacking is also "hacking" by nature, the public has not yet reached a consensus on its legality. Some believe that the legality of active defense depends on the exigency of the circumstances [http://www.bankinfosecurity.com/to-hack-back-or-not-a-5545]. If the specific circumstance is sufficiently demanding and the individual has proper intent, the active defense action could be justified. Opponents argue that active defense technically violates the law, and one practitioner even claims that it is both legally and morally wrong.

Without clear restrictions, legalizing active defense would bring huge risks of "potentially dangerous misattribution or misunderstanding [http://online.wsj.com/news/articles/SB10001424127887324682204578517374103394466]." The difficulties in differentiating aggressive back hacking from actual hacking actions would lead to serious legal issues. Although there exist different voices, most practitioners and scholars agree that back hacking is not a viable option for various reasons [http://www.infosecisland.com/blogview/23228-Another-Reason-Hacking-Back-is-Probably-a-Bad-Idea.html].

However, in the contemporary era of information sharing, the private sector has greater demand for a secure cyber environment and advanced cyber protection technologies. Some commentators have urged that active defense "must be considered as a possible device [http://digitalcommons.law.umaryland.edu/jbtl/vol8/iss1/3] in the cyber toolkit," based on the fact that private firms currently do not receive enough help from the government. As the government continues to fail to take action to protect private organizations and individuals from cyber attacks, the private sector must step in and resort to self help [http://csis.org/publication/private-retaliation-cyberspace]. However, these self-help strategies implemented by private organizations may or may not be appropriate in terms of legality. Without clear guidance from the government and law, such self-help actions could be risky and even dangerous.

The risks in private cyber security practices originate from the lack of a comprehensive regulatory and criminal framework. No new comprehensive US cyber legislation [http://fas.org/sgp/crs/natsec/R42114.pdf] has been enacted since 2002, and neither the Computer Fraud and Abuse Act (CFAA) [https://www.law.cornell.edu/uscode/pdf/uscode18/lii_usc_TI_18_PA_I_CH_47_SE_1030.pdf] nor the Electronic Communications Privacy Act (ECPA) [http://fas.org/irp/congress/2011_hr/ecpa.pdf] makes reference to the Internet. Eventually, the courts fill the significant gap between growing cyber security practices and a lack of clear legislation. This results in an unstable legislative framework, whose components, including state law, federal legislative proposals, and case law, are all in a state of flux. Practitioners need to follow and adapt to changes, which becomes a major origin of legal risks in cyber security practices.

The risks in private cyber security practices originate from the lack of a comprehensive regulatory and criminal framework.

Apart from active defense, private corporations have also developed various alternative approaches in order to reduce their vulnerabilities to cyber crimes. Some of these alternatives are based on collaboration and information sharing [http://www.bankinfosecurity.com/microsoft-fbi-takedown-citadelbotnets-a-5819/op-1] among organizations; others are built upon new technologies [http://detect-respond.blogspot.com/#!/2013/03/the-pyramid-of-pain.html] or a combination of partnerships and technologies. These approaches have been proven effective and are steadily evolving.

The future of cyber security active defense remains unclear. Will active defense become a legal and powerful tool? Or will it eventually be abandoned and replaced by less risky alternatives? The answer will depend heavily on whether the government is willing and able to allocate adequate resources to develop a clear regulatory and criminal framework for cyber security and whether the private and public sector are able to establish an effective and cooperative relationship.

Article Source: Harrington, Sean L., "Cyber Security Active Defense: Playing with Fire or Sound Risk Management?" [http://jolt.richmond.edu/v20i4/article12.pdf] *Richmond Journal of Law & Technology*, 12 (2014).

Feature Photo: cc/(UK Ministry of Defence [https://www.flickr.com/photos/48399297@N04/10086117975/])

Share this:

Facebook [https://chicagopolicyreview.org/2015/07/21/hacking-back-against-cyber-attacks/?share=facebook&nb=1]

Twitter [https://chicagopolicyreview.org/2015/07/21/hacking-back-against-cyber-attacks/?share=twitter&nb=1]

LinkedIn [https://chicagopolicyreview.org/2015/07/21/hacking-back-against-cyber-attacks/?share=linkedin&nb=1]

Email [https://chicagopolicyreview.org/2015/07/21/hacking-back-against-cyber-attacks/?share=email&nb=1]

© 2020. CHICAGO POLICY REVIEW.

Congressional Research Service
Informing the legislative debate since 1914

Cybersecurity and Information Sharing: Legal Challenges and Solutions

-name redacted-
Legislative Attorney

March 16, 2015

Congressional Research Service
7-....
www.crs.gov
R43941

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Over the course of the last year, a host of cyberattacks has been perpetrated on a number of high profile American companies. The high profile cyberattacks of 2014 and early 2015 appear to be indicative of a broader trend: the frequency and ferocity of cyberattacks are increasing, posing grave threats to the national interests of the United States. While considerable debate exists with regard to the best strategies for protecting America's various cyber-systems and promoting cybersecurity, one point of general agreement amongst cyber-analysts is the perceived need for enhanced and timely exchange of cyber-threat intelligence both within the private sector and between the private sector and the government. Nonetheless, there are many reasons why entities may opt to not participate in a cyber-information sharing scheme, including the potential liability that could result from sharing internal cyber-threat information with other private companies or the government. More broadly, the legal issues surrounding cybersecurity information sharing—whether it be with regard to sharing between two private companies or the dissemination of cyber-intelligence within the federal government—are complex and have few certain resolutions. In this vein, this report examines the various legal issues that arise with respect to the sharing of cybersecurity intelligence, with a special focus on two distinct concepts: (1) sharing of cyber-information within the government's possession and (2) sharing of cyber-information within the possession of the private sector.

With regard to cyber-intelligence that is possessed by the federal government, the legal landscape is *relatively* clear: ample legal authority exists for the Department of Homeland Security (DHS) to serve as the central repository and distributor of cyber-intelligence for the federal government. Nonetheless, the legal authorities that do exist often overlap, perhaps resulting in confusion as to which of the multiple sub-agencies within DHS or even outside of DHS should be leading efforts on the distribution of cyber-information within the government and with the public. Moreover, while the government has wide authority to disclose cyber-intelligence within its possession, that authority is not limitless and is necessarily tied to laws that restrict the government's ability to release sensitive information within its possession.

With regard to cyber-intelligence that is possessed by the private sector, legal issues are clouded with uncertainty. A private entity that wishes to share cyber-intelligence with another company, an information sharing organization like an Information Sharing and Analysis Organization (ISAO) or an Information Sharing and Analysis Centers (ISAC), or the federal government may be exposed to civil or even criminal liability from a variety of different federal and state laws. Moreover, because of the uncertainty that pervades the interplay between laws of general applicability—like federal antitrust or privacy law—and their specific application to cyber-intelligence sharing, it may be very difficult for any private entity to accurately assess potential liability that could arise by participating in a sharing scheme. In addition, concerns may arise with regard to how the government collects and maintains privately held cyber-intelligence, including fears that the information disclosed to the government could (1) be released through a public records request; (2) result in the forfeit of certain intellectual property rights; (3) be used against a private entity in a subsequent regulatory action; or (4) risk the privacy rights of individuals whose information may be encompassed in disclosed cyber-intelligence.

The report concludes by examining the major legislative proposal—including the Cyber Intelligence Sharing and Protection Act (CISPA), Cybersecurity Information Sharing Act (CISA), and the Cyber Threat Sharing Act (CTSA)—and the potential legal issues that such laws could prompt.

Contents

Contacts

Introduction

Over the course of the last year, a host of cyberattacks[1] have been perpetrated on a number of high profile American companies. In January 2014, Target announced that hackers, using malware,[2] had digitally impersonated one of the retail giant's contractors,[3] stealing vast amounts of data—including the names, mailing addresses, phone numbers or email addresses for up to 70 million individuals and the credit card information of 40 million shoppers.[4] Cyberattacks in February and March of 2014 potentially exposed contact and log-in information of eBay's customers, prompting the online retailer to ask its more than 200 million users to change their passwords.[5] In September, it was revealed that over the course of five months cyber-criminals tried to steal the credit card information of more than fifty million shoppers of the world's largest home improvement retailer, Home Depot.[6] One month later, J.P. Morgan Chase, the largest U.S. bank by assets, disclosed that contact information for about 76 million households was captured in a cyberattack earlier in the year.[7] In perhaps the most infamous cyberattack of 2014, in late November, Sony Pictures Entertainment suffered a "significant system disruption" as a result of a "brazen cyber attack"[8] that resulted in the leaking of the personal details of thousands of Sony employees.[9] And in February of 2015, the health care provider Anthem Blue Cross Blue Shield

[1] For purposes of this report, the term "cyberattack" refers to a deliberate infiltration of a computer system or network with the intent to either extract or destroy confidential information or to destroy the functioning of the system or network. *See* Jay P. Kesan and Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 439-446 (2012). It should be noted however the exact contours of what the term "cyberattack" entails is subject to much debate. *See id.* at 439 ("The modern lexicon considers all types of online intrusions to be cyberattacks, even though many commentators would assert that such indiscriminate use of the term 'cyberattack' is incorrect."); *see also* William A. Owens, Kenneth W. Dam, and Herbert S. Lin, et al., *Overview, Findings, and Recommendations*, in TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 10-11(2009) (distinguishing between the terms "cyberattack" and "cyber exploitation"); Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 823 (2012). ("The absence of a shared definition has made it difficult for analysts from different countries to develop coordinated policy recommendations and for governments to engage in coordinated actions.")

[2] Malware is the diminutive for malicious software and can come in a wide variety of forms. *See generally* Rick Lehtinen, Deborah Russell, and G.T. Gangemi Sr., COMPUTER SECURITY BASICS 80 (2d ed. 2006); *see also* Matthew J. Skelrov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 15 n.78. (2009).

[3] *See* Dan Goodin, Epic Target hack reportedly began with malware-based phishing email, ARS TECHNICA, (February 12, 2014), http://arstechnica.com/security/2014/02/epic-target-hack-reportedly-began-with-malware-based-phishing-e-mail/.

[4] *See* Press Release, *Target Provides Update on Data Breach and Financial Performance,* (January 10, 2014), *available at* http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance.

[5] *See* Press Release, *eBay Inc. To Ask eBay Users To Change Passwords*, (May 21, 2014), *available at* http://www.ebayinc.com/in_the_news/story/ebay-inc-ask-ebay-users-change-passwords.

[6] *See* Press Release, *The Home Depot Completes Malware Elimination and Enhanced Encryption of Payment Data in All U.S. Stores*, (September 18, 2014), *available at* http://www.prnewswire.com/news-releases/the-home-depot-completes-malware-elimination-and-enhanced-encryption-of-payment-data-in-all-us-stores-275649511.html.

[7] *See* Emily Glazer and Daniel Yadron, J.*P. Morgan Says About 76 Million Households Affected By Cyber Breach*, WALL STREET JOURNAL (October 2, 2014), *available at* http://www.wsj.com/articles/j-p-morgan-says-about-76-million-households-affected-by-cyber-breach-1412283372.

[8] See Press Release, Message for current and former Sony Pictures employees and dependents, and for production employees, (December 15, 2014), available at http://www.sonypictures.net/SPE_Cyber_Notification.pdf?.

[9] *See* Amelia Smith, *Sony Cyber Attack One of Worst in Corporate History*, NEWSWEEK, (December 4, 2014), *available at* http://www.newsweek.com/sony-cyber-attack-worst-corporate-history-thousands-files-are-leaked-289230.

disclosed that a "very sophisticated attack" obtained personal information relating to the company's customers and employees.[10]

The high profile cyberattacks of 2014 and early 2015 appear to be indicative of a broader trend: the frequency and ferocity of cyberattacks are increasing,[11] posing grave threats to the national interests of the United States. Indeed, the attacks on Target, eBay, Home Depot, J.P. Morgan-Chase, Sony Pictures, and Anthem were only a few of the many publicly disclosed cyberattacks perpetrated in 2014 and 2105.[12] Experts suggest that hundreds of thousands of other entities may have suffered similar incidents during the same period,[13] with one survey indicating that 43% of firms in the United States had experienced a data breach in the past year.[14] Moreover, just as the cyberattacks of 2013—which included incidents involving companies like the *New York Times,* Facebook, Twitter, Apple, and Microsoft[15]—were eclipsed by those that occurred in 2014,[16] the consensus view is that 2015 and beyond will witness more frequent and more sophisticated cyber incidents.[17] To the extent that its expected rise outpaces any corresponding rise in the ability to defend against such attacks, the result could be troubling news for countless businesses that rely more and more on computers in all aspects of their operations, as the economic losses resulting from a single cyberattack can be extremely costly.[18] And the resulting effects of a cyberattack can have effects beyond a single company's bottom line. As "nations are becoming ever more dependent on information and information technology,"[19] the threat posed by any one cyberattack

[10] *See* Press Release*, Statement regarding cyberattack against Anthem,* (February 11, 2015), *available at* https://www.anthem.com/health-insurance/about-us/pressreleasedetails/WI/2015/1813/statement-regarding-cyber-attack-against-anthem.

[11] *See generally Managing cyber risks in an interconnected world,* PRICEWATERHOUSECOOPERS, 5, (September 30, 2014) *available at* http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml (noting that in a survey of 9,700 security, IT, and business executives in 154 countries, cybersecurity incidents have risen 66% since 2009).

[12] *See 2014: A Year of Mega Breaches,* PONEMON INSTITUTE, 1, (January 2015) *available at* http://www.ponemon.org/local/upload/file/2014%20The%20Year%20of%20the%20Mega%20Breach%20FINAL3.pdf (hereinafter "Ponemon Institute- 2014") (noting breaches at CHS community Health Systems, Michaels Stores, Nieman Marcus, and Staples).

[13] *See* PRICEWATERHOUSE COOPERS, *supra* note 11, at 7 (estimating that globally 117,339 attacks occur each day).

[14] *See Is Your Company Ready for a Big Data Breach?,* PONEMON INSTITUTE, 1, (September 2014), *available at* http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf (hereinafter "Ponemon Institute- Big Data Breach"). This study, of course, only accounts for cyberattacks are actually discovered by a given business. One cybersecurity expert estimates that 85% of cyberattacks go unnoticed for two or more weeks. *See* Joshua R. McCloud, *Cisco's Internal Approach to Cyber Security,* (February 2013), *available at* http://www.cisco.com/web/AP/asiapac/academy/Archive/News_Feb.shtml.

[15] Chenda Ngak, *Are Facebook, Twitter, Apple, New York Times, NBC hacks a sign of things to come?*, CBS NEWS, February 22, 2013, http://www.cbsnews.com/8301-205_162-57570805/are-facebook-twitter-apple-new-york-times-nbc-hacks-a-sign-of-things-to-come/.

[16] *See* Sharone Tobias, *2014: The Year in Cyberattacks,* NEWSWEEK (December 31, 2014), *available at* http://www.newsweek.com/2014-year-cyber-attacks-295876.

[17] *See* Lee Raine, Janna Anderson, and Jennifer Connolly, *Cyber Attacks Likely to Increase*, PEW RESEARCH CENTER, 6-7 (October 29, 2014), *available at* http://www.pewinternet.org/files/2014/10/PI_FutureofCyberattacks_102914_pdf.pdf/ (reporting that from a canvass of "thousands of experts and Internet builders," 61% predicted that by 2025 "a major cyber attack [will] cause[] widespread harm to a nation's security and capacity to defend itself and its people"); *see also Threats Report,* MCAFEE LABS, 6-14, (November 2014), *available at* http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2014.pdf (concluding that cyber threats will increase in the year 2015); *see also* Arjun Khrarpal, *Think 2014 was bad for hacking? Worse is to come,* CNBC (January 15, 2015), *available at* http://www.cnbc.com/id/102362835# (quoting Cisco CEO John Chambers).

[18] *See* PRICEWATERHOUSE COOPERS, *supra* note 11, at 10 (noting that the "annual estimated reported average financial loss attributed to cybersecurity incidents was $2.7 million, a jump of 34% over 2013").

[19] *See* Owens, *supra* note 1, at 9.

can have "devastating collateral and cascading effects across a wide range of physical, economic and social systems."[20] With reports that foreign nations—such as Russia, China, Iran, and North Korea –may be using cyberspace as a new front to wage war,[21] fears abound that a cyberattack could be used to shut down the nation's electrical grid,[22] hijack a commercial airliner,[23] or even launch a nuclear weapon with a single keystroke.[24] In short, the potential exists that the United States could suffer a "cyber Pearl Harbor," an attack that would "cause physical destruction and loss of life"[25] and expose—in the words of one prominent cybersecurity expert–"vulnerabilities of staggering proportions."[26]

Given the growing and potentially grave threat posed by cyberattacks, one of the stated priorities of the President and congressional leadership is to enact laws that ensure that both the public and private sector are prepared to meet the cyber-challenges of the future.[27] While considerable debate exists with regard to the best strategies and methods for protecting America's various cyber-systems,[28] one point of "general agreement" amongst cyber-analysts is the perceived need for enhanced and timely exchange of cyber-threat intelligence[29] both within the private sector and

[20] See Securing America's Future: The Cyber Security Act of 2012: Hearing on S. 2105 Before the S. Comm. on Homeland Sec. and Gov't Affairs, 112th Cong. (2012) (statement of Michael Chertoff, former Sec'y of the Dep't of Homeland Sec.), available at http://www.hsgac.senate.gov/download/cybersecurity-support-statement-former-dhs-secretary-michael-chertoff.

[21] *See* Joel Brenner, *How Obama Fell Short on Cyber Security,* POLITICO MAGAZINE (January 21, 2015), *available at* http://www.politico.com/magazine/story/2015/01/state-of-the-union-cybersecurity-obama-114411.html#.VMlUeXtq3VY (noting the sources for various cyberattacks).

[22] *See* Michael Hayden, Curt Hebert, and Susan Tierney, *Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat,* BIPARTISAN POLICY CENTER, (February 28, 2014), *available at* http://bipartisanpolicy.org/library/cybersecurity-electric-grid/ ("Cyber threats to North America's electric grid are growing, making electric grid cybersecurity an increasingly important national and international issue.").

[23] *See* Pierluigi Paganini, *Cyber Threats against the Aviation Industry,* INFOSEC INSTITUTE, (April 8, 2014), *available at* http://resources.infosecinstitute.com/cyber-threats-aviation-industry/. ("Security is fundamental for the aviation industry. Considering the availability of numerous tools on the market that could be exploited in a hypothetical attack against a plane, cyber security is becoming even more crucial.")

[24] *See* Jason Koebler, *U.S Nukes Face Up to 10 Million Cyber Attacks Daily,* U.S. NEWS & WORLD REPORT, (March 20, 2014) ("The computer systems of the agency in charge of America's nuclear weapons stockpile are "under constant attack" and face millions of hacking attempts daily").

[25] *See* Leon E. Panetta, Sec'y, U.S. Dep't of Def., *Remarks on Cybersecurity to the Business Executives for National Security,* (October 11, 2012), *available at* http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

[26] *See* Joel Brenner, AMERICA THE VULNERABLE 24 (2011). While there appears to be general agreement about United States' vulnerabilities to a cyberattack, *see* Nathan Sales, *Regulating Cyber-Security,* 107 NW. U. L. REV. 1503, 1505 (2013) ("There are some naysayers but the consensus that we stand on the brink of cyber-calamity is both broad deep."), this viewpoint is not unanimous. *See, e.g.,* Jerry Brito and Tate Watkins, *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy,* 3 HARV. NAT. SEC. J. 39 (2011); Vida M. Antolin-Jenkins, Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?, 51 NAVAL L. REV. 132, 144-45 (2005).

[27] *See, e.g.,* Steven Dennis, *Obama Pushes for Deals on Cybersecurity, Trade, Taxes,* ROLL CALL (January 13, 2015), *available at* http://blogs.rollcall.com/white-house/obama-meeting-with-top-congressional-leaders-without-harry-reid/?pos=adpb ("Obama says he's spoken to Speaker John A. Boehner, R-Ohio, and Senate Majority Leader Mitch McConnell, R-Ky., on cybersecurity and 'I think we agreed that this is an area where we can work hard together, get some legislation done and make sure that we are much more effective in protecting the American people from these kinds of cyberattacks'").

[28] *See generally* Henry Farrell, *The political science of cybersecurity I—why people fight so hard over cybersecurity*, WASHINGTON POST (January 13, 2014), *available at* http://www.washingtonpost.com/blogs/monkey-cage/wp/2014/01/23/the-political-science-of-cybersecurity-i-why-people-fight-so-hard-over-cybersecurity/.

[29] Throughout this report, use of terms "cyber-intelligence," "cyber-information," "cyber-threat information," and "cybersecurity information" are used to holistically capture the entire range of possible information that could help (continued...)

between the private sector and the government.[30] The argument for the real time sharing of cyber-intelligence—which could include the sharing of vulnerability data (the vulnerabilities an intruder might exploit to gain access to a computer system), threat data (the types of malware circulating the Internet and the nature of the threats a given entity has faced), and countermeasure data (the steps an entity has taken to prevent or mitigate the effects of a cyberattack)[31]—is grounded in the idea that effective cybersecurity depends upon robust knowledge about potential threats and wide dissemination of the best practices and strategies to combat such threats.[32]

Despite widespread agreement about the need for enhanced cyber-information sharing, there is similar agreement among cyber-experts that current public and private sector information sharing efforts are simply inadequate.[33] While there may be many reasons why entities may opt to not

(...continued)

deter or mitigate a cyber-attack, including vulnerability, threat, and countermeasure data. *See infra* note 31 and accompanying text.

[30] *See* Bipartisan Policy Center, *Cyber Security Task Force: Public-Private Information Sharing,* July 2012, at p. 5, *available at* http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/Public-Private%20Information%20Sharing.pdf. This is not to say that there is agreement as to the particulars of how information sharing should be facilitated, such as the need for privacy and civil liberty protections for information shared amongst private and public entities. *See, e.g.,* Erin Kelly, *Obama, Congress may find cybersecurity consensus,* USA TODAY (January 25, 2015), *available at* http://www.usatoday.com/story/news/politics/2015/01/25/cybersecurity-information-sharing-bill/22229049/ ("That doesn't mean that there are no conflicts between the White House and Congress on the issue. House Republican leaders are still angry that the president threatened to veto an information-sharing bill they passed in the last Congress. Obama said the bill did not do enough to protect the privacy of Americans' personal data in the information-sharing process.").

[31] *See* Sales, *supra* note 26, at 1546. Threat data may consist of "signatures," patterns of network traffic deployed to detect and mitigate malicious cyber-activity, which in turn are comprised of cyber threat "indicators"—a combination of data such as IP addresses, domain names, email headers, files, and internal strings that identify the malicious activity. *See* Jeremy J. Broggi, *Building on Executive Order 13,636 to Encourage Information Sharing for Cybersecurity Purposes,* 37 HARV. J.L. & PUB. POL'Y 653, 657 (2014); *see generally* Lehtinen, *supra* note 1, at 80.

[32] *See* Sales, *supra* note 26, at 1546*; see also* Bipartisan Policy Center, *supra* note 30, at 7 ("With more robust information sharing, there can be greater situational awareness about the health of the nation's information technology architecture. A real-time understanding of threats and vulnerabilities is necessary for government officials and industry leaders to make decisions about tactical protective and response measures."); Kimberly Peretti, *Cyber Threat Intelligence: To Share or Not to Share—What Are the Real Concerns?,* 13 PVLR 1476 (2014) ("[T]he receipt of critical threat data can and has been shown to prevent potential cyberattacks and mitigate ongoing attacks."); Denise E. Zheng and James A. Lewis, *Cyber Threat Information Sharing: Recommendations for Congress and the Administration,* CTR. FOR STRATEGIC AND INT'L STUDIES 1 (March 2015), available online https://csis.org/files/publication/150310_cyberthreatinfosharing.pdf ("Cyber threat information sharing.... is a critical step toward improving cyber defenses."). For arguments against the value of cyber-information sharing, *see* Paul Rosenzweig, *The Administration's Cyber Proposals—Information Sharing,* LAWFARE, (January 16, 2015), *available at* http://www.lawfareblog.com/2015/01/the-administrations-cyber-proposals-information-sharing/ ("Given all the strum and drang, the worst part about all of this is that it seems to me to be portending a big debate over something that won't matter that much. Most of the analysts I know are in pretty wide agreement that the most significant types of threats come from sophisticated actors who are creating and deploying novel cyber threats. For those sorts of new threats, no amount of information sharing is useful.").

[33] *See* Gregory T. Nojeim, *Cybersecurity and Freedom on the Internet,* 4 NAT'L SECURITY L. & POL'Y 119, 126 (2010) ("Although laws authorize such sharing of information, actual practice has been inadequate.") (hereinafter "Nojeim-Cybersecurity"); *see also* Peretti, *supra* note 32, at 4 ("While an increasing number of companies are recognizing the benefits of sharing information regarding cyber threats, many remain wary.... "); *Exchanging Cyber Threat Intelligence: There Has to Be a Better Way,* PONEMON INSTITUTE, (April 2014), *available at* http://content.internetidentity.com/acton/attachment/8504/f-001b/1/-/-/-/-/Ponemon%20Study.pdf (hereinafter "Ponemon Institute—Threat Intelligence") ("71 percent of respondents say there has to be a better way to exchange threat information than what exists today.").

participate in a cyber-information sharing scheme,[34] a primary rationale for such a decision concerns the potential *liability* that could result from sharing internal cyber-threat information with other private companies or the government. Indeed, in a recent survey of over 700 information technology security practitioners, half of the respondents listed worries about "potential liability [from] sharing" as the main reason for not participating in an initiative for exchanging threat information.[35] More broadly, the legal issues surrounding cybersecurity information sharing—whether it be with regard to sharing between two private companies or the dissemination of cyber-intelligence within the federal government—are complex and have few certain resolutions. In this vein, this report analyzes the major legal issues regarding cyber-threat information sharing by beginning with a discussion of the current legal authorities respecting the exchange of cyber-intelligence. Included in this discussion will be an examination of the various sources of liability that could result from information sharing. The report concludes by discussing several of the major legislative proposals aimed at reforming federal cyber-information sharing laws and potential legal issues that such laws could prompt.

Conceptualizing the Legal Issues Regarding Cyber Information Sharing

While often the concept of "cyber-information sharing" is thought of as a monolith, the sharing of cyber-intelligence touches on three related, but distinct concepts. First, cyber-information sharing is often used in the context of describing efforts to promote the dissemination of cyber-intelligence *from* the federal government *to* other government entities or the private sector. This sort of cyber information sharing would occur, for example, when the Federal Bureau of Investigation (FBI) provides the Department of Homeland Security (DHS) or privately owned banks with the IP addresses of computers known to have launched distributed denial of service (DDoS) attacks against other entities within the financial sector.[36] Second, cyber-threat information sharing also embraces the concept of private entities sharing cyber-intelligence with each other, such as when several companies in a particular sector establish a formal exchange or

[34] Among these concerns include worries about compromising proprietary information, a desire to not aid competitors, losing customer goodwill, and reputational harms that may occur if an entity discloses details about a prior cyberattack. *See* Sales, *supra* note 26, at 1549; *see also* Derek E. Bambauer, *Ghost in the Network,* 162 U. PA. L. REV. 1011, 1046 (2014) ("Firms have significant incentives not to disclose breaches or attacks. Revealing lapses could have reputation-related market effects. Publicly traded companies ... suffer drops in share price immediately after revealing security breaches. Disclosing vulnerability information risks further dissemination (even if inadvertent) that could lead to additional attacks ... firms may not want to aid competitors either by reducing their information security costs or by protecting them from the same attack.").

[35] *See* Ponemon Institute—Threat Intelligence, *supra* note 33, at 3.

[36] *See, e.g., Cybersecurity: Enhancing Coordination to Protect the Financial Sector, Hearing Before Senate Committee on Banking, Housing, and Urban Affairs*, 113th Cong. (2013) (statement of Joseph M. Demarest, Assistant Director, Cyber Division, Federal Bureau of Investigation, *available at* http://www.fbi.gov/news/testimony/cyber-security-enhancing-coordination-to-protect-the-financial-sector ("The FBI worked closely with Department of Homeland Security (DHS) to issue Joint Indicator Bulletins (JIBs) to the U.S. banks, which included thousands of IP addresses that participated in the attacks. The U.S. banks used the IP addresses to better mitigate future incidents, thus helping to ensure their business operations could proceed with less interruption of service to their customers."); *see generally* Sales, *supra* note 26, at 1547 ("[T]he government's highly resourceful intelligence agencies are simply better than the private sector at detecting intrusions by sophisticated adversaries like foreign militaries and developing countermeasures. The government can provide these firms with the signatures of malware used in previous attacks, and firms can use the signature files to detect future intrusions.").

formal agreements to share relevant cyber-information with each other.[37] Finally, cyber-information sharing also describes when *private* entities share cyber-threat information in their possession *with* the government. Such information sharing could occur, for example, when private security firms report to DHS details about potential cyber-vulnerabilities unearthed in research.[38] While collectively these three variants on the concept of cyber-information sharing have some commonalities, each also raises separate legal challenges that may impede cyber-intelligence dissemination more generally.

Sharing Cyber-Information in the Possession of the Government

Perhaps the area in which there is the most legal clarity with respect to cyber-information sharing pertains to the authority of the federal government –and its subcomponents—to disseminate cyber threat information within the government and with the private sector. Two central components of DHS lead efforts to distribute cyber-intelligence to others in the government[39] and the private sector.[40]

First, the **Office of Intelligence and Analysis** (I&A), an entity established under Section 201 of the Homeland Security Act of 2002 (Homeland Security Act or the Act),[41] is generally authorized to "access and receive" information and intelligence from "agencies of the Federal Government, State and local government agencies (including law enforcement agencies), and private sector entities"[42] in order to "identify and assess" "terrorist threats to the homeland" and "actual and potential vulnerabilities to the homeland."[43] In addition, the I&A is responsible for "integrat[ing] relevant information, analysis, and vulnerability assessments" and disseminating such information in "both classified and unclassified formats, as appropriate" to "other agencies of the

[37] *See, e.g., About Us: Information Sharing and Analysis Centers (ISACs),* NATIONAL COUNCIL OF ISACS, (no date provided), *available at* http://www.isaccouncil.org/aboutus.html.

[38] *See, e.g.,* Rachael King, *Cyber Attackers Target Building Management Systems*, WALL STREET JOURNAL, (April 5, 2013), *available at* http://blogs.wsj.com/cio/2013/04/05/cyber-attackers-target-building-management-systems/.

[39] The White House recently announced the creation of the Cyber Threat Intelligence Integration Center (CTIIC), an agency housed within the Office of the Director of National Intelligence (DNI) and will be modelled off of the National Counterterroism Center (NCTC) to share cyber-intelligence across various entities within the federal government. *See* The White House, *Presidential Memorandum—Establishment of the Cyber Threat Intelligence Integration Center,* (February 25, 2015), http://www.whitehouse.gov/the-press-office/2015/02/25/presidential-memorandum-establishment-cyber-threat-intelligence-integrat.

[40] *See Stakeholder Priorities for the Quadrennial Homeland Security Review Hearing Before the Subcomm. on Oversight and Managment Efficiency of the H. Comm. on Homeland Security*, 113th Cong. (2014) (statement of Frank J. Cilluffo, Director Homeland Security Policy Institute and Cybersecurity Initiative The George Washington University) ("Currently responsibility for cyber analysis is split between the DHS Office of Intelligence and Analysis (I&A), and the National Protection and Programs Directorate.").

[41] *See* P.L. 107-296, Title II, Subtitle A, §201, codified at 6 U.S.C. §121(a). Under the Homeland Security Act of 2002, the term "terrorism" encompasses an act that is (1) "dangerous to human life or potentially destructive of critical infrastructure or key resources;" (2) a violation of federal or state or local criminal law; and (3) appears to be intended to either (a) intimidate or coerce a civilian population, (b) influence the policy of a government by intimidation or coercion, or (c) affect the conduct of a government by mass destruction, assassination, or kidnapping. *See* 6 U.S.C. §101(16).

[42] 6 U.S.C. §121(d)(1).

[43] *Id.* §121(d)(1)(A)-(C).

Federal Government, State, and local government agencies and authorities, the private sector, and other entities."[44] In turn, pursuant to 6 U.S.C. Section 143, DHS, through I&A, is required to provide to state and localities "analysis and warnings related to threats to, and vulnerabilities of," "critical information systems,"[45] a term of art presumably[46] controlled by the Homeland Security Act's definition for the term "critical infrastructure":

> [S]ystems ... so vital to the United States that the incapacity or destruction of such systems ... would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[47]

Moreover, DHS is authorized "upon request" to provide the same "analysis and warnings" to "private entities that own or operate critical information systems."[48] In practice, the I&A has primarily exercised its authority by focusing its efforts on *analyses* of cyber-threat information and the distribution of those analyses to various public and private entities.[49]

In addition to the I&A, DHS's **National Protection and Programs Directorate** (NPPD) and its subcomponents play perhaps an even more important role with respect to the sharing of cyber-threat information with other government and private entities.[50] Within the NPPD exists the Office of Cybersecurity and Communications (CS&C), an office Congress created in 2006[51] that is tasked with overseeing the "security, resiliency, and reliability of the nation's cyber and communications infrastructure."[52] To execute this mission, CS&C, supports "24x7 information sharing, analysis, and incident response" through the National Cybersecurity and Communication Integration Center (NCCIC or Center).[53] Established in 2009, the NCCIC is a "24-hour, DHS-led

---

[44] 6 U.S.C. §121(d)(3), (8), (13), (21).

[45] *Id.* §143(1)(A).

[46] *See* Perales v. Sullivan, 948 F.2d 1348, 1355 (2d Cir. 1991) ("Similar language in two different sections of the same law should be given a similar interpretation.") (citing Northcross v. Board of Education, 412 U.S. 427, 428 (1973) (*per curiam*))

[47] *See id*. §101(4) (citing 42 U.S.C. §5195c(e)) (defining "critical infrastructure," which includes both critical assets and systems).

[48] *See id.* §143(1)(A).

[49] *See Office of Intelligence and Analysis' Vision and Goals*, *Hearing Before the H. Comm. on Homeland Security,* 111th Cong. (2010) (statement of Under Secretary and Chief Intelligence Officer Caryn Wagner), *available at* http://www.dhs.gov/news/2010/05/12/testimony-under-secretary-and-chief-intelligence-officer-caryn-wagner-and-principal (" I&A also possesses a cyber intelligence analytic program. This team provides a national intelligence analytical framework in support of key cybersecurity customers, such as the DHS National Cybersecurity and Communications Integration Center (NCCIC), the DHS United States Computer Emergency Readiness Team (US-CERT), and the Industrial Control Systems CERT. We are working with partners in the community to collaborate on strategic cyber analysis, and we continue to determine the amount of analytic support necessary to the Department's cybersecurity mission.").

[50] *See About the National Protection and Programs Directorate,* Dep't of Homeland Security, (July 9, 2014), *available at* http://www.dhs.gov/about-national-protection-and-programs-directorate.

[51] *See* Dep't of Homeland Sec. Appropriations Act, 2007, P.L. 109-295, Title VI, Subtitle A, §611(13), 120 Stat. 1409, *codified at* 6 U.S.C. §321c.

[52] *See About the National Protection and Programs Directorate,* Dep't of Homeland Security, (July 9, 2014), *available at* http://www.dhs.gov/about-national-protection-and-programs-directorate (describing the "mission" of CS&C).

[53] *See Facilitating Cyber Threat Information Sharing and Partnering with the Private Sector to Protect Critical Infrastructure: An Assessment of DHS Capabilities, Hearing Before Subcomm. on Cybersecurity, Infrastructure Protection and Security Technologies H. Comm. on Homeland Security,* 113th Cong. (2013) (statement of NPPD Office of CS&C Acting Assistant Secretary Roberta Stempfley and NCCIC Director Larry Zelvin) (hereinafter "Stempfley and Zelvin").

coordinated watch and warning center" monitoring "threats and incidents affecting the nation's critical information technology and cyber infrastructure."[54] NCCIC, through the United States Computer Emergency Readiness Team (US-CERT), helps operate "key aspects" of several information sharing programs, including the Cyber Information Sharing and Collaboration Program (CISCP) and Enhanced Cybersecurity Services (ECS).[55] CISCP allows for often *unclassified*[56] "cyber threat, incident, and vulnerability information" to be disclosed "in near real-time" with private information sharing organizations and select owners and operators of so-called critical infrastructure and key resources.[57] ECS entails a "voluntary information sharing program" that, in part, "shares *sensitive and classified* government ... cyber threat information" with certain private actors.[58]

In late 2014, Congress enacted the National Cybersecurity Protection Act of 2014 (NCPA), which formally codified NCCIC's authority, allowing the "Center to carry out certain responsibilities of

[54] *See* Press Release, *Secretary Napolitano Opens New National Cybersecurity and Communications Integration Center,* (October 30, 2009), *available at* http://www.dhs.gov/news/2009/10/30/new-national-cybersecurity-center-opened.

[55] *See* Stempfley and Zelvin, *supra* note 53.

[56] *See* Jason Miller, *DHS finds classified cyber sharing program slow to take off,* FEDERAL NEWS RADIO, (June 13, 2013), *available at* http://www.federalnewsradio.com/473/3356694/DHS-finds-classified-cyber-sharing-program-slow-to-take-off (distinguishing between ECS and CISCP based on the types of information shared with the private sector); *see also* Robert Gyenes, *A Voluntary Cybersecurity Framework Is Unworkable—Government Must Crack the Whip,* 14 PGH. J. Tech. L. & Pol'y 293, 305-06 (2014) (noting that CISCP, because of its focus on sharing unclassified information, has a higher participation rate than ECS). President Obama's 2013 Executive Order on cybersecurity expanded efforts to disclose unclassified cybersecurity information, requiring the "timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity." *See Improving Critical Infrastructure Cybersecurity,* Exec. Order No. 13,636, §4(a), 78 *Federal Register* 11,739, 11,740-41 (February 12, 2013).

[57] *See* Dep't of Homeland Sec., *Critical Infrastructure and Key Resources Cyber Information Sharing and Collaboration Program* 1, (no date provided), *available at* https://www.us-cert.gov/sites/default/files/c3vp/CISCP_20140523.pdf. According to DHS, to join CISCP and gain access to NCCIC's cyber intelligence, a private entity must sign a Cooperative Research and Development Agreement (CRADA) with the agency. *Id.* Pursuant to the Stevenson-Wydler Technology Innovation Act of 1980, agencies are authorized to enter into CRDAs with private parties "under which the Government ... provides personnel, services, facilities, equipment, intellectual property, or other resources with or without reimbursement ... and the non-Federal parties provide funds, personnel, services, facilities, equipment, intellectual property, or other resources toward the conduct of specified research or development efforts which are consistent with the mission [of the agency]." *See* 15 U.S.C. §3710a(d)(1).

[58] *See* Dep't of Homeland Sec., *Enhanced Cybersecurity Services* 1, *available at* http://www.dhs.gov/sites/default/files/publications/ECS-Fact-Sheet.pdf (emphasis added). The private entities that participate in ECS and receive government furnished threat indicators are either Commercial Service Providers (CSP) or Operational Implementers (OIs) who have been vetted by the government and entered into a Memorandum of Understanding with DHS. *See id.* at 2. CSPs, such as AT&T, provide information services to private entities, while an OI is a private entity who provides information services for its own network. *See* Defense Cyber Crime Center, *DIB Enhanced Cybersecurity Services (DECS),* (February 26, 2013), *available at* http://www.dc3.mil/data/uploads/dcise-pdf-dib-enhanced-cybersecurity-services-procedures_updated-feb-26-2013.pdf (describing the Department of Defense's precursor to ECS). Regardless, either a OI or CSP must be capable of implementing government furnished information, comply with applicable security requirements, and have appropriately cleared personnel and facilities in order to participate in ECS. *Id.* ECS was expanded pursuant to President Obama's 2013 Executive Order on cybersecurity. *See Improving Critical Infrastructure Cybersecurity,* Exec. Order No. 13,636, §4(c), 78 *Federal Register* 11,739, 11,740-41 (February 12, 2013) ("To assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm, the Secretary ... in collaboration with the Secretary of Defense, shall, within 120 days of the date of this order, establish procedures to expand the [ECS] program to all critical infrastructure sectors.") For more on the origins of ECS and the President's Executive Order, *see* CRS Report R42984, *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress*, by (name redacted) et al., at pp. 10-11.

the Under Secretary" for the NPPD.[59] Specifically, the NCPA confirmed that the NCCIC's functions include serving as an "interface" for the "real-time" "sharing of information related to cybersecurity risks, incidents, analysis, and warnings between Federal and non-Federal entities."[60] Furthermore, the NCPA directs the Center to provide a number of additional services, such as technical assistance, risk management support, and incident response capabilities to both public and private entities.[61] The NCPA requires NCCIC to include representatives of federal agencies, state and local governments, and private sector owners and operators of critical information systems,[62] while still providing the Under Secretary for the NPPD with discretion with respect to the precise makeup of the Center.[63] In February of 2015, in keeping with NCCIC's statutory role, President Obama, in an Executive Order, mandated that the Center "engage in continuous, collaborative, and inclusive coordination with" Information Sharing and Analysis Organizations (ISAOs),[64] a formal or informal entity or collaboration created or employed by public or private sector organizations that gather, analyze, and disseminate cyber-threat information.[65]

The Homeland Security Act, as amended by the NCPA, provides significant authority for DHS to disseminate a wide range of cyber-threat intelligence within the possession of the federal government to other government agencies and to the private sector. Earlier iterations of the Homeland Security Act seemingly cabined DHS's authority to collect and share cyber-intelligence only to the extent such information respected a "terrorist threat"[66] or would pertain to "critical information systems."[67] In contrast, the NCPA provides NCCIC the authority to share cyber-information to the extent that such information relates to "cybersecurity risks,"[68] a term of art that encompasses any "threats" and "vulnerabilities" to information systems and "any related consequences caused by or resulting" from a host of actions that could compromise an information system or the information stored on an information system.[69] In other words, given

[59] P.L. 113-282, 128 Stat. 3066.

[60] 6 U.S.C. §148(c)(1). The Center is composed of various federal entities, such as sector-specific agencies, law enforcement agencies, and members of the intelligence community, and non-federal entities, such as state and local governments, information sharing and analysis organizations, and owners and operators of critical information systems. *Id.* §148(d).

[61] *Id.* §148(c).

[62] *Id.* §148(d)(1)(A)-(B).

[63] *Id.* §148(d)(1)(E).

[64] *See Executive Order, Promoting Private Sector Cybersecurity Information Sharing,* THE WHITE HOUSE, (February 13, 2015), §2(c), *available at* http://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

[65] 6 U.S.C. §131(5).

[66] *See, e.g.,* P.L. 107-296, Title II, Subtitle A, §201(d)(1) ("[T]he responsibilities of the Under Secretary for Information Analysis and Infrastructure Protection shall be ... to access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies ... and private sector entities, and to integrate such information in order to ... identify and assess the nature and scope of terrorist threats to the homeland ... ").

[67] *Id.* §223 ("In carrying out the responsibilities under section 201, the Under Secretary for Information Analysis and Infrastructure Protection shall ... as appropriate, provide to State and local government entities, and upon request to private entities that own or operate critical information systems ... analysis and warnings related to threats to, and vulnerabilities of, critical information systems.").

[68] *See* 6 U.S.C. §148(c).

[69] *Id.*§148(a)(1) (defining "cybersecurity risk" to mean "threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of information or information systems, including such related consequences (continued...)

DHS's discretion in designating various entities to participate in the NCCIC,[70] it appears DHS has fairly broad authority to disseminate federal cyber threat information throughout the private sector, regardless of whether the information pertains to an industry that is "so vital to the United States that the incapacity or destruction" of that industry's assets or information systems would be "debilitating" to the country.[71] In fact, one issue that has been raised by commentators is whether the statutory authority allotted to the various entities within DHS—such as I&A and NPPD—to engage in cyber-information sharing is so broad and ill-defined that confusion could result internally within the Department as to who the central actor should be with respect to the sharing of federal cyber-intelligence.[72] The same argument could plausibly be made with respect to the authority to disseminate cyber-intelligence amongst the various entities of the federal government, as entities like the I&A[73] and NPPD[74] within DHS and new entities outside of DHS, like the newly formed Cyber Threat Intelligence Integration Center (CTICC)[75] appear to possess overlapping legal authorities with respect to the internal sharing of cyber-information within the federal government.[76]

(...continued)

caused by an act of terrorism"); *see also id.* §148(a)(4) (citing 44 U.S.C. §3502(8) (defining "information system" to mean "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information").

[70] 6 U.S.C. §148(d)(1)(E).

[71] *See* 42 U.S.C. §5195c(e) (defining "critical infrastructure," which includes both critical assets and systems).

[72] *See, e.g.,* Sean Lyngaas, *Can DHS get it together?,* FEDERAL COMPUTER WEEK, (October 31, 2014), *available at* http://fcw.com/articles/2014/10/31/cybersecurity-can-dhs-get-it-together.aspx (noting difficulty integrating threat analyses done by I&A with the work of NPPD); *see generally,* Paul Rosenzweig, *Cyber Security: A Complex 'Web' of Problems,* HERITAGE Foundation, (August 26, 2010), *available at* http://www.heritage.org/research/reports/2010/08/cyber-security-a-complex-web-of-problems#_ftnref2 ("Today, as it pertains to cyber security, America still needs clearer lines of authority within the federal government and a more coherent structure of public–private interaction to allow for effective action.") (hereinafter "Rosenzweig-Heritage"); Robert Kenneth Palmer, *Critical Infrastructure: Legislative Factors for Preventing a "Cyber Pearl Harbor,"* 18 VA. J.L. & TECH. 289, 329 (2014) ("There are too many government agencies with different cyber-missions working independently, with project duplication to the point that it is not uncommon for several different groups to be working on the same thing, unaware of each other's efforts."); *but see Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland, Hearing Before S. Comm. on Homeland Security and Gov't Affairs,* 113th Cong (2014) (testimony of Under Secretary Francis Taylor and NPPD Under Secretary Suzanne Spaulding), *available at* http://www.dhs.gov/news/2014/09/10/written-testimony-ia-and-nppd-senate-committee-homeland-security-and-governmental ("I&A and NPPD work closely together every day to recognize and reduce risks posed by cyber threats."). In this vein, some have lamented the fact that the disperse authorities respecting cyber-intelligence sharing have resulted in key entities, like US-CERT, lacking any specific authority to request cooperation from other agencies within DHS or the rest of the government on cyber-intelligence efforts. *See Examining the Cyber Threat to Critical Infrastructure and the American Economy: Hearing before the H. Comm. of Homeland Security, Subcomm. on Cybersecurity, Infrastructure Protection, and Security Technologies*, 112th Cong. 50 (2011) (testimony of Mischel Kwon, President, Mischel Kwon & Associates, LLC), available at http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg72221/pdf/CHRG-112hhrg72221.pdf ("US–CERT does not have the authority to require the departments or agencies to share detailed information, or follow any specific instructions"); *see also* Palmer, *supra* note 72, at 327 ("A significant part of the US-CERT's mission is to 'coordinate and collaborate' with critical infrastructure owners and operators, but this is rarely accomplished because the USCERT is buried within the DHS and has no authority to compel sector-specific federal agencies or law enforcement to coordinate and cooperate with the US-CERT's activities.").

[73] *See* 6 U.S.C. §121(d)(3)-(4).

[74] *See id.*§148(c)(2).

[75] *See supra* note 39.

[76] *See, e.g.,* Richard Bejtlich, *What are the prospects for the Cyber Threat Intelligence Integration Center?,* BROOKINGS INSTITUTION, (February 19, 2015), *available at* http://www.brookings.edu/blogs/techtank/posts/2015/02/19-cyber-security-center-bejlich ("Some may view CTIIC as just the latest in a long line of cyber agencies created by the government ... The concern with CTIIC, however, is the perception that it duplicates the mission of NCCIC and older (continued...)

Nonetheless, DHS's ability to share federal cyber-intelligence is not limitless. First, cyber-threat information the government provides to the private sector generally must occur on a voluntary basis.[77] The plain language of Section 223 of the Homeland Security Act limits DHS's ability to share cyber-intelligence with "private entities that own or operate critical information systems," such that information sharing can only occur "upon [those entities'] request."[78] And indeed, the NCPA contains an even more explicit provision disclaiming the Act from being "construed to require any private entity" to request any assistance from the Secretary of DHS.[79] In other words, under current law, DHS generally does not have the authority to "mandate private sector participation" in federal cyber information sharing efforts,[80] leading some to question the value of the current voluntary information sharing scheme.[81]

Second, other laws outside of the context of cybersecurity may limit the ability of the government to disseminate cyber-threat information. The Homeland Security Act itself requires DHS to ensure that any intelligence in its possession "is protected from unauthorized disclosure and handled and used only for the performance of official duties."[82] More specifically, the Act mandates that DHS adhere to (1) the requirements of the National Security Act of 1947 to the extent any information pertains to intelligence sources and methods and (2) any authorities of the Attorney General "concerning sensitive law enforcement information."[83] In other words, to the extent any federal cyber-intelligence contains sensitive information, such as the sources or methods that are the heart of an ongoing cybercrime investigation,[84] the government may be limited in its ability to disclose such information.

Beyond laws aimed at limiting disclosures that may inhibit core governmental functions, laws aimed at preserving privacy and civil liberties may also restrict DHS's ability to share certain cyber-information. The Homeland Security Act requires DHS to "ensure ... that any information databases and analytical tools developed and utilized by the Department"—which would presumably include programs like CISCP and ECS—"treat information in such databases in a manner that complies with applicable Federal law on privacy."[85] Moreover, the NCPA requires

(...continued)

units.").

[77] The federal government is authorized to provide, without request, "analysis and warnings related to threats to, and vulnerabilities of, critical information systems" to state and local government entities. *See* 6 U.S.C. §143(1). Moreover, the Homeland Security Act authorizes DHS to make general recommendations and disseminate information analyzed by the Department as "appropriate" or "necessary." *See id.* §121(d)(6)-(8).

[78] *See id.* §143(1).

[79] *See* P.L. 113-282, §8, 128 Stat. 3072.

[80] *See* Broggi, *supra* note 31, at 658 ("On the contrary, the phrase 'upon request' suggests any such mandate is forbidden.").

[81] *See* Palmer, *supra* note 72, at 358 ("Even after two decades, voluntary information sharing has failed to create an effective information sharing environment.... ").

[82] 6 U.S.C. §121(d)(11)(A); *see also* 6 U.S.C. §141(2) (authorizing the Secretary of DHS to "establish procedures on the use of information shared under this title that ... ensure the security and confidentiality of such information.... ").

[83] *Id.* §121(d)(11)(B). For more information on the laws governing the protection of classified information, *see* CRS Report RS21900, *The Protection of Classified Information: The Legal Framework*, by (name redacted).

[84] *See* Gus P. Coldebella and Brian M. White, *Foundational Questions Regarding the Federal Role in Cybersecurity*, 4 J. NAT'L SEC. L. & POL'Y 233, 240-41 (2010) ("While the government has information about malicious code and the behavior of criminal networks gained through its intelligence and law enforcement functions, fears of botching investigations or compromising sources and methods make sharing with the private sector (or even with other government agencies) difficult.").

[85] *See* 6 U.S.C. §121(d)(14)(b); *see also* 6 U.S.C. §141(3) (authorizing the Secretary of DHS to "establish procedures (continued...)

that the NCCIC "comply with all policies, regulations, and laws that protect the privacy and civil liberties of United States persons."[86] As such, if DHS's cyber intelligence included, for example, individually identifiable information—like a name or a social security number—laws like the Privacy Act of 1974 may restrict the manner in which the government may disclose such information in a cyber-information sharing program.[87]

Collectively, the legal effect of the various federal disclosure and privacy laws may limit the efficacy of any cyber-information DHS provides private entities. As one commentator recently noted, the resulting "sanitation" of cyber-intelligence has a dual effect.[88] First, the host of federal agencies that "own classified or law enforcement information germane to a particular warning" "must be coordinated with as part of the review process," resulting in significant delays before DHS can release any information to a private entity, by which time the information may be irrelevant.[89] Second, even if DHS releases government cyber threat information in a timely manner, the cyber intelligence resulting after agency review of the underlying material may omit critical information that is "actually useful to industry."[90]

Sharing Cyber-Information in the Possession of Private Entities

Whereas the law governing the dissemination of cyber-threat information in the possession of the federal government is relatively straightforward, the legal landscape surrounding the sharing of cyber-intelligence that is in the possession of private parties stands in stark contrast. Indeed, there is an array of legal concerns—some more theoretical than actual—that shroud the law governing the sharing of privately-held cyber-threat information in a cloud of uncertainty and create disincentives against the sharing of such information by private parties.[91] The legal issues can be

(...continued)

on the use of information shared under this title that ... protect the constitutional and statutory rights of any individuals who are subjects of such information.... ").

[86] *See* 6 U.S.C. §148(e)(3).

[87] *See* 5 U.S.C. §552a(b) (generally prohibiting an agency from disclosing "any record which is contained in a system of records by any means of communication to any person, or to another agency.... "). Pursuant to the Privacy Act and the Homeland Security Act, DHS has promulgated Fair Information Practice Principles (FIPPs), which generally amount to framework for how the Department uses and disseminates information containing personal identifying information. *See* Hugo Teufel III, DHS Privacy Policy Guidance, DEP'T OF HOMELAND SEC., (December 29, 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf. However, it should be noted that the Privacy Act does contains exemptions for some inter-agency data sharing for national security and law enforcement purposes, as well as routine uses described by the agency in the Federal Register. *See* 5 U.S.C. §§552a(a)(8)(B)(vi), (b)(3), (b)(7), (e)(4)(D), & (j). There are numerous other more narrowly applicable laws on privacy and data protection that protect specific types of information in the possession of the government that could implicate the sharing of federal cyber-intelligence. *See, e.g.,* 42 U.S.C. §1320(d) & 45 C.F.R. §§160, 164 (Health Insurance Portability and Accountability Act of 1996); 18 U.S.C. §1905 (Trade Secrets Act).

[88] *See* Palmer, *supra* note 72, at 326.

[89] *Id.*

[90] *Id.* at 327.

[91] *See* Peretti, *supra* note 32, at 4 (noting concerns with current legal incentives governing private cyber-information sharing); *see also* Palmer, *supra* note 72, at 317-18 ("Although many of these limitations may be less limiting than they are perceived to be, the result of these perceptions and, at the very least, the uncertainty about the state of the law as they pertain to information sharing, have created collective inaction where individual companies often simply feel safer (continued...)

divided between those that arise when private companies share cyber-information with each other and those that occur when private companies share cyber-intelligence with the government.

Sharing Cyber-Information with Another Private Entity

Information security professionals within the private sector have "long relied" on information from other private entities to "gain insight into cybersecurity threats and vulnerabilities."[92] And often the most valuable cyber-intelligence comes from peers in other companies, including direct competitors that may be subject to similar cybercrimes.[93] Private cyber-information sharing can take many forms, from informal arrangements, such as peer discussions via phone, email, or in person, to formal sharing arrangements, such as cyber-intelligence sharing through an Information Sharing and Analysis Center (ISAC), a private sector nonprofit corporation formed to facilitate the sharing of information on cyber-threats, incidents and vulnerabilities among members within a particular sector.[94] At times, the federal government has been quite supportive of such private efforts to share cyber-intelligence. Indeed, the impetus for ISACs was Presidential Decision Directive-63, issued by President Clinton in 1998, which initially called for the creation of industry-specific ISACs.[95] Nonetheless, there are several bodies of law whose basic norms run counter to the concept of a private business sharing cyber-threat information with an industry peer, raising potential liability issues for those in the private sector that wish to exchange cyber-intelligence.[96] Without any overarching federal law governing private exchanges of cyber-threat information, the potential remains for various laws facially unrelated to cyber-information sharing to discourage such activity within the private sector.

Privacy Laws

A variety of state and federal privacy laws govern the collection, storage, use, and dissemination of electronic information, potentially leaving limited room for cyber-intelligence sharing amongst private actors or between private actors and the government.

The most pertinent *federal* privacy law is the Electronic Communications Privacy Act of 1986 (ECPA), which contains three titles: (1) Title I, the Wiretap Act,[97] which regulates the interception of communications content in transit; (2) Title II, the Stored Wire and Electronic Communications and Transactional Records Access Act[98] (Stored Communications Act or SCA), which governs electronic communications already transmitted and currently in storage; and (3) Title III, the Pen

(...continued)

by keeping threat information to themselves rather than sharing it for mutual benefit."); CRS Report R43821, *Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis*, by (name redacted).

[92] *See* Peretti, *supra* note 32, at 2.

[93] *See* Ponemon Institute—Threat Intelligence, *supra* note 33, at 5 (noting that 58% of a survey's respondents rely on "peers in other companies" as their main source of threat intelligence).

[94] *See* Peretti, *supra* note 32, at 2.

[95] *See* Memorandum from President William Clinton on Critical Infrastructure Protection (Presidential Decision Directive/NSC-63) (May 22, 1998), *available at* http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

[96] *See* Peretti, *supra* note 32, at 4.

[97] 18 U.S.C. §§2510-2522.

[98] *Id.* §§2701-2711.

Register and Trap and Traces Devices Act (Pen/Trap Act),[99] which regulates the interception of noncontent communications, such as phone numbers or IP addresses. Each section of ECPA is potentially relevant to those private entities considering sharing cyber-intelligence information.

The Wiretap Act

The Wiretap Act generally provides for criminal[100] and civil damages[101] against anyone who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept" any covered communication,[102] which includes electronic communication.[103] To "intercept" an electronic communication is to use "any electronic, mechanical, or other device" to acquire the "contents" or the "substance, purport, or meaning" of the communication,[104] contemporaneously with the transmission.[105] Relatedly, the statute also generally prohibits a "person or entity providing electronic communication service to the public" from intentionally divulging the contents of any electronic communication while in transmission other than to the "addressee or intended recipient of such communication."[106] Perhaps most relevant to cyber-information *sharing*, the Wiretap Act also prohibits the *disclosure or use* of the contents of any electronic communication that was obtained in violation of the statute, such an illegal interception of electronic communications.[107]

Putting to the side the several exceptions contained in the Wiretap Act, on its face, ECPA's general prohibition on the interception of electronic communications would appear to encompass any strategy for detecting cyber-threats that involved scanning the *contents* of an electronic communication while in transmission,[108] and ECPA's general prohibition on an electronic service

---

[99] *Id.* §§3121-3127.

[100] The Wiretap Act imposes significant criminal penalties on those who violate its terms, with a minimum of a ten thousand dollar fine per violation and up to five years of imprisonment. *See id.* §§2511, 2520.

[101] *Id*. §2520(a).

[102] *Id*. §2511(1)(a). Put another way, to show a violation of Title I of ECPA, five elements must be shown: the person or entity (1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication (5) using a device. *See In re* Phramatrak Privacy Litig., 329 F.3d 9, 18 (1st Cir. 2003).

[103] An electronic communication includes any "transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photoptical system." *See* 18 U.S.C. §2510(12).

[104] 18 U.S.C. §2510(4) & (8). The statute also generally prohibits conduct related to or taken as a consequence of an illegal interception of covered communication, such as the use of a device to intercept a covered communication, the disclosure of illegally intercepted communications, or the use of illegally intercepted communications. *See* 18 U.S.C. §2511 (b)-(e).

[105] *See* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114 (3d Cir. 2003); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002); United States v. Steiger, 318 F.3d 1039, 1048-49 (11th Cir. 2003); *but see* United States v. Councilman 418 F.3d 67, 80 (1st Cir. 2005) (*en banc*) (suggesting that ECPA may not require "contemporaneity or real-time" transmission of electronic communications).

[106] *See* 18 U.S.C. §2511(3)(a).

[107] *See id.* §2511(1)(c)-(d).

[108] *See generally* Noel v. Hall, 568 F.3d 743, 749 (9th Cir. 2009) (holding that an interception of a covered communication "occurs 'when the contents of a ... communication are captured or redirected in any way.'") (quoting United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir. 1992)); *see, e.g.* Campbell v. Facebook, Inc.,—F.Supp.3d—-, 2014 WL 7336475, at *3 (N.D.Cal. December 23, 2014) (holding the use of a software application to scan the content of private messages for marketing purposes amounts to "redirection" of the contents of the users' messages); *In re*
(continued...)

provider divulging the *contents* of any communication while in transmission may bar the *real time* transmission of certain cyber-intelligence.[109] While cyber-intelligence may often not include the contents of an electronic communication and may merely contain, for example, the IP address of the origin of malware, as one commentator has suggested, many common cyber-threat detection methods require using the contents of electronic communications—such as text within the body of an email—to determine whether a particular communication is malicious.[110] Moreover, to be effective, cyber-information sharing often necessitates the use of real time sharing of cyber-threat information.[111] Nonetheless, the Wiretap Act contains two key exceptions to its general prohibition that may limit the scope of the law as it pertains to cyber-information collection and sharing.[112]

First, the Wiretap Act includes an exception to its general prohibitions when there is the presence of consent to the otherwise illicit interception or disclosure ("consent exception").[113] A private actor can only rely on the consent exception where one of the parties to the communication has given prior consent to the interception or divulgence.[114] Courts reviewing the question of whether a party to the communication consented to an interception or disclosure will look into the

(...continued)

Yahoo Mail Litig., 7 F. Supp. 3d 1016, 1027 (N.D. Cal. 2014) (holding that accessing the content of emails in transit constitutes an interception for purposes of ECPA).

[109] *See generally* Shubert v. Metrophone, Inc., 898 F.2d 401, 405 (3d Cir. 1990) (holding that §2511(3)(a) "prohibits a communication service provider from intentionally divulging the contents of a communication while in the transmission of that service.").

[110] *See* Broggi, *supra* note 31, at 661-62 ("[S]ignatures are comprised of indicators, and ... indicators may include text strings. If these strings are located in the body or subject line of an email, courts will consider them contents.").

[111] *See, e.g.,* Palmer, *supra* note 72, at 368 ("The nation needs real-time situational awareness and innovative cybersecurity standards to keep up with the technological curve of cyber-threats that confront critical infrastructure.").

[112] The Wiretap Act's prohibition on the use of a "device" to intercept any oral communication, *see* 18 U.S.C. §2511(b), contains another exception that may be relevant for those engaged in cyber-threat detection. Specifically, ECPA's definition of a "device" necessarily excludes "any device or apparatus" used by "any ... equipment or facility ... furnished to the subscriber or user ... in the ordinary course of business." *See id.* §2510(5)(a). However, the "ordinary course of business" exception may not apply to a private entity that is scanning electronic communication for potential cyber-threats. Courts have generally interpreted the ordinary course of business exemption to apply to devices that further an underlying communications system, such as routers or switchboards, which arguably is unrelated to determining whether particular communications within such a system pose a cyber-threat. *See In re* Google Inc. Gmail Litigation, No. 13–MD–02430, 2013 WL 5423918, at *8 (N.D. Cal. September 26, 2013) (holding the "ordinary course of business exception" "offers protection from liability only where an electronic communication service provider's interception facilitates the transmission of the communication at issue or is incidental to the transmission of such communication. Specifically, the exception would apply here only if the alleged interceptions were an instrumental part of the transmission of email."); *see also Campbell,* 2014 WL 7336475, at *7 (holding the ordinary course of business exception requires some nexus between interception and the subscriber's "ultimate business, that is, the ability to provide the underlying service or good"); *see generally* Sanders v. Robert Bosch Corp., 38 F.3d 736, 740 (4th Cir. 1994) (refusing to apply the ordinary course of business exemption to a voice logger); Hall v. EarthLink Network, Inc., 396 F.3d 500, 504-5 (2d Cir. 2005); Williams v. Poulos, 11 F.3d 271, 280 (1st Cir. 1993); Deal v. Spears, 980 F.2d 1153, 1158 (8th Cir. 1992); *but see* Kirch v. Embarq Mgmt. Co., 702 F.3d 1245, 1250 (10th Cir. 2012) (holding that an Internet Service Provider was operating in the ordinary course of business by allowing an online advertising company to conduct technology tests for directing online advertising on electronic communications that the provider ordinary accessed). More broadly, courts have been reluctant to find that indiscriminate recording of communications is within the ordinary course of most businesses. *See, e.g.,* United States v. Murdock, 63 F.3d 1391, 1397 (6th Cir. 1995).

[113] *See* 18 U.S.C. §2511(2)(d); *id.* §2511(3)(b)(ii).

[114] *See* 18 U.S.C. §2511(2)(d); *id.* §2511(3)(b)(ii). In addition, under the consent exception to the Wiretap Act' s interception prohibition, the exception does not apply when the underlying communication is "intercepted for the purposes of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." *Id.* §2511(2)(d).

"dimensions of the consent" and then ascertain whether the act in question "exceeded those boundaries."[115]

With respect to a private entity's efforts to collect content-based cyber-threat information and disseminate such information, the Wiretap Act's consent exception, while often a viable route to avoid liability, raises several difficult legal questions. For example, determining who is a "party to the communication" when someone is launching a cyberattack can be very difficult, as the cybercriminal may be using multiple computers and the ultimate destination of the hacker's communication may be unclear.[116] While an entity attempting to monitor its system for cyber-intruders could argue that it is a party to the underlying electronic communication being monitored because the data is flowing on its network and is being directed toward its computers and employees,[117] such an interpretation of what it means to be a party to a communication may eliminate any privacy protections for the individuals who are directly participating in the electronic communication.[118] Instead, a court may likely interpret that a party to a communication must be the individuals who actually take part in the electronic conversation.[119]

Moreover, assuming that the private entity acquiring cyber-threat information is not a party to the communication, consent must be obtained from one of the individuals taking part in the communication, which, in turn, depends on the dimensions of the consent and whether the interception or divulgence of the contents of electronic communication exceeded the boundaries of the consent.[120] Such an inquiry can be quite context specific,[121] inviting litigation and creating legal uncertainty for entities wishing to engage in cyber-information sharing. For example, courts have come to differing conclusions as to whether an electronic communications service provider's customer has consented to having the provider intercept certain communications, largely because of the specific nature of the interception in question and the precise terms of service to which the customer agreed.[122] Importantly, consent cannot be "casually" inferred,[123]

---

[115] *See* Gilday v. Dubois, 124 F.3d 277, 297 (1st Cir. 1997) (citing Griggs-Ryan v. Smith, 904 F.2d 112, 116 (1st Cir. 1990).

[116] *See* Dep't of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations,* 172 (2009), *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

[117] *See* Pitts Sales, Inc. v. King World Prods., 383 F. Supp. 2d 1354, 1361 (S.D. Fla. 2005) (holding that a "party to the communication" under §2511(2)(d) is a party "who is present when the ... communication is uttered and need not directly participate in the conversation"); *see also* United States v. Mullins, 992 F.2d 1472, 1478 (9th Cir. 1993) (stating that the consent exception of §2511(2)(d) authorizes monitoring of computer system misuse because the owner of the computer system is a party to the communication).

[118] *See generally* Brown v. Waddell, 50 F.3d 285, 289 (4th Cir. 1995); *see also* Orin Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Wasn't,* 97 NW. U. L. REV. 607, 620 (2003) 664-665 ("[L]abeling the [provider] a party to the communication may sound logical ... but ultimately would eviscerate the privacy protections of the Wiretap Act.").

[119] *See* Caro v. Weintraub, 618 F.3d 94, 97 (2d Cir. 2010) (holding that a "a party to the conversation is one who takes part in the conversation.").

[120] *See In re Pharmatrak Privacy Litig*., 329 F.3d at 19 (citing Griggs-Ryan v. Smith, 904 F.2d 112, 119 (1st Cir. 1990)). Moreover, consent may be explicit or implied, but it must be actual consent rather than constructive consent. *Id.*

[121] United States v. Footman, 215 F.3d 145, 155 (1st Cir. 2000) ("The question of consent, either express or implied, may vary with the circumstances of the parties.").

[122] *See, e.g.,* Backhuat v. Apple, Inc.,—F.Supp.3d—-, 2014 WL 6601776, at *8 (N.D. Cal. November 19, 2014) ("In light of the specific language of the license agreement, the Court concludes that a reasonable iMessage user would not be adequately notified that Apple would intercept his or her messages when doing so would not 'facilitate delivery' of the messages."); *In re Yahoo Mail Litig.,* 7 F.Supp.3d at 1029 ("The Court concludes that the [Yahoo Global Communications Additional Terms of Service for Yahoo Mail and Yahoo Messenger] establishes explicit consent by Yahoo Mail users to Yahoo's conduct."); *In re Google Inc. Gmail Litig.,* 2013 WL 5423918, at *11–14 ("[A]
(continued...)

and absent actual notice of the nature of the interception or divulgence, consent can only be implied if the "surrounding circumstances convincingly show that the party knew about and consented to the interception."[124] Courts, interpreting the consent exception narrowly to ensure the exemption does not swallow the rule, have held that merely providing a person notice that an entity has the capability of intercepting communications cannot be considered implied consent.[125] And deficient notice will "almost always defeat a claim of consent."[126] As a consequence, for a private entity that wishes to employ and share the results of a cyber-threat detector, which often is created with the goal of invisibly tracking communications without alerting either internal or external users of its operation, notice to a party of an electronic communication that is sufficient to create consent may, at times, defeat the entire purpose of monitoring and sharing the contents of electronic communications.

Second, the Wiretap Act also includes a "provider exception" which allows the provider of electronic communications to "intercept, disclose, or use" the contents of communications when the activity is a "necessary incident to ... the protection of the rights or property of the provider of that service."[127] On its face, the provider exception is limited to protecting the "rights or property of the provider," as opposed to any third party.[128] While at least one court has read the provider exception broadly to allow a service provider to intercept or disclose covered communications for purposes of aiding third parties,[129] several courts have cabined the provider exception in terms of whether the interception was done for the purpose of protecting the provider's own "equipment and rights."[130] And the Department of Justice's (DOJ's) Office of Legal Counsel has likewise concluded that the provider exception "must protect the provider's own rights or property, and not

(...continued)

reasonable Gmail user who read the Privacy Policies would not have necessarily understood that her emails were being intercepted to create user profiles or to provide targeted advertisements. Accordingly, the Court finds that it cannot conclude at this phase that the new policies demonstrate that Gmail user Plaintiffs consented to the interceptions.").

[123] *See Griggs-Ryan,* 904 F.2d at 117-18.

[124] *See Berry v. Funk,* 146 F.3d 1003, 1011 (D.C. Cir. 1998).

[125] *See Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 581 (11th Cir. 1983).

[126] *See In re Pharmatrak Inc.,* 329 F.3d at 20.

[127] *See* 18 U.S.C. §2511(2)(a)(i). The provider exception also contains a provision that allows the service provider to intercept, disclose, or use cover communications when the activity is a necessary incident to the rendition of a service. *Id.* This exception generally allows interception that is "unavoidable" and a part and parcel of modern telecommunications. U.S. Dep't of Justice, *supra* note 116, at 177 (citing United States v. New York Tel. Co., 434 U.S. 159, 168 n.13 (1977)).

[128] *See* 18 U.S.C. §2511(2)(a)(i).

[129] *See, e.g.,* United States v. Pervaz, 118 F.3d 1, 5 (1st Cir. 1997) (holding that a company had the right to intercept covered communications where there was evidence that its customers were being defrauded); *see generally* United States v. Harvey, 540 F.2d 1345, 1352 (8th Cir. 1976) ("18 U.S.C. §2511(2)(a)(i) ... was designed to allow the disclosure of justified wire monitoring" in order to provide evidence for "wire fraud prosecution"); *New York Tel. Co.*, 434 U.S. at 168 n.13 (stating in *dicta* that the provider exception "excludes all normal telephone company business practices from the prohibitions of the [Wiretap] Act.").

[130] *See* United States v. Mullins, 992 F.2d 1472, 1478 (9th Cir. 1993) (holding that an employee of an electronic communication service can act to "protect the rights and property of her employer by monitoring ... apparent misuse of [the] electronic communication service."); Campiti v. Walonis, 611 F.2d 387, 393 (1st Cir. 1979) ("The section is obviously intended to allow the telephone company to intercept and disclose calls as a necessary protection of *its* equipment and rights") (emphasis added); United States v. Auler, 539 F.2d 642, 646 (7th Cir. 1976) (holding that telephone companies which intercept calls pursuant to §2511(2)(a)(i) may forward to the police no more of the content of those calls than "necessary to protect company rights and property."); Hodge v. Mountain States Tel. & Tel. Co., 555 F.2d 254, 260 (9th Cir. 1977) ("Congress enacted §2511(2)(a)(i) 'to reflect existing law' which allowed telephone companies to intercept communications in order to protect the *integrity* of their property.") (emphasis added).

those of any third party.... "[131] As a consequence, there is a strong argument that while ECPA may authorize private entities to monitor their *own* system and to share cyber-intelligence necessary to protect their *own* system,[132] the law likely does not authorize service providers to disclose or divulge in real time to other private entities or the government[133] the contents of electronic communications for the purpose of protecting a third party's property or rights.[134] In other words, a more narrow reading of the provider exception may cast doubt on the legality of certain cyber-information sharing methods.

The Stored Communications Act

In contrast to the Wiretap Act, which focuses on the interception and disclosure of the contents of communications in transmission, Title II of ECPA—the SCA—is centrally concerned with access to and the disclosure of both content and *non-content* based electronic communications that are kept in *storage*.[135] In relevant part,[136] the SCA in Section 2702 *generally* prohibits service

---

[131] *See Legal Issues Relating to the Testing, Use, & Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch,* 33 OP. O.L.C. 1 (2009).

[132] *See* Broggi, *supra* note 31, at 669-70; *see also Protecting America From Cyber Attacks: the Importance of Information Sharing, Hearing Before the Senate Homeland Security and Gov't Affairs Committee,* (January 28, 2015), statement of Gregory T. Nojeim, Senior Counsel and Director of the Freedom, Security and Technology Project, at pg. 5, *available at* https://d1ovv0c9tw0h0c.cloudfront.net/files/2015/01/HSGAC-Cybersec-tes-1-28-15-final-TEH.pdf (hereinafter "Nojeim Testimony").

[133] The Wiretap Act does have other means for the *government* to intercept or receive electronic communications. *See, e.g.,* 18 U.S.C. §§2516-2518 (authorizing government access to covered communications pursuant to or in anticipation of a court order); *id.* §2511(2)(i) (permitting "a person acting under color of law" to "intercept" the contents of "wire or electronic communications of a computer trespasser transmitted to, through, or from [a] protected computer" under limited circumstances).

[134] *See* Aaron J. Burstein, *Amending the ECPA to Enable a Culture of Cybersecurity Research*, 22 HARV. J.L. & TECH. 167, 188 (2008) ("Even if a researcher intercepts electronic communications contents under the provider exception, disclosing the contents to *outside* researchers might stretch the requirement of protecting the original service provider's rights or property.") (emphasis added). Moreover, even if a provider, in collecting and sharing cyber-threat information, is ostensibly acting out of self-interest, courts have been clear that ECPA, by permitting interceptions to "protect the rights or property" of the provider, does not allow "unlimited" interceptions. *See Auler,* 539 F.2d at 646 (holding that the authority of a service provider to intercept and disclose covered communications is "not unlimited"); *Councilman,* 418 F.3d at 82 (holding that it was "indisputable" that the "narrow[]" provider exception did not exempt a provider who intercepted and copy all incoming communications to gain a commercial advantage). Instead, there must be a "substantial nexus" between the monitoring and the threat to the provider's rights or property. *See* United States v. McLaren, 957 F. Supp. 215, 219 (M.D. Fla. 1997). The Department of Justice has interpreted the provider exception to permit "providers and their agents to conduct reasonable monitoring that balances the providers' needs to protect their rights and property with their subscribers' right to privacy." *See* U.S. Dep't of Justice, *supra* note 116, at 173. At least one commentator has suggested that the substantial nexus test may limit the scope of what types of information can be gathered to combat cyber-threats. *See* Burstein, *supra* note 134, at 187 ("Although cybersecurity researchers might ... provide information that allows their employers to protect their networks, this connection is likely to be highly attenuated ... since researchers usually develop methods of detecting malicious traffic, their results might not be immediately applicable to that purpose.").

[135] *See* 18 U.S.C. §§2701-2702. What sorts of "storage" that the SCA regulates will depend several statutory terms that will be explained in more detail *infra*.

[136] The SCA also prohibits unauthorized access to an ECS facility and "thereby obtains, alters, or prevents authorized access to [an] ... electronic communication while it is in electronic storage.... " *See* 18 U.S.C. §2701(a). However, Section 2701 exempts from that general prohibition "conduct authorized ... by the person or entity providing [an] ... electronic communications service," *see id.* §2701(c)(1), meaning that service providers that "obtain" electronic communication while in storage for the purpose of determining cyber-threats are likely immune from liability under the first prohibition in the SCA. *See* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 115 (3d Cir. 2003) ("[W]e read §2701(c) literally to except from Title II's protection all searches by communications service providers ... because Fraser's email was stored on Nationwide's system (which Nationwide administered), its search of that email falls (continued...)

providers engaged in either "electronic communications service" (ECS) or remote computing service (RCS) to the public from divulging the contents[137] of communications in their possessions[138] and subjects those that violate the SCA to civil liability.[139] Notwithstanding that general statement about Section 2702, the SCA is a notoriously complicated statute,[140] and, accordingly, Section 2702(a)'s central prohibition regarding the disclosure of the contents of communications requires some clarification and several caveats.

First, to run afoul of Section 2702(a)(1)-(2)'s prohibition, the entity in question must provide *either* ECS or RCS. ECS, as defined under the SCA, includes any service which provides users the means to "send or receive ... electronic communication,"[141] such as businesses that provide text messaging[142] or email[143] services. An RCS, as defined by the SCA , entails "the provisions to the public of computer storage or processing services by means of an electronic communications system."[144] Courts have interpreted an RCS to refer to the long-term processing or storage of data by an off-site third party.[145] Second, not all disclosures by an ECS or RCS are prohibited by the SCA; only disclosures of the *contents* of communications[146]—as opposed to address information, like an email address[147]—would fall within the prohibition. Third, for an *ECS provider*, only disclosures made while the underlying communication is *in electronic storage* amount to a violation of the statute[148]—a status defined by the act as either (1) temporary, intermediate storage of an electronic communication incidental to the transmission of that communication; or (2) any storage of an electronic communication for backup protection.[149] The definition of "electronic storage" has been the source of considerable disagreement, with one prominent judicial opinion

(...continued)

within §2701(c)'s exception to Title II."); *see also In re Yahoo Mail Litig.,* 7 F. Supp. 3d at 1026-27 ("The SCA grants immunity to 18 U.S.C. §2701(a) claims to [ECS providers] for accessing content on their own servers."); Crowley v. Cybersource Corp., 166 F. Supp. 2d 1263, 1272 (N.D. Cal. 2001) (holding that ECS "could not have limited access to its own facilities."); *see generally Councilman,* 418 F.3d at 82 (noting the "breadth" of §2701(c)(1)'s provider exception).

[137] 18 U.S.C. §2702 prohibits what service providers can divulge with respect to *non-content* information only as it relates to disclosures made to the government. *See id.* §2702(a)(3). For a discussion of §2702(a)(3), *see infra* "Privacy Concerns."

[138] *See* 18 U.S.C. §2702(a)(1)-(2).

[139] *See* 18 U.S.C. §2702(b)-(c) (including in the civil relief for a violation of the SCA (1) equitable relief; (2) actual damages or at least $1,000; (3) punitive damages for willful or intentional conduct; (4) attorney fees).

[140] United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998) (describing the SCA as a "complex, often convoluted, area of the law.").

[141] 18 U.S.C. §2510(15).

[142] *See, e.g.,* Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 902 (9th Cir. 2008), *rev'd on other grounds by* City of Ontario v. Quon, 560 U.S. 746 (2010).

[143] *See, e.g.,* Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004).

[144] *Id.* §2711(2). In turn, an electronic communication system is "any wire, radio, electromagnetic, photoptical or photo electronic facilities for the transmission of wire or electronic communications, and any comput facilities or rleated electronic equipment for the electronic storage of such communications." *Id.* §2510(14).

[145] *See Quon,* 529 F.3d at 901.

[146] 18 U.S.C. §2702(a)(1).

[147] *See, e.g., In re* Zynga Privacy Litig., 750 F.3d 1098, 1108 (9th Cir. 2014) (noting that "email and IP addresses 'constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers.'") (internal citations omitted).

[148] 18 U.S.C. §2702(a)(1).

[149] 18 U.S.C. §2710(17)(A)-(B).

interpreting "electronic storage" to encompass both electronic messages that have yet to be delivered to their intended recipient, as well as electronic messages in backup storage by the provider until "the underlying message has expired in the normal course,"[150] while others have criticized the notion of "electronic storage" encompassing opened emails serviced by an ECS.[151] Fourth, for an *RCS provider* to violate 18 U.S.C. Section 2702(a)(2), the provider must disclose the contents of communications that are (1) "on behalf of, and received by" a subscriber or customer of the service; and (2) "solely for the purpose of providing storage or computer processing services to ... [that] subscriber or customer."[152] The statutory prohibition necessarily excludes providers of RCS to the public who are authorized to access the contents of communication for purposes other than for storage and computer processing, such as for advertising purposes.[153]

Putting to the side the exceptions to SCA's prohibition found in 18 U.S.C. Section 2702(a)(1)-(2), unlike the Wiretap Act, the SCA's prohibition on disclosing communications in storage will be unlikely to prohibit many forms of cyber-information sharing. After all, to violate the statute, a company must not only disclose the *contents* of communications to another private entity, but the company doing the disclosure must provide ECS or RCS to the *public*.[154] In other words, if, for example, an email provider to the public shares the IP address that was the source of a malicious email to a ISAO, that email provider did not share content information and therefore likely did not violate the SCA. Moreover, if a private entity provides email services to its employees and shares the text of an email that is the source of a computer virus with another company, that private entity likely did not violate the SCA because that entity does not provide ECS or RCS to the *public*.

Nonetheless, many Internet Service Providers (ISPs) or email providers ostensibly provide ECS or RCS to the public,[155] and those companies may be interested in sharing the *contents* of information with outsiders for cybersecurity purposes. If so, it is uncontroversial to say that because of disputes over key terms like "electronic storage" and "RCS" and "ECS," the SCA, as currently written and interpreted, is hardly a model of clarity.[156] The resulting ambiguity about the legality of information sharing within the SCA's general ambit may deter providers of ECS or RCS to the public from sharing cyber-threat information with other private entities.[157] After all,

[150] *See Theofel,* 359 F.3d at 1076.

[151] *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 987 (C.D. Cal. 2010); United States v. Weaver, 636 F. Supp. 2d 769, 771-73 (C.D. Ill. 2009); *see generally* 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, 1216-18 (2004) (explaining that emails that are in transit or have been delivered but are unopened are in electronic storage by an ECS, while emails that have been opened and saved exclusively on a server are stored in RCS) (hereinafter "Kerr-Guide").

[152] 18 U.S.C. §2702(a)(2)(A)-(B).

[153] *Id.* §2702(a)(2)(B); *see also* Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256, 264 n.8 (S.D.N.Y. 2008); Juror Number One v. Superior Court, 206 Cal. App. 4th 854, 862 ("Thus, if the service *is* authorized to access the customer's information for other purposes, such as to provide targeted advertising, SCA protection may be lost.").

[154] 18 U.S.C. §2702(a)(1)-(2).

[155] *See* Kerr-Guide, *supra* note 151, at 1229-33; *see also In re* Application of the United States of America for a Search Warrant for Contents of Electronic Mail and for an Order Directing a Provider of Electronic Communication Services to not Disclose the Existence of the Search Warrant, 665 F. Supp. 2d 1210, 1214 (D. Or. 2009) ("Today, most ISPs provide both ECS and RCS; thus, the distinction serves to define the service that is being provided at a particular time (or as to a particular piece of electronic communication at a particular time), rather than to define the service provider itself.").

[156] *See Smith*, 155 F.3d at 1055.

[157] *See* Burstein, *supra* note 134, at 189; *see also infra* note 401 (discussing potential litigation costs).

ambiguity in the law often breeds litigation, and the costs of litigation may be significant enough to deter companies from engaging in cyber-information sharing.[158]

The hesitancy to participate in information sharing schemes may exist notwithstanding several exceptions[159] to the SCA's general prohibition on the disclosure of certain types of electronic communication held in storage.[160] For example, while the SCA excludes from its prohibition on the disclosure of communications disclosures made to a "person employed or authorized ... to forward such communication to its destination,"[161] that exception only eliminates liability for those entities wishing to gather and share cyber-threat information *within* that organization[162] and does not sanction the sharing of the contents of a communication with an outsider. Moreover, the SCA also contains a consent exception, allowing an ECS or RCS provider to divulge the contents of a communication if the sender or recipient of that communication consents or, in the case of an RCS, if the *subscriber* of the communication consents to the disclosure.[163] Like the Wiretap Act's consent exception, the SCA's consent exception is largely fact dependent, arguably providing little assurance to a communications services provider that wishes to wholly eliminate litigation risk.[164] More specifically, the scope of the SCA's consent exception is directly linked to a service provider's status as providing ECS or RCS, which may make the viability of the consent defense contingent on the murky distinction between when a provider is acting in either role.[165] Finally, similar to the Wiretap Act, the SCA also contains a provider exception, and, much like its counterpart in the Wiretap Act, the SCA's provider exception is limited to allowing disclosures that are necessary for the "protection of the rights or property of the *provider*"[166] and arguably does not extend to the protection of third parties that the provider may wish to share cyber-intelligence.[167]

---

[158] *Id.*

[159] Besides the other exceptions mentioned in this paragraph, under the SCA's exceptions to the prohibition in 18 U.S.C. §2702(a)(1)-(2), providers may divulge the contents of a communication to another private party to the extent the disclosure is made: (1) to the addressee or intended recipient of such communication, *id* §2702(b)(1), or (2) to the National Center for Missing and Exploited Children as required by federal statutes intended to prevent sexual exploitation or trafficking of children or criminalize the possession, creation, or transportation of child pornography, *id.* §§2702(b)(6), 2252A.

[160] *See* 18 U.S.C. §2702(b).

[161] *Id.* §2702(b)(4)

[162] *See* Burstein, *supra* note 134, at 189.

[163] *See* 18 U.S.C. §2702(b)(3) ("A provider ... may divulge the contents of a communication ... with the lawful consent of the originator or an address or intended recipient of such communication, or the subscriber in the case of [RCS].")

[164] *Compare* Bower v. Mirvat El-Nady Bower, 808 F. Supp. 2d 348, 351 (D. Mass. 2011) (finding no consent); *with* Flagg v. City of Detroit, 252 F.R.D. 346, 364 (E.D. Mich. 2008) (finding consent).

[165] *See Theofel,* 359 F.3d at 1076; *Quon,* 529 F.3d at 901-02; *see generally* Kerr-Guide, *supra* note 151, at 1215-16 ("The classifications of ECS and RCS are context sensitive: the key is the provider's role with respect to a particular copy of a particular communication, rather than the provider's status in the abstract. A provider can act as an RCS with respect to some communications, an ECS with respect to other communications, and neither an RCS nor an ECS with respect to other communications.").

[166] *See* 18 U.S.C. §2702(b)(5) ("A provider ... may divulge the contents of a communication ... as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service.") (emphasis added).

[167] *See* Burstein, *supra* note 134, at 190; *see also supra* note 133 (discussing the "substantial nexus" test).

The Pen/Trap Act

The final major federal privacy law potentially relevant to cyber-information sharing amongst private parties is found in Title III of ECPA, Pen/Trap Act.[168] The Pen/Trap Act has been referred to as the "non-content counterpart" to the Wiretap Act, in that the Pen/Trap Act is concerned with the *real time* capturing of *non-content* information,[169] such as IP addresses and the "to" and "from" fields in an email.[170] Specifically, in 18 U.S.C. Section 3121, the Pen/Trap Act generally prohibits any person from installing or using a "pen register or a trap and trace device," devices used outside of the ordinary course of business that capture either incoming or outgoing non-content electronic information about the source of a communication, without first receiving permission from a court.[171] Violations of the Pen/Trap Act can result in criminal penalties, including not more than one year in prison.[172] Like its counterpart the Wiretap Act, the Pen/Trap Act, also contains several exceptions to its general prohibition, including a (1) "provider exception," which permits service providers to use pen/trap devices for the "operation, maintenance, and testing of [an] ... electronic communication service" or to protect the "rights and property" of the provider or the "users of that service from abuse of service or unlawful use of service,"[173] (2) "consent exception," which allows the use of pen/trap devices where the user of the service has provided consent.[174] Nonetheless, in sharp contrast to the Wiretap Act and the SCA, the Pen/Trap Act contains no provisions barring the *disclosure or divulgence* of non-content information derived from a pen/trap device.[175]

For a private entity wishing to share non-content cyber-threat information with a third party, the Pen/Trap Act likely does not raise serious legal concerns. First, the Pen/Trap statute's provider exception likely eliminates any potential criminal liability that could arise from a company

---

[168] 18 U.S.C. §§3121-3127.

[169] *See* Burstein, *supra* note 134, at 191.

[170] *See* Daniel J. Solove, *Reconstructing Electronic Surveillance Law,* 72 GEO. WASH. L. REV. 1264, 1287 (2004) (contending that "e-mail headers (the addressing information on e-mail messages), IP addresses, and Uniform Resource Locators ... fall under [the] definition [of information captured by a pen/trap device]."); *see also* Dep't of Justice, *supra* note 116, at 154 ("Because Internet headers contain both 'to' and 'from' information, a device that reads the entire header ... is both a pen register and trap and trace device.... ").

[171] 18 U.S.C. §3121(a). Specifically, in relevant part, the Pen/Trap statute defines a "pen register" as a device that records or captures information that is "reasonably likely to identify the source of [an] ... electronic communication," *see id.* §3127(3), whereas a "trap and trace device" is defined as one that captures incoming electronic or other impulses that "identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of [an] ... electronic communication," *id.* §3127(4). Both definitions exclude devices that capture content information, *id.*§3127(3)-(4), and the definition for a pen register excludes "any device ... used by a provider or customer of [an] ... electronic communication service for billing, or recording as an incident to billing ... or any device ... used ... for cost accounting or other like purposes in the ordinary course of business," *id.*§3127(4).

[172] *See id.*§3121(d).

[173] 18 U.S.C. §3121(b)(1).

[174] *Id.* §3121(b)(3). The government can obtain authority to install a pen/trap device by certifying to a court "that the information likely to be obtained [from a pen register] is relevant to an ongoing criminal investigation" being conducted by a law enforcement agency. *See* 18 U.S.C. §3122(b).

[175] *Cf.* United States v. Reed, 575 F.3d 900, 914 (9th Cir. 2009) (concluding that the Pen/Trap Act contains no requirement that non-content information form a pen/trap device be sealed from public disclosure); *see* Burstein, *supra* note 134, at 192 ("The Pen/Trap statute's exception, however, si concerned only with the condition for allowing a service provider to install a pen register; the statute lacks a corresponding disclosure provision."); *see also* Broggi, *supra* note 31, at 672 ("Unlike the Wiretap Act however, the statute is silent regarding voluntary disclosure of information obtained under these exceptions.").

monitoring and capturing non-content information for cybersecurity purposes. After all, the Pen/Trap Act's provider exception sweeps more broadly than the provider exceptions in the Wiretap Act or the SCA, in that Title III of ECPA allows providers to use a pen/trap device "relating to the operation, maintenance, and testing of [an] ... electronic communication system.... "[176] Given that nearly any electronic communication system, such as email or Internet communication, necessarily depends on routing information from one source to another,[177] it is arguable that most private entities with genuine cybersecurity concerns may likely be capturing non-content information as a natural product of the operating of an electronic communication system anyway.[178]

Moreover, even if an entity's decision to capture non-content address information is not related to the "operation, maintenance, and testing of [an] ... electronic communication system," the second clause of the Pen/Trap Act's provider exception allows the use of a pen/trap device to protect the rights or property of the provider or the users of the service from "abuse of service or unlawful use of service,"[179] which would appear to encompass the circumstance where a private entity collects non-content information to identify the source of a potential cyber-threat.[180] In addition, even if the provider exception does not allow the use of a pen/trap device, the consent exception would allow a provider to capture non-content cyber-threat information with the agreement of the provider's user.[181] Importantly, because the Pen/Trap Act only criminalizes the illegal use of pen/trap devices and does not regulate the disclosures of non-content information culled from a pen/trap device, once a provider has legally used a pen/trap device, there appears to be no reason why a private entity should fear liability under the Pen/Trap Act if a company were, for example, to share the IP address that was the source of malware with another private company.[182]

Other Federal and State Privacy Laws

While ECPA is the most prominently mentioned federal privacy law that could implicate cyber-threat information sharing efforts, other federal privacy laws could also plausibly deter the exchange of cyber-intelligence amongst private entities. As noted above, ECPA's privacy protections are tied to (1) the age of the underlying communication, with communications in storage generally getting less protection than communications that are being transferred in real time, and (2) whether the underlying communication reveals substantive content, with non-content information, such as IP addresses and email addresses, receiving fewer protections under the statute.[183] In contrast to ECPA, a host of various federal privacy laws target *specific industries*

[176] 18 U.S.C. §3121(b)(1).

[177] *See* David D. Clark and Susan Landau, *Untangling Attribution*, 2 HARV. NAT'L SEC. J. 531, 534-35 (2011) (describing all "data transport service of the Internet" as being based on packets, "small units of data prefixed with delivery instructions.").

[178] *See* Columbia Pictures Industries v. Bunnell, No. 06-1093FMCJCX, 2007 WL 2080419, at *11 (C.D. Cal. May, 29, 2007 (holding that the capturing of an IP address necessary to "operate [a] website" falls within the Pen/Trap Act's provider exception).

[179] 18 U.S.C. §3121(b)(1).

[180] *See* Broggi, *supra* note 31, at 672 ("The purpose of using signatures to scan network traffic is to protect the network and its users from malicious activity.").

[181] 18 U.S.C. §3121(b)(3).

[182] There could be an argument that sharing non-content information with the *government* raises liability issues under the SCA. *See infra* "Privacy Concerns." Nonetheless, neither the SCA nor the Pen/Trap Act provide for criminal or civil liability when a private entity discloses non-content information to another private entity.

[183] *See generally* Omer Tenne, *Quantifying Harm Structure: A New Harm Matrix for Cybersecurity Surveillance,* 12 J. (continued...)

that tend to control *personally identifying information* (PII), such as names, addresses, phone numbers, or Social Security numbers. For example, the Cable Communications Policy Act of 1984 (CCPA) generally prohibits "cable operators"[184] from collecting and disclosing PII,[185] subjecting entities that violate the CCPA's privacy protections to civil liability.[186] Some courts, interpreting the CCPA, have concluded that cable providers when providing Internet services can be subject to the Act's privacy provisions,[187] raising the specter of civil liability if a cable ISP were to disclose PII—like a name or an email address—while sharing cyber-threat information with another private entity.

Much as the CCPA could raise liability concerns for cable ISPs wishing to share cyber-information with other private entities, so too could a variety of federal privacy laws raise legal questions for the entities that are regulated by such laws. Indeed, several discrete federal privacy laws regulate how PII is collected and disseminated. These laws target a variety of distinct entities, including

- consumer reporting agencies[188]

(...continued)

ON TELECOMM. & HIGH TECH. L. 391, 393-95 (2014) (discussing the key "legal distinctions that serve as proxies for the measurement of privacy and civil liberties harms.").

[184] The CCPA defines cable operators as:

> any person or group of persons (A) who provides cable service over a cable system and directly or through one or more affiliates owns a significant interest in such cable system, or (B) who otherwise controls or is responsible for, through any arrangement, the management and operation of such a cable system.

47 U.S.C. §522(5).

[185] 47 U.S.C. §551(b)(1) & (c)(1). The statute does not define the term of art "personally identifiable information," but does exclude from the term "any record of aggregate data which does not identify particular persons." *Id.* §551(a)(2)(A). Nonetheless, courts have recognized the term to include "specific information about the subscriber, or a list of names and addresses on which the subscriber is included.... " *See* Scofield v. Telecable of Overland Park, Inc., 973 F.2d 874, 876 n. 2 (10th Cir.1992). Another court has held that a person's name, address, and telephone are included in term "personal identifiable information." *See* Warner v. Am. Cablevision of Kansas City, Inc. ., 699 F.Supp. 851, 855 (D.Kan.1988); *see also* Pruitt v. Comcast Cable Holdings, LLC, 100 Fed. App'x. 713, 716 (10th Cir.2004) (holding that a cable box did not contain PII where, *inter alia*, it did not contain the name, address, or "any other information regarding the customer."). There are several exceptions to the CCPA's general prohibition on collecting or disclosing PII, including a consent exception, *see* 47 U.S.C. §551(b)(1) & (c)(1), an exception based on the need to conduct a "legitimate business activity," *id.* §551(b)(2) & (c)(2), and an exception for disclosure to the government based on a court order, *id.*§551(c)(2)(B).

[186] *Id.* §551(f) (allowing for liquidated damages calculated at a rate $100 for each day of a violation and punitive damages).

[187] *See* Digital Sin, Inc. v. Does 1-176, 279 F.R.D. 239, 241 (S.D.N.Y. 2012) (finding that "many ... ISPs ... qualify as 'cable operators' under the CPPA and subject to the restrictions found in 47 U.S.C. §551); *see also* Warner Bros. Record Inc. v. Doe, 555 F. Supp. 2d 1, 2 (D.D.C. 2008) (ordering a subpoena to be issued upon a cable ISP under 47 U.S.C. §551(c)(2)); TCYK, Inc. v. Does 1-20, No. 3:13–cv–3927–L, 2013 WL 6475040, at *2 (N.D. Tex. December 10, 2014) ("The Cable Privacy Act prohibits cable operators, which includes the ISPs identified here, from disclosing subscribers' personal information without their consent or a court order."); AF Holdings LLC v. Doe, No. 12cv1519–BTM, 2012 WL 3238023, at *1-3 (S.D. Cal. January 29, 2013) (issuing an order under the CCPA for Cox Communications to produce "produce documents and information sufficient to identify the user of the specified IP address."); *see generally* United States v. Kennedy, 81 F. Supp. 2d 1103, 1111 (D. Kan. 2000) (assuming without holding that the CCPA applies to a "provider of high speed Internet services over cable wires"); *but see* Klimas v. Comcast Cable Communs., Inc., 465 F.3d 271, 273 (6th Cir. 2006) (holding that the CCPA's prohibition on the collection and dissemination of PII did not extend cable providers that also functioned as ISPs).

[188] *See* 15 U.S.C. §§1681, *et seq*. (Fair Credit Reporting Act).

- operators of websites or online services directed to children[189]
- financial institutions[190]
- videotape service providers[191]
- educational agencies or institutions[192]
- health plans, health care clearinghouses, and health care providers[193]
- telecommunications carriers[194]

To the extent any one of these entities wishes to share cyber-intelligence within its possession with others in the private sector, legal questions may abound if any of the information to be shared contains material that is potentially protected under federal privacy law. None of the aforementioned federal privacy laws specifically contemplate any exceptions for the sharing of cyber-information for cybersecurity purposes. And, there is very little, if any, case law examining how a given law applies to the specific context of the collection and dissemination of information for cybersecurity purposes, leaving a legal lacuna for those regulated entities that may wish to engage in cyber-information sharing.

Beyond *federal* privacy laws, *states and localities* have enacted countless laws that may prevent or deter private entities from sharing cyber-intelligence with others. All but one of the fifty states has an eavesdropping law that is generally modeled off the Wiretap Act,[195] and a majority of states regulate the collection and dissemination of electronic communications.[196] While many of the state communications privacy laws mirror federal law, state laws are often more restrictive or may simply regulate different aspects of communications privacy than federal law,[197] multiplying

[189] *See id.* §§6501-6506 (Children's Online Privacy Protection Act).

[190] *See id.* §§6801-6809 (Gramm-Leach-Bliley Act (GLBA)).

[191] *See* 18 U.S.C. §2710 (The Video Privacy Protection Act).

[192] *See* 20 U.S.C. §1232g (Family Educational Rights and Privacy Act).

[193] *See* 42 U.S.C. §300gg, 29 U.S.C §§1181 *et seq*., 42 U.S.C. §§1320d *et seq*., 45 C.F.R. Part 160 and Part 164, Subparts A and E (Health Insurance Portability and Accountability Act (HIPAA)).

[194] *See* 47 U.S.C. §222 (Federal Communications Act). Section 222 could take on an important role with respect to ISPs, who may be the primary entities interested in engaging in cyber-information sharing, depending on whether such entities are considered a "common carrier" for purposes of Title II of the Communications Act and on whether the Federal Communications Commission promulgates new rules regarding how ISPs should protect customer proprietary network information under Section 222. *See* Press Release, *FCC Adopts Strong, Sustainable Rules to Protect Open Internet,* Federal Communications Commission, (February 26, 2015), at pg. 4, *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0226/DOC-332260A1.pdf (noting that, under newly proposed net-neutrality rules, Section 222 of the Communications Act will apply to ISP); *see also In the Matter of* Protecting and Promoting the Open Internet, GN Docket No. 14-28, ¶¶ 53-54, 462-467 (F.C.C. February 26, 2015), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0312/FCC-15-24A1.pdf (contemplating a "separate rulemaking procedure" for imposing customer privacy rules respecting ISPs).

[195] *See* CRS Report R41734, *Privacy: An Abridged Overview of the Electronic Communications Privacy Act*, by (name redacted), at p. 81 ("Appendix A"). Vermont is the only state that has not adopted its own state wiretapping statute. *Id.*

[196] *Id.*

[197] *See* Elisabeth Pride, *Down the Rabbit's Hole: Baby Monitors, Family Movies and Wiretap Law,* 23 J. AM. ACAD. MATRIMONIAL LAW. 131, 149 (2010) ("Generally speaking, the state wiretap laws are modeled on the federal Act and substantially mirror its language, but may be more restrictive in many respects.... "); *see also* Daniel R. Dinger, *Should Parents Be Allowed to Record a Child's Telephone Conversations When They Believe the Child Is in Danger?: An Examination of the Federal Wiretap Statute and the Doctrine of Vicarious Consent in the Context of a Criminal*
(continued...)

the legal questions facing those entities wishing to engage in cyber-information sharing. For example, eight states currently generally require both parties to an electronic communication to consent to its interception and/or further dissemination,[198] allowing, in the words of one commentator, cyber "attackers a veto on whether their packets are inspected for malicious code"[199] and potentially deterring some entities from collecting and divulging cyber-threat information to others.

Moreover, much like the federal government, some states have laws that target the collection and divulgence of PII within the possession of entities that may wish to engage in cyber-information sharing.[200] Although an examination of the various state privacy laws is beyond the scope of this report, these laws may raise liability concerns for entities that do business in multiple states and wish to disseminate cyber-threat information outside of the company.

Antitrust Laws

In addition to federal and state privacy laws, antitrust laws also have generated liability concerns for private entities that wish to collaborate over cybersecurity.[201] Indeed, in a recent survey, more than a quarter of IT professionals identified "anti-competitive concerns" as one of the central reasons for not participating in information sharing programs.[202] Deterring anticompetitive conduct by businesses, such as coordinated action that undermines competition, is at the heart of federal antitrust law.[203] Specifically, the Supreme Court in interpreting the Sherman Antitrust Act—the "primary federal antitrust enforcement mechanism"[204]—has recognized that the law's facial prohibition in Section 1 on *all* contracts, combinations, or conspiracies that result in a restraint of trade or commerce[205] should be read to prohibit only those agreements that *unreasonably* restrain trade.[206] While courts interpreting the reach of the Sherman Act generally view any concerted activity with some degree of skepticism,[207] certain agreements, such as price fixing and market allocation among competitors, are viewed as being so "inherently

(...continued)

Prosecution, 28 Seattle U.L. Rev. 955, 965-67 & n.58 (2005) (discussing the differing state wiretap laws).

[198] *See* Cal. Penal Code §632.7; Fla. Stat. Ann. §934.03; Ill. Comp. Stat. Ann. ch. 720 §§5/14-2—5/14-3; Md. Cts. §Jud. Pro. Code. Ann. §10-402(c)(3); Mich. Comp. Laws. Ann. §750.539c; Mont. Code. Ann. §§45-8-213; Ore. Rev. Stat. §165.540(c); Pa. Stat. Ann. tit. 13 §1504.

[199] *See* Bipartisan Policy Center, *supra* note 28, at 11.

[200] *See, e.g.,* Minn. Stat. §325M.02.(Minnesota's Internet Privacy Act) (generally prohibiting ISPs from "knowingly disclose a consumer's 'personally identifiable information.'").

[201] *See* Palmer, *supra* note 72, at 318; *see also* Peretti, *supra* note 32, at 5.

[202] *See* Ponemon Institute—Threat Intelligence, *supra* note 33, at 4; *see generally* Sales, *supra* note 26, at 1530 (finding that antitrust "liability fears appear to be fairly widespread" amongst firms that may wish "to share information or to adopt common security standards.").

[203] *See id.* at 1528-29. Several federal laws have prohibitions on anticompetitive behavior, including the Sherman Act, *see* 15 U.S.C. §§1-7, the Wilson Tariff Act, *id.* §§8-11, the Clayton Act, *id.* §§12-27, and the Federal Trade Commission Act, *id.* §45.

[204] *In re* Flonase Antitrust Litig., 692 F. Supp. 2d 524, 539 (E.D. Pa. 2010).

[205] *See* 15 U.S.C. §1.

[206] Board of Trade of Chicago v. United States, 246 U.S. 231, 238, 38 S. Ct. 242, 62 L. Ed. 683 (1918) (reasoning that the term "restraint of trade" in §1 cannot possibly refer to any restraint on competition because "[e]very agreement concerning trade, every regulation of trade, restrains. To bind, to restrain, is of their very essence").

[207] Copperweld Corp. v. Independence Tube Corp., 467 U.S. 752, 768 (1984).

anticompetitive that each is illegal *per se* without inquiry into the harm it has actually caused."[208] Other agreements, such as mergers or joint ventures that may facilitate more effective competition, are adjudged under the "rule of reason," in which a court will weigh the legitimate justifications for a restraint against any anticompetitive effects.[209] In other words, determining whether a given agreement between two private businesses violates the Sherman Act largely depends upon the specifics of that particular agreement.[210] Businesses that are alleged to violate federal antitrust laws face potential criminal prosecutions,[211] as well as civil actions that could be initiated by the federal government,[212] state governments,[213] or even aggrieved private litigants.[214] Civil litigation risks treble damages—damages three times the amount of actual damage—being paid to successful plaintiffs.[215]

While fears abound that any coordination on cyber-defense could give rise to antitrust liability,[216] the likelihood of such liability will likely depend on the nature and purpose of the underlying agreement to share cyber-threat information.[217] Exchanges of information among competitors do not constitute *per se* violations of the Sherman Act, as the Supreme Court has found that such practices can "increase economic efficiency and render markets more ... competitive."[218] Moreover, the Court has been reluctant "to condemn rules adopted by professional associations as unreasonable *per se*.... "[219] As a consequence, perhaps a few agreements to coordinate on cyber-defense—such as an agreement amongst competitors to "implement a uniform set of cyber-

[208] *Id.*; *see also* Nat'l Collegiate Athletic Ass'n v. Bd. of Regents of Univ. of Okla., 468 U.S. 85, 103-04 (1984) ("*Per se* rules are invoked when surrounding circumstances make the likelihood of anticompetitive conduct so great as to render unjustified further examination of the challenged conduct."); United States v. Socony-Vacuum Oil Co., 310 U.S. 150, 223 (1940) ("[C]ombination[s] formed for the purpose and with the effect of raising, depressing, fixing, pegging, or stabilizing the price of a commodity in interstate or foreign commerce is illegal *per se*.").

[209] *See Copperweld Corp.*, 467 U.S. at 768; *see generally Board of Trade,* 246 U.S. at 238 ("[T]he court must ordinarily consider the facts peculiar to the business to which the restraint is applied; its condition before and after the restraint was imposed; the nature of the restraint and its effect, actual or probable. The history of the restraint, the evil believed to exist, the reason for adopting the particular remedy, the purpose or end sought to be attained, are all relevant facts.").

[210] *See* Ken Heyer, *A World of Uncertainty: Economics and Globalization of Antitrust,* 72 ANTITRUST L.J. 375, 378 (2005) (arguing that "antitrust analysis and decisionmaking" entails "considerable uncertainty and imprecision surrounding particular case decisions.").

[211] *See* 15 U.S.C. §1 (subjecting those guilty of violating §1 to fines "not exceeding $ 100,000,000 if a corporation, or, if any other person, $ 1,000,000," and "imprisonment not exceeding 10 years.... ").

[212] *Id.*§15a.

[213] *Id.*§15c.

[214] *Id.* §15.

[215] *Id.* §15(a) ("[A]ny person who shall be injured in his business or property by reason of anything forbidden in the antitrust laws ... shall recover threefold the damages by him sustained.... ").

[216] *See, e.g.,* Info. Tech Industry Council, *ITI Recommendation: Addressing Liability Concerns Impeding More Effective Cybersecurity Information Sharing* 3 (2012), *available at* http://www.itic.org/dotAsset/fae2feab-7b0e-45f4-9e74-64e4c9ece132.pdf (suggesting that the if a company "voluntarily reports what may be a cybersecurity threat or incident in an information sharing entity, such as an ISAC," that includes competitors of the company, a "[p]otential result" would be for a "plaintiff [to] claim[] that the information shared is an effort to harm competition," resulting in a lawsuit under federal antitrust laws).

[217] *See* Dep't of Justice and Fed. Trade Comm'n, *Antitrust Policy Statement on Sharing of Cybersecurity Information* 8 (April 10, 2014), *available at* http://www.justice.gov/atr/public/guidelines/305027.pdf (hereinafter "DOJ-FTC Joint Statement") (noting that any antitrust analysis of a given cyber information sharing scheme is "intensely fact-driven.").

[218] *See* United States v. United States Gypsum Co., 438 U.S. 422, 443 n.16 (1978).

[219] *See* FTC v. Indiana Federation of Dentists, 476 U.S. 447, 458 (1986).

security practices"[220] by either agreeing to "pass on" certain associated costs to customers[221] or adopt cybersecurity practices that provide inferior products to end users[222]—may "amount to a 'naked' restraint that results in reflexive condemnation under the *per se* rule."[223] Nonetheless, most efforts to share cybersecurity information amongst private entities, particularly within a formal organization like an ISAC, will likely be adjudged under the rule of reason.[224] A rule of reason analysis would weigh the legitimate justifications for engaging in concerted efforts to share cyber-information against any anticompetitive effects.[225] As such, a rule of reason analysis regarding cyber-information sharing may weigh the interest in combatting fraudulent cyber-activity[226] versus the potentiality of certain actors being excluded from the cyber information forum for anticompetitive reasons.[227] Nonetheless, there is no case law that squarely addresses how antitrust laws apply to coordinated efforts to combat cyber-threats, and given the central role of common law in defining the limits of federal antitrust law, the net result may be considerable legal uncertainty for those private entities that may wish to engage in such activities.

Recognizing the legal uncertainty that exists with respect to antitrust law and cybersecurity information sharing, in April of 2014, DOJ and the Federal Trade Commission (FTC) issued a joint policy statement that attempted to clarify the extent to which the exchange of cyber-threat information amongst private parties could raise antitrust issues.[228] The joint policy statement confirmed that information sharing agreements are typically examined under a rule of reason analysis,[229] and the statement continued by recognizing that the exchange of cyber-threat information has numerous positive effects that will weigh in favor of its legality, including helping "secure our nation's networks of information and resources."[230] Moreover, the joint policy statement emphasized that the typical nature of cyber-threat information—described as being "very technical in nature"—is often unlikely to contain "competitively sensitive information" that would allow participants to "raise prices or reduce output, quality, service, or

[220] *See* Sales, note 26, at 1531.

[221] *See id.* ("Whether the companies have agreed to purchase and install new firewall software ... industry members ... might decide to pass on these costs to consumer, either in the form of a general price hike or as free standing surcharge."); *see generally* United States v. Container Corp. of Am., 393 U.S. 333, 338 n.4 (1969) ("[A]ll forms of price-fixing are per se violations of the Sherman Act.").

[222] Sales, note 26, at 1531-32 ("Suppose firms in a particular industry agree to install intrusion-detection or –prevention capabilities to scan for malware ... [t]he effect [of which] is often to slow down the network's performance ... [T]he shared security standards still plausibly could be described as an unlawful price-fixing agreement ... [because] the firms have agree to require consumers to pay the *same* price for a *lesser* product.... ").

[223] *Id.* at 1531.

[224] *See United States Gypsum Co*., 438 U.S. at 443 n.16; *see also* Augusta News Co. v. Hudson News Co., 269 F.3d 41, 47 (1st Cir. 2001) ("[T]he legality of *most* kinds of agreements (*e.g.*, R&D projects, information sharing, distribution contracts) is tested by the rule of reason.").

[225] Paladin Assocs. v. Montana Power Co., 328 F.3d 1145, 1156 (9th Cir. 2003).

[226] *Cf.* Michelman v. Clark-Schwebel Fiber Glass Corp., 534 F.2d 1036, 1048 (2d Cir. 1976) (holding that the concerted exchange of credit information was "necessary to protect ... against" fraud and, therefore, did not amount to "violation of §1 ... provided that any action taken in reliance upon [such information was] the result of each firm's independent judgment.... ").

[227] *Cf.* Reg'l Multiple Listing Serv. of Minn., Inc. v. Am. Home Realty Network, Inc., 9 F. Supp. 3d 1032, 1039 (D. Minn. 2014) (holding that an allegation that several real estate agents colluded in creating an information sharing network to exclude another broker sufficed to satisfy a Sherman Act §1 claim).

[228] *See* DOJ-FTC Joint Statement, *supra* note 217.

[229] *Id.* at 5.

[230] *Id.* at 6.

innovation."[231] Instead, the two agencies underscored that the primary antitrust concern in the context of cyber information sharing is the sharing competitively sensitive information, such as "current, and future prices, cost data, or output levels" that could allow for "competitive coordination among competitors."[232]

Notwithstanding the value of the joint guidance, as the guidance concedes, any analysis of the legality of a cyber-information sharing agreement is "intensely fact-driven,"[233] and, given the predominant role of the rule of reason with respect to examining the legality of any cyber-threat sharing agreements,[234] definitive conclusions by the government about the legality of cybersecurity information sharing arrangements vis-à-vis antitrust law may simply be impossible.[235] Moreover, given the role of private parties in enforcing federal antitrust law through civil lawsuits,[236] even if government entities like the FTC and the DOJ generally agreed that antitrust laws should not be enforced with respect to concerted actions over cybersecurity, nothing prevents an aggrieved private party from initiating an antitrust lawsuit to prevent collaboration over cyber-information sharing,[237] meaning that without a change in the current law liability risks from antitrust suits may remain for any private entity interested in sharing cybersecurity information.

Tort Law

Another often-cited source of liability that may dissuade private entities from participating in cyber-information sharing schemes is tort law, specifically torts founded upon negligence– that is, the fear that by sharing and obtaining cyber-information a private entity may be liable for negligently failing to act upon certain threat information.[238] Generally under tort law, to establish that a defendant has acted negligently, a plaintiff must show: (1) a duty of care owed to the plaintiff by the defendant; (2) a breach of that duty by the defendant; (3) causation (i.e., the resulting injury was both the "but for" and "proximate cause or foreseeable consequence of the risk created by the defendant's act or omission"); and (4) a cognizable injury or harm to the plaintiff.[239] In the context of a lawsuit following a cyberattack, an injured party may seek

[231] *Id.* at 7-8.

[232] *Id.* at 4.

[233] *Id.* at 8.

[234] *Cf.* FTC v. Acavis, Inc. 133 S. Ct. 2223, 2245 (Roberts, C.J., dissenting) (describing the rule of reason as "unruly").

[235] The DOJ has developed a business review procedure, whereby groups can submit a specific plan to collaborate on cybersecurity efforts to the Justice Department for a determination by the agency of whether the proposed collaboration would raise antitrust concerns. *See* 28 C.F.R. §50.6; *see, e.g.,* Letter from Joel I. Klein, Assistant Attorney General, Dep't of Justice, Antitrust Div., to Barbara Greenspan, Assoc. Gen. Counsel, Elec. Power Research Inst., Inc. (October 2, 2000), *available at* http://justice.gov/atr/public/busreview/6614.htm.

[236] 15 U.S.C. §15(a).

[237] In order to succeed on such a claim, in addition to demonstrating a violation of federal antitrust law, a private party would have demonstrate an "antitrust injury"—i.e., that it possesses "antitrust standing"—which requires a showing that the plaintiff was harmed by the defendant's anticompetitive contract combination, or conspiracy, and that harm flowed from an "anti-competitive aspect of the practice under scrutiny." Atl. Richfield Co. v. USA Petroleum Co., 495 U.S. 328, 334 (1990).

[238] *See, e.g.,* Eric Engleman, *Companies Want Lawsuit Shield to Share Cyber Threat Data*, BLOOMBERG BUS. WK. (March 7, 2013), http://www.businessweek.com/news/2013-03-07/companies-want-lawsuit-shield-to-share-cyber-threat-data ("Companies are concerned about ... negligence lawsuits for failing to act on information they receive.... ").

[239] *See* Nat'l Research Council, CRITICAL INFORMATION INFRASTRUCTURE PROTECTION AND THE LAW: AN OVERVIEW OF KEY ISSUES 45-46 (Stewart D. Personick & Cynthia A. Patterson eds., 2003).

compensation from a company whose network was breached, arguing that the company owed its customers a duty of reasonable security to protect against cybercriminals stealing their data.[240] However, while courts have *generally* recognized that "cyber attacks are [a] foreseeable" risk for which a service provider must account,[241] courts have been fairly reluctant to find that a *particular* cyberattack should have been anticipated by a service provider.[242] After all, just as a business has no duty to protect its customers against unforeseeable crimes from third parties,[243] so too must the "duty to implement security thwarting third-party cybercrimes ... turn on whether the crime was foreseeable."[244] In other words, under tort law, a business likely does not have a duty to guard against "innovative [cyber-]breaches that have no known or effective defense at the time of the attack."[245]

Because tort liability for a cyberattack will likely turn on the amount of knowledge a given party may have about a cyberattack, cyber-information sharing schemes have the potential to change the tort liability calculus for those entities that participate. For example, if a company opts to *share* information about the origins of a recent cyberattack perpetrated on that company with a public information sharing group, like an ISAC, the company may be admitting that it could have foreseen the attack or mitigated its effects in some way, providing potential plaintiffs with credible evidence to support a potential tort lawsuit. Likewise, entities that *receive* information about a potential cyberattack, fail to act, and then subsequently are targeted by the attack, can no longer credibly claim that the harm from the cyberattack was unforeseeable. In this sense, tort law can have the perverse effect of incentivizing private entities to "simply stay[] in the dark" about potential cyberattacks and to not participate in cyber-information sharing programs.[246]

Nonetheless, even if participation in a cyber-information sharing agreement increases tort liability risks, it remains very difficult for a plaintiff to succeed on the theory that a private entity failed to prevent a cyberattack. First, in order for cyber-threat sharing to increase tort liability risks, an entity would have to have some considerable bad luck. The company in question would not only have to suffer a cyberattack, but that cyberattack would have to be linked to a cyberattack in which information was shared about, *and* the cyberattack would have to result in actual damages for a plaintiff. Notwithstanding popular media accounts regarding potential losses created by a

---

[240] *Id.* at 45.

[241] *See* Baidu, Inc. v. Register.com, Inc., 760 F. Supp. 2d 312, 320 (S.D.N.Y. 2010).

[242] *See, e.g.,* Citizens Bank of Pa. v. Reimbursement Techs., Inc., No. 12–1169, 2014 WL 2738220, at *3-4 (E.D. Pa. June 17, 2014) (finding that a defendant "could not have foreseen" the particular circumstances that led to a data breach); *but see In re* Target Corp. Customer Data Sec. Breach Litigation,—F. Supp. 3d—, MDL No. 14–2522, 2014 WL 6775314, at *3-4 (D. Minn. December 2, 2014) (finding that the cyberattack against Target was foreseeable because Target had allegedly affirmatively disabled a security feature that would have prevented the attack).

[243] *See* RESTATEMENT (SECOND) OF TORTS §448 ("The act of a third person in committing an intentional tort or crime is a superseding cause of harm ... unless the actor at the time of his negligent conduct realized or should have realized the likelihood that such a situation might be created, and that a third person might avail himself of the opportunity to commit such a tort or crime.").

[244] *See* Michael L. Rustad & Thomas H. Koenig, *Extending Learned Hand's Negligence Formula to Information Security Breaches,* 3 ISJLP 237, 251 (2007); *see also* Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime,* 20 BERKELEY TECH. L.J. 1553, 1553 (2005) ("Any duty to protect computer users from the cybercrimes of third persons must be predicated on a preventable risk.").

[245] *See* John A. Fisher, *Secure My Data or Pay the Price: Consumer Remedy for Negligent Enablement of Data Breach,* 4 WM. & MARY BUS. L. REV. 215, 230 (2013).

[246] *See* Palmer, *supra* note 72, at 323 (arguing that tort law creates an "incentive to not meaningfully participate in information sharing by simply staying in the dark and not expose itself to potential liability.").

cyberattack,[247] most of the cost of a cyberattack will be borne by the company attacked and will not result in actual losses for potential plaintiffs in a tort lawsuit, like a customer.[248] And courts have been loath to allow a lawsuit to proceed based on the potential for future injury resulting from a cyberattack.[249] Second, and perhaps most importantly, the economic loss doctrine—which prohibits parties from recovering financial losses, absent injury to person or property, under tort law[250]—often prevents recovery in a lawsuit respecting a cyberattack because "[m]any of the harms that would result from a cyber-attack on, say, the power grid or the financial sector would be purely economic in nature."[251] And indeed, in recent tort lawsuits regarding cyberattacks, courts have dismissed tort claims at early stages of the litigation because of the economic loss doctrine.[252] In short, the litigation risks posed by tort lawsuits respecting a cyberattack may be fairly minimal regardless of whether an entity is involved in cybersecurity sharing.[253]

---

[247] *See, e.g.,* PRICEWATERHOUSE COOPERS, *supra* note 13, at 10 (noting that the "annual estimated reported average financial loss attributed to cybersecurity incidents was $2.7 million, a jump of 34% over 2013.").

[248] *See* Jacob W. Schneider, Note, *Preventing Data Breaches: Alternative Approaches to Deter Negligent Handling of Consumer Data,* 15 B.U. J. SCI. & TECH. L. 279, 281-82 (2009) ("When an individual's personal information is stolen, there is no guarantee that it will be used fraudulently. In fact, only 2% of stolen credit card information from data breaches is subject to misuse. Of all identity theft reports, only 1.5 to 4% are the result of stolen credit card information. This probability goes down even further when the volume of personal information is large—since identity thieves can only make use of a small number of accounts.").

[249] *See* Randolph v. ING Life Ins. & Annuity Co., 973 A.2d 702, 708 n.9 (D.C. 2009) (collecting cases where courts "have dismissed similar negligence actions for failure to state a claim, or have entered summary judgment for defendants, in the absence of allegations of present injury to plaintiffs.").

[250] *See* Nat'l Research Council, *supra* note 239, at 50.

[251] *See* Sales, *supra* note 26, at 1535.

[252] *See, e.g., In re* Target Corp. Data Sec. Breach Litigation,—F. Supp. 3d.—, MDL No. 14–2522, 2014 WL 7192478, at * 20 (dismissing several tort claims related to Target's 2013 data breach under the economic loss doctrine); *see also In re* TJX Cos. Retail Sec. Breach Litig., 564 F.3d 489, 498 (1st Cir. 2009) ("AmeriFirst says that it did suffer property damage because it had a property interest in the payment card information, which the security breach rendered worthless. Electronic data can have value and the value can be lost, but the loss here is not a result of physical destruction of property."); Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club, Inc., 918 N.E. 2d 36, 39, 49-51 (Mass. 2009) ("[T]he plaintiffs suffered only economic harm due to the theft of the credit card account information ... the economic loss doctrine barred recovery on their negligence claims.").

[253] The Bipartisan Policy Center has hypothesized that "domain names and companies who host websites" that may be the subject of cyber-threat information may sue "entities that collect and aggregate cyber-threat information," like ISACs, regarding the "accuracy of their data," potentially chilling cyber-information sharing. *See* Bipartisan Policy Center, *supra* note 30, at 9-10. Presumably such a lawsuit would be based on a defamation claim—that is, an allegation that a defendant negligently published an unprivileged, false, and defamatory statement to a third party. *See* RESTATEMENT (SECOND) OF TORTS §558. The study from the Bipartisan Policy Center does not cite to any lawsuits that have been filed against a cyber-information sharing organization or any other accounts of such an organization being threatened with a lawsuit for the publication of cyber-threat information, making it difficult to assess whether such lawsuits have actually chilled information sharing efforts. *See* Bipartisan Policy Center, *supra* note 30, at 9-10. Nonetheless, Congress, in the Communications Decency Act (CDA), has already provided immunity to defamation lawsuits directed at services that provide information to multiple users by giving them access to a computer server. *See* 47 U.S.C. §230(c)(1). Courts interpreting the CDA have generally agreed that the Act immunizes online information hosts from liability for defamatory material posted through their services by third parties. *See, e.g.,* Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997); Green v. America Online, 318 F.3d 465, 471 (3d Cir. 2003); Universal Communications Systems, Inc. v. Lycos, Inc., 478 F.3d 413, 422 (1st Cir. 2007); Doe v. MySpace, Inc., 528 F.3d 413, 420 (5th Cir. 2008); Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1170-71 (9th Cir. 2008); Klayman v. Zuckerberg, 753 F.3d 1354, 1359 (D.C. Cir. 2014). So long as a cyber-information sharing service is not "creating or developing" cyber-threat information and sharing it with other entities, *see Fair Hous. Council of San Fernando Valley,* 489 F.3d at 925, it appears the CDA likely shields such entities from any defamation lawsuits that could potentially chill broader cyber-information sharing efforts.

Other Sources of Liability

Beyond privacy, antitrust, and negligent tort law, several other laws could be the source of liability concerns for private entities that choose to share cyber-information with each other. For example, the 2013 Target data breach incident led to a shareholder derivative suit against Target's officers and board of directors, that alleged that those actors violated fiduciary obligations of trust, loyalty, good faith, and due care by failing to take adequate steps to prevent the cyberattack and by making inaccurate disclosures to their shareholders about the extent of the damage from the attack.[254] Shared cyber-information could be critical evidence in a similar suit. If, for example, a company that suffered a data breach like Target shared cyber-threat information with an ISAC prior to the attack, one could imagine such evidence being used in a similar shareholder lawsuit to establish that the company's officers had specific knowledge about the company's cyber-vulnerabilities or the extent of a cyber-attack on a given day.

And a shareholder derivative lawsuit is only one genre of litigation that could both result from a cyberattack *and* be aided by shared cyber-information.[255] For example, institutional customers who sue a bank in the wake of a cyberattack that has resulted in fraudulent wire transfers could be helped by evidence that a bank knew about particular risks posed by a cyberattack. The general framework governing the rights and obligations between a bank and customers respecting fraudulent wire transfers is found in Article 4A of the Uniform Commercial Code (UCC).[256] Article 4A generally requires banks to bear the risk if a third party steals a customer's identity, resulting in a fraudulent wire transfer.[257] Nonetheless, the UCC contains an exception whereby a customer will bear the risk of a fraudulent payment order if: (1) a bank and its customer agree to implement a security procedure designed to protect against fraud; (2) the security procedure that is implemented is a "commercially reasonable" method of providing security against unauthorized payment orders; and (3) the bank demonstrates that it accepted the payment order in good faith and in compliance with the security procedure.[258] While the question of whether a particular security procedure can be deemed "commercially reasonable" will likely depend on the specific facts surrounding a cyberattack and the procedures a bank had in place to prevent such a fraudulent transfer,[259] one critical factor may be a bank's prior awareness of the risks posed by a cyberattack.[260] In this vein, knowledge that a bank knew about a cybersecurity risk because of shared cyber intelligence could implicate that bank's liability with regard to a suit under the UCC.

---

[254] *See* Collier v. Steinhafel, No. 14-cv-266, Docket #1, Compl. (D. Minn. January 29, 2014).

[255] Even in the context of securities litigation, in addition to state common law breach of fiduciary duty claims, federal law allows a private actor to sue as a result of a material misstatement or omission in connection with the purchase or sale of any security, *see* Halliburton Co. v. Erica P. John Fund, Inc., 134 S. Ct. 2398, 2407 (2014), which could plausibly include a claim for failing to disclose cybersecurity risks to investors or federal regulators, *see infra* notes 310-314 and accompanying text.

[256] *See* U.C.C. §4A *et seq*.

[257] Choice Escrow & Land Title, LLC v. BancorpSouth Bank, 754 F.3d 611, 616 (8th Cir. 2014).

[258] *Id.*

[259] *Compare id.* at 622 (concluding that a bank's security procedures, which included password protection, daily transfer limits, device authentication, and dual control, were "commercially reasonable") *with* Patco Constr. Co. v. People's United Bank, 684 F.3d 197, 212 (1st Cir. 2012) (concluding that a "one-size-fits-all" security procedure that provided the same security to all wire transfers regardless of size was commercially reasonable).

[260] *Compare Choice Escrow,* 754 F.3d at 620 (holding that where a bank was aware of a new cyber-threat, offered its customer an updated security procedure to combat the new cyber-threat, and the customer declined to utilize the new security procedure, the bank acted in a commercially reasonable way) *with Patco Constr. Co.,* 684 F.3d at 213 (concluding that a bank's failure to implement additional security procedures was "especially unreasonable in light of the bank's knowledge of ongoing fraud.").

More broadly, there are "a myriad of legal theories, including ... breach of express or implied contract, state deceptive trade practices act violations or state data breach notification violations" that could be the basis for a lawsuit against an entity that suffered a data breach.[261] Shared cyber-information could be critical evidence that helps prove, for example, the timing of when a cyberattack occurred or the company's knowledge of the attack and the sufficiency of the company's cyber-defenses at the time of the breach,[262] which could result in private entities being less likely to share cyber-intelligence with any other entity or organization.

Sharing Cyber -Information with the Government

Just as private entities are increasingly recognizing the need to access cyber-intelligence gathered by their peers,[263] the federal government may need access to cyber-threat information in the possession of the private sector in order to make informed decisions about the government's and the nation's cybersecurity needs. As Lisa Monaco, the President's Homeland Security Advisor, recently noted, the "private sector has vital information we don't always see unless they share it with us."[264] Nonetheless, obtaining cyber-intelligence from the private sector can be difficult for the federal government. Putting aside the difficult issues that may arise when a private party affirmatively *refuses* to divulge cyber-intelligence within its possession to the federal government and the government is forced to obtain, for example, a warrant or a subpoena to access such information,[265] the federal government may not know that a private entity possesses certain cyber-intelligence, and the only way the government can learn about a potential cyber-threat is by having the private party voluntarily share that information with the government. The voluntary disclosure of cyber-intelligence to the government may, however, be something private parties are reluctant to do because of various legal concerns.

Before discussing those legal concerns, it is important to note from the onset that the government, and specifically DHS, has ample legal authority to *receive* voluntarily[266] shared cyber-information. For example, under Section 201 of the Homeland Security Act, the I&A is authorized to "receive ... information ... [from] private sector entities ... in support of the mission responsibilities of" DHS.[267] Moreover, the NCPA provided explicit statutory authority for the NCCIC to serve as an "interface for the *multi-directional* ... sharing of information related to cybersecurity risks, incidents, analysis, and warnings.... "[268] More broadly, the Critical

[261] *See* Peretti, *supra* note 32, at 6.

[262] *Id.*

[263] *See supra* note 93 and accompanying text.

[264] See Lisa O. Monaco, Remarks as Prepared for Delivery by Assistant to the President for Homeland Security and Counterterrorism Lisa O. Monaco Strengthening our Nation's Cyber Defenses, (February 11, 2015), available at http://www.whitehouse.gov/the-press-office/2015/02/11/remarks-prepared-delivery-assistant-president-homeland-security-and-coun.

[265] These legal issues related to compelled disclosures of cyber-intelligence are beyond the scope of this report. For background on the various methods the government could use to compel a private actor to disclose cyber-intelligence, *see* CRS Report 95-1135, *The Federal Grand Jury*, by (name redacted); *see also* CRS Report R41733, *Privacy: An Overview of the Electronic Communications Privacy Act*, by (name redacted); CRS Report RL33320, *National Security Letters in Foreign Intelligence Investigations: Legal Background*, by (name redacted).

[266] The Critical Infrastructure Information Act of 2002 defines the term "voluntary"—in the context of cyber information sharing—as the "submittal of critical infrastructure information to a covered Federal agency

[267] *See* 6 U.S.C. §121(d)(1).

[268] *See* 6 U.S.C. §148(c)(1).

Infrastructure Information Act (CIIA), a subtitle within the Homeland Security Act, has extensive provisions regarding the treatment of "critical infrastructure information" that is "voluntarily submitted to a ... federal agency",[269] reflecting an assumption that the federal government is not precluded from receiving from a private entity voluntarily shared information pertaining to critical infrastructure.[270]

Freedom of Information Act Disclosures

One central concern for those private entities that may wish to share cyber-intelligence with the government is that the information shared, which may include proprietary information or even simply embarrassing material,[271] could be disclosed through the Freedom of Information Act (FOIA), whether through an affirmative agency disclosure or through a public request.[272] FOIA generally provides that government agencies "shall make available to the public" certain agency records, except insofar as the records are protected from disclosure under several exemptions to the Act.[273] Congress, in the CIIA, provided an exemption to FOIA for any "critical infrastructure information" (CII)[274] that is "voluntarily submitted" to DHS[275] for use by that agency regarding the "security of critical infrastructure" and related purposes.[276] In turn, DHS, through administrative regulations, has created the Protected Critical Infrastructure Information (PCII) Program to ensure that information that is voluntarily shared with the agency receives the protections created by the CIIA.[277]

For those private entities concerned that cyber-intelligence shared with the government will be indiscriminately disseminated through a FOIA request, there are three central concerns with the state of the current law with respect to FOIA and cyber-information sharing. First, the FOIA exemption contained in the CIIA is limited to information that relates to "critical

[269] *See* 6 U.S.C. §133.

[270] *See* Broggi, *supra* note 31, at 658-59.

[271] For example, if a successful cyberattack obtained trade secret information from a company, and that company wanted to disclose details about the cyberattack to the government, the cyber-information disclosed could include details and descriptions about the "type and value of compromised data." *See* Emily Frye, *The Tragedy of the Cybercommons: Overcoming Fundamental Vulnerabilities to Critical Infrastructures in a Networked World,* 58 BUSLAW 349, 375 (2002).

[272] *See* Bipartisan Policy Center, *supra* note 30, at 6; *see also see* Zheng and Lewis, *supra* note 32, at 5 (Risk of public disclosure of information shared with the government and potential use of the information in regulatory actions ahve a chilling effect on voluntary cyber threat information sharing.").

[273] *See* 5 U.S.C. §552(a).

[274] CII is statutory defined as "information not customarily in the public domain and related to the security of critical infrastructure or protected systems," including information about (1) actual or potential conduct that would be illegal or harm interstate commerce or threaten public health or safety; (2) vulnerabilities that would prevent the ability to resist such conduct; or (3) any strategies to better protect critical infrastructure systems from such conduct. 6 U.S.C. §131(3).

[275] The CIIA uses the phrase "covered Federal agency" as the entity to whom voluntarily shared CII can be submitted in order to receive protections under Section 214. *See* 6 U.S.C. §133(a). Nonetheless, the CIIA defines the phrase "covered Federal agency" to mean DHS. *See id.* §131(2).

[276] *See* 6 U.S.C. §133(a)(1)(A) ("[C]ritical infrastructure information ... that is voluntarily submitted to a covered agency for use by that agency regarding eh security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other information purpose, when accompanied by an express statement ... shall be exempted from disclosure ... under section 552 of title 5, United States Code.... "). The CIIA also exempts CII from state or local laws requiring the disclosure of information or records. *See id.* §133(a)(1)(E)(i).

[277] *See* 6 C.F.R. part 29.

infrastructure,"[278] a term that is confined to only those "systems and assets" that are "vital" to the United States and whose "incapacity or destruction" would have some sort of "debilitating impact" on the country.[279] In other words, unless a private entity is involved with the "backbone of our nation's economy, security and health,"[280] any cyber-information a private entity shares with the federal government would not fall under the FOIA exemption provided in the CIIA.

Second, even if an entity sharing information with DHS is involved with "critical infrastructure," the potential exists that not all cyber-information falls within the CIIA's protections. Instead, only "critical infrastructure information" is exempt from FOIA,[281] a phrase that, while fairly broad in scope, is not limitless.[282] For example, the Homeland Security Act facially limits CII to "information related to the *security* of critical infrastructure,"[283] which could arguably exclude information pertaining to a cyberattack that is not intended to disable or destroy a critical infrastructure system, such as an attack aiming to commit economic espionage.[284] Accordingly, private actors may question whether particular threat information falls within the CIIA's definition for CII, arguably creating legal uncertainty to those who wish to share cyber-information with the federal government.[285]

Finally, the PCII program created by DHS has a host of various procedural rules that a private entity must follow to ensure that the information provided to DHS receives protections under the CIIA. For example, any CII, to avoid being disclosed under FOIA, will need to be submitted to DHS's PCII Program Manager and will need to contain several certifications and disclaimers,[286] even if the information has been already submitted to another DHS entity, like the NCCIC. As one commentator has noted, the PCII Program's procedural restrictions "necessarily add an extra layer of process that may be sufficient to ultimately defeat the purpose of near real-time information sharing,"[287] if the restrictions do not defeat cyber-information sharing efforts entirely.[288]

It should be noted, however, that just because cyber-intelligence that is provided to DHS may be excluded from the *CIAA's* FOIA exemption that does not necessarily mean that the information will necessarily be disclosed to the public. Indeed, FOIA contains several broad exemptions that may prevent the release of shared cyber-intelligence even if the information does not fall within

[278] 6 U.S.C. §133(a)(1)(A).

[279] 6 U.S.C. §101(4) (citing 42 U.S.C. §5195c(e)).

[280] *See* Dep't of Homeland Sec., *What is Critical Infrastructure,* (November 1, 2013), *available at* http://www.dhs.gov/what-critical-infrastructure; *cf.* Remijas v. Neiman Marcus Group, LLC, No. 14-C-1735, 2014 WL 4627893, at *2 (N.D. Ill. September 16, 2014) (noting that "cyber-attack/credit card cases" do not "implicate ... questions of national security.")

[281] 6 U.S.C. §133(a)(1)(A).

[282] *See supra* note 274.

[283] 6 U.S.C. §131(3).

[284] *See generally* Kenneth Einar Himma, *Legal, Social, and Ethical Issues of the Internet, in* 1 HANDBOOK OF INFORMATION SECURITY 247, 259-60 (Hossein Bidgoli, ed., 2006) (discussing the difficulty with ascribing meaning to the term "security" in the context of computer security).

[285] *See* Peretti, *supra* note 32, at 5.

[286] *See* 6 C.F.R. §29.6(a)(1); *see also id.* §29.6(a)(3)-(4).

[287] *See* Peretti, *supra* note 32, at 6.

[288] For general criticism of the PCII program, *see* Zheng and Lewis, *supra* note 32, at 5-6.

DHS's definition of PCII.[289] For example, FOIA does not apply to material that involves "trade secrets" or otherwise "privileged or confidential" "commercial or financial information."[290] Nonetheless, without a broader exemption for cyber-information shared with the government, an argument can be made that private cyber-threat information that could contain sensitive material may be disclosed more broadly through FOIA.

Intellectual Property Concerns

Related to the concern about cyber-information sharing and FOIA is the more general concern that cyber-intelligence, once shared with the government, could waive all intellectual property rights associated with such information.[291] The primary body of intellectual property law that could be implicated by cyber-intelligence sharing is trade secret law. The law of trade secrets, which aims to encourage companies and individuals to invest in collecting information that could help secure competitive advantages in the marketplace, protects against the disclosures of "any formula, pattern, device, or compilation of information which is used in one's business and which gives [that business] an opportunity to obtain an advantage over competitors who do not know or use it."[292] Put another way, information is protected as a trade secret to the extent that information (1) has independent value because the information is not generally known and (2) is the subject of efforts to maintain its secrecy.[293] If any person or entity attempts to misappropriate a trade secret, a court can issue injunctive relief or monetary damages against such a defendant.[294]

A private entity, by sharing cyber-intelligence with the government, could risk losing trade secret protection for any valued information that is associated with the cyber-intelligence. For example, when a company shares information about a particular cyber-incident with the government, that entity may be divulging information about internal business operations or disclosing details about the underlying proprietary data that may have been stolen during the course of a cyberattack.[295] The failure to take reasonable steps to prevent gratuitous disclosures of trade secret information forfeits any protection afforded under the law,[296] and the voluntary disclosure of information to a third party generally erodes any trade secret protection for that information.[297]

While the disclosure of cyber-threat information in an unprotected forum—whether public or private—likely risks trade secret protections for that information, in the context of a private entity sharing cyber-intelligence with another party, contractual terms can be negotiated between the parties to provide protections for the intellectual property rights associated with shared cyber-intelligence.[298] With respect to sharing cyber-intelligence with the federal government, some have

[289] *See* 6 C.F.R. §29.3(a) ("Information that is separately exempt from public disclosure under [FOIA] ... does not lose its separate exemption from public disclosure due to the applicability of these procedures or any failure to follow them.").

[290] 5 U.S.C. §552(b)(4).

[291] *See* Miller, *supra* note 56 (noting that "companies are approaching [DHS's cyber-information sharing] programs cautiously" because of fears about loss of intellectual property rights).

[292] RESTATEMENT (FIRST) OF TORTS §757, cmt. b.

[293] *See* Unif. Trade Secrets Act §1(4).

[294] *See* Unif. Trade Secrets Act §§2-3.

[295] *See* Frye, *supra* note 271, at 375.

[296] *See* Fail-Safe, LLC v. A.O. Smith Corp., 674 F.3d 889, 893 (7th Cir. 2012).

[297] *Id.*

[298] *See* Eric G. Orlinsky, Kathryn L. Hickey, and David T. Shafer, *Cybersecurity: A Legal Perspective,* 47-DEC MDBJ (continued...)

raised concerns about how well the agreements between the government and private entities protect trade secret information that is disclosed in the course of exchanging cyber-intelligence.[299] Specifically, according to DHS, in order to gain access to NCCIC's cyber-intelligence information, a private entity must sign a Cooperative Research and Development Agreement (CRADA) with the agency,[300] and the text of the information-sharing CRADA reportedly includes language that potentially forfeits intellectual property rights in the shared material.[301] Regardless of whether a CRADA could be altered to avoid using such language or whether such language is just the natural result of sharing cyber-information among several public and private actors, as Gregory Garcia, former Assistant Secretary of DHS for Cybersecurity, noted, the CRADAs governing cyber-information sharing "cause[] some companies a lot of heartburn and ... will prevent them from participating or if they do participate they might not do so as robustly if that intellectual property provision did not exist."[302]

Regulatory Enforcement Concerns

Perhaps the primary concern amongst private actors interested in sharing cyber-intelligence with the government is that government regulators will either be "tipped off" because of the shared information and begin an investigation or will "use shared information" as evidence in a regulatory "action against a company."[303] The fear that the government will use information that a private entity shared for cybersecurity purposes *against* that entity may be particularly pronounced if the underlying information pertains to a cyber-breach that resulted in the loss of personal or regulated data.[304]

(...continued)

32, 34 (2014) ("Due in part to the reliance on technology to share information, contractual relationships need to be built, and contractual provisions now need to be crafted, with an eye towards cybersecurity. The method and location of storage, and the means of regulating access to sensitive information are all critical to maintaining cybersecurity when multiple parties are involved in a project. To best protect the intellectual property and information of a business, as well as sensitive customer information, parties should discuss and expressly agree to contractual terms that address the nuances of information-sharing, information management, and security of data.").

[299] *See* Miller, *supra* note 56.

[300] *See* Dep't of Homeland Sec., *Critical Infrastructure and Key Resources Cyber Information Sharing and Collaboration Program,* 1, (no date given) *available at* https://www.us-cert.gov/sites/default/files/c3vp/CISCP_20140523.pdf.

[301] *See* Jenny Menna, *DHS Information Sharing Update,* contained in *Minutes of Meeting,* INFORMATION SECURITY AND PRIVACY ADVISORY BOARD, (June 12, 2013), *available at* http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2013-06/ispab_meeting-minutes_june-2013_approved.pdf ("[T] he problem with [the CRADA] is Intellectual Property, and if shared, it would be community property. It is entirely up to the signer to determine if they want their participation / information to be shared."); *see also* Miller, *supra* note 56 ("We talk about legal instruments that enable that sharing and the lawyers at DHS settle on a [CRADA], which among other things stipulates that information shared in a CRADA environment becomes in effect community property so you lose the rights to that intellectual property.") (quoting Gregory Garcia, a former DHS Assistant Secretary for Cybersecurity). For further criticism of the CRADA as a legal instrument used to facilitate cyber-information sharing, *see* Zheng and Lewis, *supra* note 32, at 5 ("The CRADA process is lengthy and resource-intensive, requiring significant involvement of companies' legal counsel.").

[302] *See also* Miller, *supra* note 56 (quoting Gregory Garcia, a former DHS Assistant Secretary for Cybersecurity).

[303] *See* Peretti, *supra* note 32, at 6; *see also* Fairborz Farahmand, et al. *Evaluating Damages Caused by Information Systems Security Incidents,* in ECONOMICS OF INFORMATION SECURITY 96 (eds. L. Jean Camp and Stephen Lewis) (2004) ("[C]ompanies are reluctant to give the government information on attacks and vulnerabilities that regulators may use against them later on.").

[304] *See* Peretti, *supra* note 32, at 6.

For example, over the past decade, the FTC, which generally is tasked under the Federal Trade Commission Act with promoting economic competition and consumer protection by eliminating acts or practices that are "unfair or deceptive,"[305] has been at the forefront of federal cybersecurity efforts. In particular, the independent agency has initiated several enforcement actions under Section 5 of the FTC Act that have resulted in tens of millions of dollars in civil penalties, more than fifty private settlements, and expensive compliance obligations for the companies investigated.[306] Some have suggested that the FTC could learn from cyber-intelligence that was shared with DHS that a company has failed to take proper cybersecurity measures, resulting in an FTC investigation of the company.[307] And, perhaps such a scenario is not purely theoretical. In 2010, a cyber-intelligence company shared information with the government that a Georgia-based medical laboratory called LabMD had allowed the billing information for nearly 9,000 patients to be accessed on a peer-to-peer network service, and, in turn, the FTC used the shared information to commence an investigation against LabMD.[308]

In addition to the FTC, the other primary federal agency often mentioned as having an interest in taking regulatory actions as a result of shared cyber-intelligence is the Securities and Exchange Commission (SEC), an independent regulatory agency authorized to administer the Securities Act of 1933 and the Securities Exchange Act of 1934.[309] The two laws are generally aimed at ensuring that investors receive adequate information about the securities being offered to the public for sale and preventing deceit, misrepresentations, and other fraud in the sale of securities.[310] In this vein, the two laws contain detailed disclosure requirements for the sale of securities to the public, including the need for companies to file initial registration statements and periodic reports with the SEC.[311]

Under SEC guidelines, corporations and attorneys are advised to report material cyber-risks and incidents to the SEC.[312] Material cyber-risks and incidents might include new expenditures on corporate cybersecurity, loss of intellectual property, or incidents that have adverse impacts on customers or clients or even that cause "reputational damage adversely affecting customer or investor confidence."[313] Because the failure to disclose material information to the SEC could

[305] *See* 15 U.S.C. §45.

[306] *See To Business' Chagrin, Cybersecurity Is FTC's Turf Now,* LAW 360, (June 10, 2014), *available at* http://www.law360.com/articles/545258/to-business-chagrin-cybersecurity-is-ftc-s-turf-now; *see also* Julie Brill, *On the Front Lines: The FTC's Role in Data Security*, Keynote Address Before the Center for Strategic and International Studies, (September 17, 2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/582841/140917csisspeech.pdf.

[307] *See* Info. Tech Industry Council, *supra* note 216, at 2 (suggesting as a "potential result" of disclosing cyber intelligence to the government, the FTC could "use[] the information submitted ... as evidence in a case against Company A for violating the security provisions of HIPAA.").

[308] *See* Eva M. Wooten and Lei Shen, *The Curious Case of LabMD: New Developments in the "Other" FTC Data-Security Case,* (August 11, 2014), *available at* http://www.mayerbrown.com/The-Curious-Case-of-LabMD-New-Developments-In-The-Other-FTC-Data-Security-Case/. For more on the LabMD litigation, *see* CRS Report R43723, *The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority*, by (name redacted).

[309] 15 U.S.C. §78d.

[310] *See* James M. Bartos, UNITED STATES SECURITIES LAW: A PRACTICAL GUIDE 2-3 (3d. ed.) (2006).

[311] 15 U.S.C. §§77g, 77j.

[312] See *Disclosure Guidance: Topic No. 2: Cybersecurity*, U.S. Sec. & Exch. Comm'n (October 13, 2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[313] *Id.*

prompt investigations led by the Commission, risking civil liability and even criminal penalties for the companies involved,[314] a fear exists that information disclosed by a company to the government as part of a cyber-information sharing arrangement, such as details about a cyber-breach, could be used as evidence to show that the company withheld material information from the SEC.[315]

Current law provides fairly limited assurances that shared cyber-intelligence will not be subsequently used by the FTC, SEC, or any other government entity that could use such disclosures in the course of a regulatory enforcement action.[316] Under the CIIA, CII disclosed to DHS cannot be used by "any other Federal, State, or local authority, or any third person, in any civil action arising under Federal or State law" if the information was submitted in "good faith."[317] Moreover, the CIIA prohibits CII from being used or disclosed by "any officer or employee of the United States for purposes other" than (1) for the "purposes [of the CIIA]"; (2) in furtherance of an investigation or the prosecution of a criminal act; or (3) when the information is disclosed to Congress, or its representatives, or the Comptroller General, or its representatives.[318] The latter provision, if violated by an officer or employee of the United States could result in criminal penalties or loss of employment.[319] Nonetheless, the CIIA's prohibitions on the collateral use of certain cyber-information suffer from many of the shortcomings of the CIIA's FOIA exemption—namely, the limited scope of the term "CII" and the potential obstacles posed by DHS's requirements under the PCII Program.[320] Moreover, phrases like "good faith" and "purposes [of the CIIA]" are not defined by the Act, and there is no case law interpreting the collateral use restrictions of the CIIA, leaving considerable ambiguity as to the scope of those provisions.[321]

Privacy Concerns

Related to the concerns from those in the private sector that the government may use (or misuse) information obtained from cyber-information sharing for a regulatory purpose are broader worries about divulging large volumes of often-sensitive cyber-intelligence to the government. These concerns may be particularly worrisome in the wake the 2013 unauthorized disclosures of classified information by Edward Snowden, a former National Security Agency (NSA) contractor, regarding the size and scope of American foreign intelligence efforts.[322] Many of these

[314] *See* Bartos, *supra* note 310, at 2-3.

[315] *See* Info. Tech Industry Council, *supra* note 216, at 3.

[316] *Id.* (fearing that "[g]overnment prosecutors, law enforcement agencies, or civil attorneys" could use cyber-intelligence "as the absis for establishing a violation of civil or criminal law" against the company that shared the information).

[317] 6 U.S.C. §133(a)(1)(C).

[318] *Id.* §133(a)(1)(D).

[319] *Id.* §133(f).

[320] *See supra* "Freedom of Information Act Disclosures," pp. 33-35.

[321] *See* 6 U.S.C. §133(a)(1)(C)-(D). The phrase "good faith" is a notoriously "elusive" concept, *see generally* Roger Brownsword et al., "Good Faith in Contract," in GOOD FAITH IN CONTRACT: CONCEPT AND CONTEXT 1 (Roger Brownsword ed., 1999), and it may be equally elusive to divine the general purposes of a law and whether those purposes fit with the particular collateral use in question, *see generally* Davis County Solid Waste Mgmt. v. United States EPA, 101 F.3d 1395, 1409 (D.C. Cir. 1996) ("[I]t is often difficult to determine whether an interpretation of a statute frustrates or advances congressional purposes.").

[322] *See generally* Geoff Dyer and Hannah Kuchler, *Barack Obama's cyber security push spurs privacy fears*, FINANCIAL TIMES, (February 12, 2015), http://www.ft.com/cms/s/0/64842466-b2b2-11e4-a058-
(continued...)

disclosures revealed that the government had access to wide swaths of information about the customers of several technology giants, harming those firms' relationships with their customers and reportedly harming the firms' bottom lines.[323] As a result, in the words of one commentator, the "big consequence of Edward Snowden's NSA leaks" may be that companies that would have otherwise been interested in sharing cyber-intelligence with the government "will be extremely wary of anything that has the words 'government' and 'information sharing' so close together."[324]

While most of privacy concerns from the private sector regarding sharing cyber-information with the government are non-legal in nature—that is, the debates center on whether information sharing *should* occur given the concerns for personal privacy, not on whether information sharing with the government *can* occur as a result of current federal privacy laws—some have voiced concerns over whether the Stored Communications Act allows for private entities to voluntarily share certain cyber-information with the government.[325] The SCA was discussed earlier in this report in the context of a service provider disclosing the *contents* of electronic communications to another private entity for cybersecurity purposes.[326] While the content based restrictions contained in Section 2702(a)(1)-(2) apply equally to electronic communications that are shared with the government and, therefore, raise similar legal issues to those discussed above,[327] the SCA also contains a provision explicitly regulating the dissemination of *non-content* information to governmental entities.[328]

Specifically, under 18 U.S.C. Section 2702(a)(3), providers of a RCS or an ECS to the public[329] are generally prohibited from "knowingly divulging a record or other information pertaining to a

(...continued)

00144feab7de.html#axzz3T8sCV7hl.

[323] *See* Mark D. Young, *National Insecurity: The Impacts of Illegal Disclosures of Classified Information,* 10 ISJLP 367, 402 (2014) ("Snowden's disclosure of classified information has not only chilled the relationship between Silicon Valley and the U.S. government, but also it has damaged the bottom line for American technology firms ... [R]ecent losses for Google, Cisco, and AT&T can be attributed to the alleged role of American technology companies in the Snowden scandal.").

[324] *See* Gyenes, *supra* note 56, at 304; *see also* Young, *supra* note 323, at 402 ("With their bottom lines at risk, it is understandable that American technology companies would distance themselves from the U.S. government.").

[325] *See* David Inserra and Paul Rosenzweig, *Cybersecurity Information Sharing: One Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace,* HERITAGE FOUNDATION, (April 1, 2014), *available at* http://www.heritage.org/research/reports/2014/04/cybersecurity-information-sharing-one-step-toward-us-security-prosperity-and-freedom-in-cyberspace#_ftnref17 ("[T]he Stored Communication Act seem[s] to prohibit or potentially prohibit the sharing of cybersecurity information."); *see also* Burstein, *supra* note 134, at 189-90.

[326] *See supra "*The Stored Communications Act," at pp. 18-21.

[327] *See* 18 U.S.C. §2702(a)(3) (excluding from the prohibition on the disclosure of non-content information to a governmental entity "the contents of communication covered by paragraph (1) or (2)). There are specific exceptions to the prohibitions contained in 18 U.S.C. §§2702(a)(1)-(2) based on if the disclosure is made to a governmental entity. For example, the contents of communication can be disclosed: (1) to a law enforcement agency if the contents were inadvertently obtained by the service provider and appear to relate to the commission to a crime, *id.* §2702(b)(7); (2) to a governmental entity if the provider in good faith believes that "that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency," *id.* §2702(b)(8); (3) pursuant to a warrant if procedures outlined in 18 U.S.C. §2703 are followed, *id.* §§2702(b)(2); and (4) as required by certain provisions of the Foreign Intelligence Surveillance Act of 1978, *see id.* §§2702(b)(2), 2511(2)(a).

[328] *See id.* §2702(a)(3); *see also id.* §2510(6) (defining the term "person" to include "any employee or agent of the United States or any State or political subdivision thereof.... ").

[329] Unlike 18 U.S.C. §2702(a)(1), §2702(a)(3) is not limited to disclosures made by an ECS when the underlying communications are held *in storage*, meaning that the prohibition on disclosing non-content information to the government generally applies to all providers of ECS to the public, which is defined broadly as "any service which (continued...)

subscriber or customer of such service ... to any governmental entity."[330] The SCA provides no definition for what "record[s] or other information pertaining to a subscriber or customer" entail,[331] leading to some dispute about the scope of the SCA's prohibition on non-content information. Courts have interpreted "record information" to have a broad import that at the very least includes information like a subscriber's name, identity, address, and communication records, and *may* include broader information that merely relates to a customer or subscriber.[332] The DOJ has issued a White Paper that attempts to cabin the type of "record information" falling within Section 2702(a)(3)'s prohibition to information that "can identify or otherwise provide information about any particular subscriber or customer."[333] In other words, in the view of the Justice Department, private entities can divulge to the government information like the "characteristics of a computer virus or malicious cyber tool" or aggregate information about Internet traffic patterns without running afoul of 18 U.S.C. Section 2702(a)(3).[334] Putting aside the merits of DOJ's position[335]—one commentator has suggested that the SCA's prohibitions on the disclosure of electronic communications to the government "could be and is being construed by many to include the coding of viruses and malware and the IP addresses from which cyber attacks are originating"[336]—the fact that a dispute remains over the scope of the SCA's prohibition on disclosures to the government arguably indicates there is considerable uncertainty

(...continued)

provides to users ... the ability to send or receive ... electronic communications," *see* 18 U.S.C. §2510(15).

[330] *Id.* §2702(a)(3).

[331] *See In re* United States ex rel. an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 573 (D. Md. 2011) ("The statute offers no definition nor explanation of what constitutes 'records' or 'information pertaining to a subscriber.'").

[332] *See In re* United States for an Order Directing Provider of Elec. Commun. Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010) (noting the breadth of the term "record or other information pertaining to a subscriber or customer"); *see also In re Zynga Privacy Litig.*, 750 F.3d at 1104 ("Although there is no specific statutory definition for "record," the Stored Communications Act provides examples of record information ... includ[ing] among other things, the 'name,' 'address,' and 'subscriber number or identity' of 'a subscriber to or customer of such service,' but not 'the contents of communications.'"); *see also* Telecomms. Regulatory Bd. v. CTIA, 752 F.3d 60, 68 (1st Cir. 2014) ("[T]he SCA clearly prohibits communications providers from disclosing to the government basic subscriber information—including a customer's name, address, and telephone number—without a subpoena.").

[333] *See* Dep't of Justice, *Sharing Cyberthreat Information Under 18 U.S.C. §2702(a)(3)*, (May 9, 2014), at pg. 3, *available at* http://www.justice.gov/criminal/cybercrime/docs/guidance-for-ecpa-issue-5-9-2014.pdf (hereinafter "DOJ White Paper").

[334] *Id.*

[335] A detailed examination of the merits of the DOJ's interpretation of 18 U.S.C. §2702(a)(3) are beyond the scope of this report. Nonetheless, the DOJ White Paper notes several strong arguments for why the SCA should not bar the government from receiving information that does not identify specific customers or subscribers, including the general purposes of the Act to provide privacy protections for information about individuals that are in the hands of third-party service providers. *See id.* at 4-5. On the other hand, the text of the SCA, while using the article "a" in the phrase "record or other information pertaining to a subscriber ... or customer," *see id.* at 4 (arguing that the use of the singular noun implied Congress was concerned with information as it pertained to a specific identifiable customer), uses the phrase "pertaining to," which has generally been interpreted has having a *very* broad meaning and being synonymous with the phrase "relates to." *See, e.g.,* James Madison Project v. CIA, No. 8-cv-1323, 2009 WL 2777961, at *4 (E.D. Va. August 31, 2009) (noting the breadth of the phrase "pertaining to"). Moreover, the fact that Congress has in other privacy laws explicitly exempted information that does not pertain to a particular individual, *see, e.g.,* 47 U.S.C. §222(c)(3); 47 U.S.C. §551(a)(2)(A), indicates that Congress was interested in protecting a broader set of information than just personally identifiable information with the SCA. *See supra* "Other Federal and State Privacy Laws," at pp. 23-26; *see generally In re* Haas, 48 F.3d 1153, 1156 (11th Cir. 1995) ("Where Congress knows how to say something but chooses not to, its silence is controlling.") (citing Bfp v. Resolution Trust Corp., 511 U.S. 531, 554 (1994)).

[336] *See* Inserra and Rosenzweig, *supra* note 325.

as to whether federal privacy law generally prohibits many forms of cyber-intelligence sharing with the government.[337]

Like its general prohibitions pertaining to the disclosures made by providers of ECS or RCS to other private entities, the SCA's prohibition respecting disclosures made by service providers to the government has several exceptions,[338] which arguably do little to clarify the legal landscape for those interested in sharing cyber-information with the government. For example, the SCA contains a provider exception and a consent exception for disclosures made by a service provider to the government.[339] As noted above, the SCA's provider exception may only extend to allow for the disclosure of information that is directly related to protecting the rights or property of the *provider*, as opposed to third parties' interests.[340] And the scope of the consent exception will often be tied to the specific facts respecting a particular customer's agreement to allow the service provider to submit cyber-intelligence to the government.[341]

The SCA does contain a third exception specific to disclosures to the government: the Act allows disclosures of content and non-content information to be made by a provider if the provider believes in "good faith" that an "emergency involving danger of death or serious physical injury to any person requires disclosure without delay" of the communications or information "relating to the emergency."[342] The SCA's "exigent circumstances" exception, however, is an exception that has been read narrowly to allow the government to access information necessary to "prevent or minimize" a true, active emergency and extends no further.[343] It is unclear whether many types of cyber-information in the hands of the private sector would reveal information that would help alleviate an active emergency situation so that the intelligence could be disclosed to the government under the SCA's exigent circumstances exception. More broadly, given the ambiguities associated with the SCA's general prohibition on voluntary disclosures to the government with regard to electronic communications and the exceptions to that prohibition, much like other areas of law regarding cyber-information sharing, federal privacy law as it pertains to the dissemination of cyber-intelligence from the private sector to the federal

[337] As the DOJ notes in its White Paper, "determining when data does or does not pertain to a subscriber or customer will be a highly fact-specific inquiry," leaving considerable uncertain with respect to the scope of the SCA even if the DOJ's more narrow interpretation of §2702(a)(3) governed. *See* DOJ White Paper, *supra* note 333, at 7. It is also important to note that the Department of Justice does not enforce §2702 of the SCA, as that section is only enforceable through a private right of action. *See* 18 U.S.C. §2707. In other words, DOJ's position as staked out in the White Paper does nothing to prevent a private actor from suing a service provider for violating §2702(a)(3) by disseminating aggregate cyber-information to the government, and the DOJ's White Paper will receive no deference from a court resolving such litigation. *See* Fed. Labor Relations Auth. v. United States Dep't of Treasury, 884 F.2d 1446, 1451 (D.C. Cir. 1989) (holding that *Chevron* deference should not be afforded to an agency who has no special duty to interpret a particular statute).

[338] *See* 18 U.S.C. §2702(b)-(c).

[339] *See id.* §2702(b)(2)&(5) (provider exception with respect to the contents of communication); *id.* §2702(b)(3) (consent exception with respect to the contents of communication); *id.* §2702(c)(3) (provider exception with respect to non-content information); *id.* §2702(c)(2) (consent exception with respect to non-content information).

[340] *See supra* notes 166-167 and accompanying text.

[341] *See supra* notes 164-165 and accompanying text.

[342] *See* 18 U.S.C. §2702(b)(8), (c)(4).

[343] *See* United States v. Caraballo, 963 F. Supp. 2d 341, 361 (D. Vt. 2013); *see also* United States v. Tsarnaev,—F. Supp. 3d.—, No. 13-CR-10200, 2014 WL 5308087, at *8-9 n.2 (D. Mass. October 17, 2014) (finding that the exigent circumstnaces exception to the SCA allowed the government to access an "at large" suspect's emails from Yahoo!); *see generally* United States v. Crouch, 666 F. Supp. 1414, 1416 (N.D. Cal. 1987) (holding that ECPA's emergency authorizations should be read narrowly).

government raises many questions and has few clear answers. http://www.lexis.com/research/xlink?app=00075&view=full&searchtype=get&search=750+F.3d+1098%2520at%25201104

Legislative Options for Cyber-Information Sharing

Given the two major categories of cyber-information sharing—sharing of information in the possession of the government and sharing of information in the possession of the private sector—and the myriad of legal issues arising with respect to each category, legislative changes to federal law that aims to encourage the dissemination of cybersecurity information among the public and private sectors could take countless forms. Indeed, during the 113th and 114th Congresses, several legislative proposals have been introduced that aim to remove the current legal obstacles that may be preventing more robust cyber-intelligence sharing, whether by removing discrete legal barriers to information sharing[344] or by effectuating more wholesale change with regard to the distribution of cyber-intelligence within the public and private sectors.[345] While any one of the various legislative proposals on cybersecurity information sharing could merit a lengthy discussion, six themes permeate the various proposals aimed at promoting cybersecurity information sharing—one overarching theme, two that pertain to cyber-information possessed by the government, and three that pertain to cyber-information in the control of the private sector.

Creating a Broader Legal Framework for the Sharing of Cyber-Information

A central difficulty with the current law on cyber-security information is simply that there is very little federal law on the subject. The only federal law that directly contemplates the concept of the federal government and private entities sharing cyber-intelligence with each other is the Homeland Security Act,[346] and that law, by its very terms, is generally limited to the sharing of cybersecurity information as it pertains to critical infrastructure systems.[347] As a result of the lack of any federal framework to guide public and private entities interested in sharing cyber-intelligence, the law must be guided by several disparate areas of law whose guiding principles may be antithetical to the widespread dissemination of cyber-intelligence.[348]

---

[344] *See, e.g.,* National Cybersecurity and Critical Infrastructure Protection Act of 2014, H.R. 3696, 113th Cong. §103 (establishing a framework for sharing information with at least 16 different industry specific ISACs); Cyber Economic Espionage Accountability Act, S. 111, 113th Cong. §3 (requiring the disclosure by the federal government to the public a "list of persons" responsible for cyber-economic espionage); Cybersecurity Public Awareness Act of 2013, S. 1638, 113th Cong. §3 (requiring several reports listing major cyber incidents involving executive agencies); Cyber Information Sharing Tax Credit Act, S. 2717, 113th Cong. §2 (allowing for tax credits for certain expenses incurred for sharing cyber-intelligence).

[345] *See, e.g.,* Cyber Intelligence Sharing and Protection Act, H.R. 3523, 112th Cong, H.R. 624, 113th Cong, H.R. 234, 114th Cong. (hereinafter "CISPA") (all other references to CISPA will be references to H.R. 234 in the 114th Cong.); Cyber Threat Sharing Act of 2015, S. 456, 114th Cong. (herein "CTSA"); Cybersecurity Information Sharing Act of 2014 , S. 2588, 113th Cong. (hereinafter "CISA"). All references to CISA in this report refer to the 2014 version of the bill. As of publication, the Senate was beginning deliberations on a 2015 version of the bill. *See Discussion Draft—*Cybersecurity Information Sharing Act of 2015, S. ____, 114th Cong., *available at* http://www.burr.senate.gov/public/_files/CISA%202015%20Discussion%20Draft.pdf.

[346] 6 U.S.C. §§101 *et seq.*

[347] *See id.* §§121, 143.

[348] *See generally supra* "Sharing Cyber-Information in the Possession of the Government" and "Sharing Cyber-
(continued...)

To provide clarity to an area of law much in need of clarification, several proposals begin by squarely authorizing some degree of sharing of cyber-intelligence between the public sector and the private sector and between private entities. For example, the Cyber Intelligence Sharing and Protection Act (CISPA), a bill that has passed the House of Representatives the past two Congresses, would explicitly authorize (1) the federal government to "facilitate information sharing, interaction, and collaboration" between the federal government and the private sector,[349] and (2) private sector cybersecurity providers and entities that protect their own information networks to "share cyber threat information with any other entity" of their choosing, including certain entities within the federal government.[350] Similarly, the Cyber Threat Sharing Act of 2015 (CTSA) would allow (1) the NCCIC to "receive and disclose cyber threat indicators" to the rest of the federal government and the private sector,[351] and (2) private entities to share "cyber threat indicators" with certain private sector organizations and the NCCIC.[352]

Having created a general framework that contemplates broader cybersecurity information sharing, the legislative proposals on cybersecurity information sharing *begin* to diverge on three central issues: (1) the *types* of cybersecurity information that is authorized for dissemination within the private sector and between the private and public sectors; (2) the *entities* that can *receive* such information; and (3) the *purposes* for which such information can be used.

- **Types of Cybersecurity Information:** The broadest approach is epitomized by bills like the Cybersecurity Information Sharing Act of 2014 (CISA), which would allow entities to share information about (1) cyber-vulnerabilities, (2) cyber-threats, *and* (3) broader efforts and strategies that have been used to prevent or mitigate cyberattacks,[353] encompassing nearly any type of information within an entity's possession that merely pertains to cybersecurity. A more narrow approach would be that of proposals like the (CTSA), which allows public and private entities to share only limited types of cyber-threat information and does not contemplate entities sharing cybersecurity strategies with each other.[354]

(...continued)

Information in the Possession of Private Entities."; *see also* Zheng and Lewis, *supra* note 32, at 8 ("Sharing is not directly authorized by law ... which has created uncertainty around the legality of sharing cyber threat information.").

[349] *See* CISPA §2(b)(4)(C).

[350] *See id.* §3 (enacting §1104(b)).

[351] *See* CTSA §2 (enacting §229(c)(1)).

[352] *Id.* §2 (enacting §229(b)(1)).

[353] *See* CISA §3(a)(2) (allowing for the sharing of "cyber threat indicators" from the federal government to the private sector); *id.* §4(c)(1) (allowing an "entity" to share with or receive from the federal government or "any other entity" "cyber threat indicators" and "countermeasures"); *see generally id.* §1(7) (defining the term "cyber threat indicator" to include (1) malicious reconnaissance (e.g., anomalous patterns of communications); (2) methods of defeating a security control or exploitation of a security control or exploitation of a security vulnerability; (3) security vulnerabilities, (4) methods of causing a user to unwittingly defeat a control; (5) malicious cyber command and control; (6) actual or potential harm caused by an incident (including information exfiltrated from the information system); (7) any other attribute of a cybersecurity threat); *id.* §1(4)(defining "countermeasure" as "an action, device, procedure, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that prevents or mitigates a known or suspected cybersecurity threat or security vulnerability.").

[354] *See* CTSA §2 (enacting §229(b)-(c)). For example, the CTSA maintains most of the CISA's definition for "cyber threat indicator," but excludes from the definition "actual or potential harm caused by an incident," including data associated with such an incident. *See id.* §2 (enacting §229(a)(3)). Moreover, the CTSA narrows the definition of "cyber threat indicator" in that "reasonable efforts must be made to remove information that may be used to identify (continued...)

- **Who Can Receive Covered Cybersecurity Information:** Bills like CISPA, which generally authorizes a private entity to share cyber-intelligence with "any other entity" it so chooses,[355] contrast sharply with proposals like the CTSA, which limits sharing by private parties to ISAOs and the NCCIC[356] and does not contemplate sharing of cyber-information between, for example, two private entities outside of an ISAO.
- **Purposes For Which Shared Covered Cyber-Information Can Be Used:** CISPA, for example, allows the disclosing entity to place "any restrictions" on the use of shared information[357] and generally[358] limits shared intelligence so that such material can only be used for a "cybersecurity purpose,"[359] a term of art that broadly encompasses nearly any effort that is aimed at protecting a system or network from a range of different cyberattacks.[360] In contrast, the CTSA more closely circumscribes the uses for which shared information can be put. The CTSA, in addition to having provisions analogous to CISPA that limit the use of covered cyber-information based on the restrictions imposed by the sharing entity[361] and general cybersecurity purposes,[362] would affirmatively require those that share and use "cyber threat indicators" to make "reasonable efforts" to minimize information unrelated to a cyber-threat that may be used to identify specific persons and to "safeguard information" that may be used to identify specific persons from unintended or unauthorized disclosures.[363]

The issues of *what* can be shared, with *whom* covered information can be shared, and the *purposes* for which that information can be used once shared will necessarily define the scope and overall goals of any cybersecurity information sharing legislation. Proposals that sharply circumscribe the types of information that can be shared, the parties that can receive such

(...continued)

specific persons reasonably believed to be unrelated to the cyber threat" for such information to be considered a "cyber threat indicator." *See id.* §2 (enacting §229(a)(3)(B)). The CTSA does not allow private or public entities to share countermeasures as defined by the CISA.

[355] *See* CISPA §3 (enacting §1104(b)).

[356] *See* WHD §103(b); *see also* CTSA §2 (enacting §229(b)(1)).

[357] *See* CISPA §3 (enacting §1104(b)(2)(A)).

[358] CISPA does prohibit shared information from being used for an "unfair competitive advantage to the detriment" of the entity that provided the information. *Id.* §3 (enacting §1104(b)(2)(B)).

[359] *Id.* §3 (enacting §1104(b)(2)(D)).

[360] *See id.* §3 (enacting §1104(f)(8)) (defining cybersecurity purpose to mean "the purpose of ensuring the integrity, confidentiality, or availability of, or safeguarding, a system or network," including protecting a system or network from (1) a vulnerability; (2) a threat to its integrity, confidentiality, or availability; (3) an effort to deny access or degrade, disrupt, or destroy; (4) an effort to gain unauthorized access (other than by solely violating a terms of service agreement).

[361] *See* CTSA §2 (enacting §229(b)(3)(C)).

[362] *See id.* §2 (enacting §229(b)(3)(A)) (mandating that shared cyber-threat indicators can only be used for the "purpose" of protecting an "information system or information that is stored on, processed by, or transiting an information system from cyber threats;" "identifying or mitigating such cyber threats;" or "reporting a crime."). A cyber threat is defined by the CTSA as "any action that may result in ... unauthorized access" (other than solely violating a terms of service agreement) "in order to damage or impair the integrity, confidentiality, or availability of an information system; or ... unauthorized exfiltration, deletion, or manipulation of information that is stored on, processed by, or transiting an information system." *See id.* §2 (enacting §229(a)(2)).

[363] *See id.* §2 (enacting §229(b)(3)(B)).

information, and the uses for that information once it is received will necessarily discourage the dissemination and utilization of cyber-intelligence when compared to bills that take a different approach. On the other hand, proposals that generally authorize vast amounts of cyber-information to be disseminated to a wide range of public and private entities to be used for any number of purposes may be open to criticism that such proposals go too far and undermine other interests, like individual privacy rights. Nonetheless, the three central issues animating the legal frameworks for cybersecurity information reform proposals are only the starting points for the legal discussions on cyber-information reforms. Generally the major proposals on cyber-intelligence sharing begin by establishing fairly broad authorizations for the dissemination of cyber-intelligence and then regulate such activities accordingly,[364] creating several other avenues for legal debate.

Clarifying Which Government Agency Leads the Efforts on Cyber-Information Sharing

Once a legislative proposal has generally authorized broader cybersecurity information sharing between the public and private sectors, the legislation may need to resolve what entity in the government needs to be the liaison between the public and private sector with regard to such sharing of information. As noted above, while ample legal authority currently exists for DHS to serve as the central repository and distributor of cyber-intelligence for the federal government,[365] the legal authorities that do exist often overlap, perhaps resulting in confusion as to which of the multiple sub-agencies within DHS or even outside of DHS, like the newly formed CTICC, should be leading efforts on cybersecurity information sharing.[366]

While earlier versions of cybersecurity legislation contemplated placing the Office of the Director of National Intelligence (DNI) or the Department of Defense (DOD) at the forefront of federal cyber-information sharing efforts,[367] more recent legislation has tasked DHS with the role of coordinating cyber-information sharing. For example, the CTSA designates the NCCIC as the entity charged with receiving and disclosing all "cyber threat indicators" to federal and non-federal entities.[368] Less specific, CISPA allows the President to designate an "entity within [DHS] as the civilian Federal entity to receive cyber threat information"[369] and share that information with other governmental entities,[370] while allowing the President to designate an entity within DOJ to serve as the entity that receives information related to cybercrimes[371] and disseminates such information throughout the federal government.[372] Other legislation may attempt to task

[364] *See, e.g.,* CISPA §3 (enacting §1104(b)(2)) (authorizing the sharing of cyber-threat information, but regulating the use and protection of such information).

[365] *See supra* notes 66-71 and accompanying text (on federal authority to distribute cyber-information); *see also supra* notes 267-270 and accompanying text (on federal authority to receive cyber-information from the private sector).

[366] *See supra* notes 72-76 and accompanying text.

[367] *See, e.g.,* SECURE IT, S. 3342, 112th Cong. §103(a)(1).

[368] *See* CTSA §2 (enacting §229(c)(1) (The Secretary shall designate the [NCCIC] to receive and disclose cyber threat indicators to Federal and non-Federal entities in as close to real time as practicable, consistent with, and in accordance with the purposes of, this section.").

[369] *See* CISPA §2(b)(1).

[370] *See id.* §2(b)(3).

[371] *See id.* §2(b)(2).

[372] *See id.* §2(b)(3).

several federal agencies with the job of promulgating regulations with respect to the receipt and distribution of cyber-intelligence. CISA, for example, would require the DNI, DHS, DOD, and DOJ to consult and jointly develop procedures that facilitate the timely sharing of federal "cyber threat indicators."[373] The bill would also require the Attorney General to promulgate "policies and procedures" with regard to the receipt of cyber-threat indicators form the private sector.[374] Nonetheless, CISA does contemplate a central role for DHS with regard to the receipt and disclosure of cyber-information, requiring the agency to "develop and implement a capability and process" for accepting cyber threat indicators and countermeasures and ensuring all appropriate federal entities "receive such cyber threat indicators.... "[375]

Few proposals, however, would attempt to resolve the issue of overlapping legal authorities that currently exist with respect to cyber-information sharing. While an argument could be made that the CTSA's naming of the NCCIC as the entity charged with receiving and distributing cyber threat indicators clarifies internal divisions of authority as to what agencies must take the lead on cyber-information sharing efforts,[376] nothing in the legislation explicitly repeals similar authority provided to other federal entities in earlier laws, implying that such authorities remain.[377] Other proposals, such as CISPA, go so far as to disclaim "limit[ing] or modify[ing]" "existing" information sharing relationships,[378] indicating that such proposals would do little to modify the existing division of authority within the federal government with respect to cybersecurity information sharing.

Increasing the Amount and Quality of Government Cyber-Information Disclosed to the Private Sector

Beyond clarifying *who* in the government is tasked with receiving and disseminating cyber-information, another central theme for cybersecurity proposals is ensuring that the underlying information that is disseminated from the government is both voluminous and helpful. As discussed above, while the government has wide authority to disclose cyber-intelligence within its possession, that authority is not limitless and is necessarily tied to laws that restrict the government's ability to release sensitive information within its possession.[379] More broadly, delays in the dissemination and sanitation of cyber-intelligence arguably may severely diminish the effectiveness of such information.[380]

To increase the speed at which cyber-threat information is distributed and the volume of cyber-intelligence that is disclosed, two main strategies are contemplated by various cybersecurity

[373] *See* CISA §3(a).

[374] *Id.* §5(a).

[375] *See id.* §5(c)(1).

[376] *See generally* Washington Gas Light Co. v. Byrnes, 137 F.2d 547, 561 (D.C. Cir. 1943) ("When ... a new law is designed to achieve a clear purpose, it must be respected; and inconsistent procedures, previously existing must be disregarded.").

[377] *See generally* Nat'l Ass'n of Home Builders v. Defenders of Wildlife, 551 U.S. 644, 662 (2007) ("'[R]epeals by implication are not favored' and will not be presumed unless the 'intention of the legislature to repeal [is] clear and manifest.'") (internal citations omitted).

[378] *See* CISPA §6(f)(1).

[379] *See supra* notes 82-87 and accompanying text.

[380] *See supra* notes 88-90 and accompanying text.

proposals. First, several pieces of cybersecurity legislation would require DHS to create the capabilities to distribute cyber-intelligence in "real time" to other federal agencies[381] and even the private sector.[382] CISA, for example, contemplates real time or instantaneous, "automated" distribution of cyber-information being facilitated through the creation of a universal electronic format for cyber-information.[383] Second, several bills contemplate authorizing additional access to classified cyber-intelligence within the possession of the government by those in the private sector.[384] For example, CISPA mandates that the DNI establish procedures to allow the intelligence community to share classified cyber-threat intelligence with the private sector,[385] including requiring the expedited issuance of security clearances for those who may need access to cyber-intelligence.[386]

Nonetheless, most of the proposals encouraging faster and more robust dissemination of cyber-information speak only in the most general terms and delegate the authority to accomplish, for example, real time dissemination of cyber-information to an agency like DHS or the DNI.[387] There is an inherent tension between (1) allowing for the rapid disclosure of a large volume of sensitive cyber-intelligence and (2) preserving the privacy and national security interests that currently limit the disclosure of such information. What remains to be seen is whether legislation or subsequent agency action can effectively accomplish the competing goals that underlie the debate over recent cybersecurity information sharing efforts.

Minimizing Liability Related to Distributing Privately Held Cyber-Intelligence

Perhaps the most heavily debated legal issue respecting cyber-information sharing legislation is how to adequately minimize the host of liability issues that may arise for those in the private sector that may wish to disclose cyber-intelligence to outsiders.[388] As noted above, those in the private sector that wish to engage in cyber-information sharing may be exposed to civil and even criminal liability from a host of different federal and state laws.[389] Moreover, because of the uncertainty that pervades the interplay between laws of general applicability—like federal antitrust or privacy law—and their specific application to cyber-intelligence sharing, it may be

[381] *See, e.g.,* CISPA §2(b)(4)(A)-(B) (allowing for real time distribution to other federal entities); CTSA §2 (enacting §229(c)(3)) (same); CISA §5(c)(1)(C) (same).

[382] *See, e.g.,* CTSA §2 (enacting §229(c)) ("The Secretary shall designate the Center to receive and disclose cyber threat indicators to Federal and non-Federal entities in as close to real time as practicable, consistent with, and in accordance with the purposes of, this section."); CISA §3(b)(1).

[383] *See* CISA §§2(8), 5(c).

[384] *See, e.g.,* CTSA §2 (enacting §229(c)(2) (authorizing DHS to coordinate federal efforts to "ensure that useful classified ... cyber threat indicators are shared in a timely manner with non-Federal entities."); CISA §3(a)(1) (authorizing the development of procedures that allow for the "timely sharing of classified cyber threat indicators in the possession of the Federal Government with cleared representatives of appropriate entities."); CISPA §3(a) (enacting §1104(a) (authorizing the DNI to establish procedures regarding the sharing and use of classified cyber-intelligence).

[385] *See* CISPA §3(a) (enacting §1104(a)(1)).

[386] *Id.* §3(a) (enacting §1104(a)(3)).

[387] *See supra* notes 382-384.

[388] *See, e.g.,* Paul Rosenzweig, *Comparing the Senate Cybersecurity Liability Provisions,* LAWFARE, (March 18, 2012), *available at* http://www.lawfareblog.com/2012/03/comparing-the-senate-cybersecurity-liability-provisions/ (hereinafter "Rosenzweig-Lawfare").

[389] *See generally supra* "Sharing Cyber-Information in the Possession of Private Entities."

very difficult for any private entity to accurately assess potential liability that could arise by participating in a sharing scheme.[390] Without some assurances with regard to liability, the potential exists that a private entity may simply refuse to participate in information sharing, reasoning that any amorphous benefits that could be realized would simply not cover the cost of liability.[391] As a consequence, several cybersecurity proposals have attempted to minimize potential exposure for and rationalize any costs associated with sharing privately held cyber-intelligence,[392] initiating a legal debate of its very own on how to properly scope such liability protections.[393]

"Tailored" Approach to Minimizing Liability

There are two central legal approaches to crafting liability immunity provisions in the context of cybersecurity information sharing legislation. First, some have argued for including more narrowly tailored immunity provisions, such that a provision is tied to a particular law that could be the source of civil or criminal liability for private entities that engage in cyber-information sharing.[394] For example, Gregory Nojeim of the Center for Democracy and Technology has argued for passing legislation that creates an additional exemption to ECPA, authorizing service providers to "make disclosures to other service providers or to the government to help protect the systems of *other* service providers."[395]Likewise, others have advocated for a "cyber-security exception to the antitrust laws," by creating an explicit "legislative carve-out" allowing for the exchange of "vulnerability, threat, and countermeasure information and the development of common security protocols."[396] The upside of the "tailored" approach to liability protection is that by crafting narrow immunity provisions there is less of a risk that any new cybersecurity legislation will disrupt or undermine the goals of previously existing legislative schemes by, for example, immunizing anticompetitive behavior or actions that erode third-party privacy interests.

Nonetheless, the tailored immunity approach has a significant drawback, as well, in that crafting an immunity provision for each and every source of liability that a private entity could face with regard to the sharing of cyber-intelligence may simply be impossible. After all, those entities that collect or disclose cybersecurity information could potentially face countless lawsuits arising under (1) any of the three titles of ECPA, (2) any of a number of other federal privacy laws, (3) federal antitrust law, (4) state common law tort, fiduciary duty, or implied contract claims, or (5) a variety of state privacy or antitrust laws.[397] An argument can be made many of these legal claims are simply meritless or inapplicable with respect to the most benign forms of a cyber-intelligence sharing. Nonetheless, the fact remains that at least in the view of many information technology experts significant gray areas exist in various places in the law deterring more

[390] *Id.*

[391] *See* Brian B. Kelly, *Investing in a Centralized Cybersecurity Infrastructure: Why 'Hacktivism' Can and Should Influence Cybersecurity Reform,* 92 B.U.L. REV. 1663, 1696 (2012).

[392] *See, e.g.,* CISPA §3 (enacting §1104(b)(3)); CTSA §2 (enacting §229(b)); CISA §6.

[393] *See, e.g.,* Rosenzweig-Lawfare, *supra* note 388.

[394] *See* Nojeim Testimony, *supra* note 132, at 5 ("Companies that share information under such a narrow exception will enjoy the liability protections already built into theses statutes. As other statutes that limit information sharing for cyber security purposes are identified, Congress may consider additional exceptions.").

[395] *Id.* (emphasis added).

[396] *See* Sales, *supra* note 26, at 1551.

[397] *See generally supra* "Sharing Cyber-Information in the Possession of Private Entities."

aggressive forms of cyber-intelligence sharing,[398] perhaps warranting more broad-based liability protections. Moreover, because of the potential bases for civil liability, like antitrust and tort law, are based in part on evolving common law standards, enacting cybersecurity information sharing legislation that includes a narrowly tailored immunity provision may not deter the lawsuits of tomorrow that are unanticipated by lawmakers.[399] Finally, even if many of the legal claims levied against entities that share cyber-threat information may be meritless, a determination of the legal merits will often require factual development by the litigants, as federal litigants, for example, need only plead a plausible theory as to liability in order to avoid the initial dismissal of a federal complaint.[400] As a result, liability carve-outs that are limited to only the most meritorious legal claims may not prevent private entities from being subject to potentially expensive factual discovery that may deter cybersecurity information sharing efforts.[401]

"Broad" Approach to Minimizing Liability

Perhaps as a result of the drawbacks of the tailored approach, most of the recent legislation on cybersecurity information sharing has taken the opposite approach: proposing more sweeping language that broadly immunizes private entities involved in collecting and disclosing cyber-intelligence and then drafting tailored exceptions to curb the scope of the immunity. The "broad" approach to civil liability protections for those that wish to collect and share cybersecurity information commonly has four foundations:

- **Notwithstanding Clauses:** Several cybersecurity bills, in authorizing the collection or sharing of cyber-information, will preface any such language with a "notwithstanding" clause.[402] For example, Section 3 of CISA states "Notwithstanding any other provision of law, an entity may ... share with, or receive from, any other entity or the Federal Government cyber threat indicators and countermeasures."[403] Courts generally interpret notwithstanding clauses as signifying that any phrases following the clause "supplant" and "supersede" any conflicting law,[404] which in the context of cybersecurity legislation would imply that any authorizing language to collect and disseminate covered cyber-

[398] *See* Ponemon Institute—Threat Intelligence, *supra* note 33, at 3.

[399] For example, Professors Rustad and Koenig have written extensively on the need for courts to begin to recognize new torts based on the negligent enablement of cybercrime. *See supra* note 244.

[400] *See* Ashcroft v. Iqbal, 556 U.S. 662, 679 (2009). For example, rule of reason antitrust cases often require resolution at the summary judgment as opposed to motion to dismiss stage because of the factually intensive nature of such cases. *See* C. Paul Rogers III, *The Incredible Shrinking Antitrust Law and the Antitrust Gap,* 52 U. LOUISVILLE L. REV. 67, 79 (2013).

[401] Litigation costs in a "typical" federal lawsuit were recently estimated at nearly $20,000 for defendants, but in cases involving large corporations discovery expenses can balloon to over $700,000. *See The Costs and Burdens of Civil Discovery: Hearing before the Subcommittee on the Constitution of the Committee on the Judiciary,* 112th Cong, 1st Sess 4-5 (2011) (written statement of William H. J. Hubbard, Ass't. Prof. of Law, University of Chicago Law School). Discovery can be particularly expensive in cases involving electronic data, such as those involving cyber-information, as discovery involving electronic data on average costs of "tens or hundreds of thousands of dollars" in even average cases. *See* Scott A. Moss, *Litigation Discovery Cannot be Optimal but Could be Better: The Economics of Improving Discovery Timing in a Digital Age,* 58 DUKE L.J. 889, 894 (2009).

[402] *See, e.g.,* CISPA §3 (enacting §1104(b)(1)-(2); CTSA §2 (enacting §229(b)(1)); CISA §4(c)(1).

[403] *See* CISA §4(c)(1).

[404] *See In re* Robinson, 764 F.3d 554, 560 (6th Cir. 2014); Gonzales v. Arrow Fin. Servs., LLC, 660 F.3d 1055, 1066 n.8 (9th Cir. Cal. 2011); Multi-State Communications, Inc. v. FCC, 728 F.2d 1519, 1525 (D.C. Cir. 1984).

information that followed a notwithstanding clause would supersede any laws of general applicability that may deter or prohibit such behavior.

- **Limitation of Liability Clauses:** Beyond the use of notwithstanding clauses, recent cybersecurity legislation has additionally contained explicit provisions that pertain to liability and contemplate dismissal of lawsuits at early stages of litigation generally pertaining to cyber-information collection and/or sharing.[405]
- **Good Faith Safe Harbors:** In addition to explicit liability limitations, CISPA and CISA both contain provisions that would allow defendants whose conduct otherwise would not fall within the scope of the limitation of liability clause to seek dismissal on the ground that the defendant relied in good faith that the conduct complained of was "permitted" under the law.[406]
- **Preemption Clauses:** Finally, to ensure that no *state* or *local* laws interfere with cybersecurity information sharing, recent cybersecurity proposals have contained explicit preemption clauses that functionally displace any non-federal laws that could be the source of liability for or otherwise interfere with any activities permitted under a given cyber-information sharing proposal.[407]

The broad approach to liability protections for private entities that collect and disseminate cyber-intelligence should not be conflated with a "limitless" approach. Rather the scope of the immunity provisions under the broad approach is necessarily a product of language contained within the four key clauses. As a consequence, cybersecurity bills vary considerably with respect to the scope of liability protections for information sharing. For example, CTSA only prohibits civil or criminal causes of action from being maintained against entities for receiving or disclosing "lawfully obtained cyber threat indicators" from the NCCIC or a self-certified ISAO.[408] The plain language of the CTSA would not immunize an entity with regard to (1) activities taken to *acquire* cyber-threat information; (2) the sharing of information outside of the NCCIC or a self-certified ISAO; or (3) if the underlying information were not "lawfully obtained cyber threat indicators," which presumably would exclude from the provision "cyber threat

[405] *See, e.g.* CISPA §3 (enacting §1104(b)(3)) ("No civil or criminal cause of action shall lie or be maintained in Federal or State court ... for using cybersecurity systems to identify or obtain cyber threat information or for sharing such information in accordance with this section; or ... for decisions made for cybersecurity purposes and based on cyber threat information identified, obtained, or shared under this section."); CTSA §2 (enacting §229(d)(1)(A)) ("A civil or criminal action may not be filed or maintained in a Federal or State court against an entity for the voluntary disclosure or receipt under this section of a lawfully obtained cyber threat indicator, that the entity was not otherwise required to disclose, to or from ... [the NCCIC] or a [self-certified ISAO]."); CISA §6(a)-(b) ("No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the monitoring of information systems and information ... [and] the sharing or receipt of cyber threat indicators or countermeasures.... ").

[406] *See* CISPA §3 (enacting §1104(b)(3)(B)) (exempting from the liability limitation clause any acts that lack good faith, including "any act or omission taken with intent to injure, defraud, or otherwise endanger any individual, government entity, private entity, or utility."); CISA §6(c) ("[A] good faith reliance by an entity that the conduct complained of was permitted under this Act shall be a complete defense against any action brought in any court against such entity.").

[407] *See, e.g.,* CISPA §3 (enacting §1104(e) ("This section supersedes any statute of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under subsection (b)."); CTSA §2 (enacting §229(f)(2)) ("This section supersedes any law or requirement of a State or political subdivision of a State that restricts or otherwise expressly regulates the retention, use, or disclosure of a cyber threat indicator by a private entity."); CISA §8(j)(1) ("This Act supersedes any statute or other law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this Act.").

[408] *See* CTSA §2 (enacting §229(d)(1)(A)).

indicators" for which "reasonable efforts" had not been made to eliminate personal information from such information.[409] In contrast, bills like CISA more broadly prohibit causes of action based on the collection, sharing, or receipt of information with any other entity or the federal government.[410] Moreover, beyond the general language respecting the four key clauses pertaining to immunity, legislative proposals may have specific carve-outs that pertain to a given cause of action, such as provisions in CISA that maintain antitrust claims based on "price-fixing" or "monopolization"[411] or tort claims based on "gross negligence" or "willful misconduct."[412]

The question that remains to be answered with respect to the broad approach toward liability protection is whether such an approach will truly accomplish the goals of minimizing exposure and creating more legal certainty for those private parties that may wish to share cyber-intelligence. Given the host of limits and caveats that have been placed on the general immunity provisions in the various cybersecurity bills, one might ask whether the resulting language creates a host of new legal questions and produces an equally uncertain legal landscape as to the liability risks posed by information sharing. More broadly, phrases like "good faith" and "notwithstanding" are arguably not legal silver bullets that will necessarily eliminate all litigation associated with cyber-information collection and sharing.[413] Nonetheless, given that legal certainty may simply be impossible with respect to an activity at the epicenter of so many areas of law, the ultimate questions for lawmakers with respect to information sharing immunity provisions will be how much legal uncertainty can be tolerated by the private sector and how much of a role should other laws—like federal privacy and antitrust laws—play with regard to cyber-intelligence collection and dissemination.

Increasing the Participation of Private Sector Cyber-Information Sharing

Questions respecting liability protections in cybersecurity legislation take place in a broader debate over how to increase the participation of private sector entities that currently may be reluctant to share cyber-intelligence within their possession. One solution that has been suggested is to amend current law on cybersecurity information sharing, which contemplates private entities *voluntarily* sharing and receiving information,[414] and impose a mandate on entities to collect cyber-intelligence from their own computer networks and share it with other private entities and the government or else risk civil liability for refusal to comply with the mandate.[415]

---

[409] *See id.* §2 (enacting §229(a)(3)(B)).

[410] *See* CISA §6(a)-(b).

[411] *See id.* §8(e) (allowing claims based "price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, boycotting or exchanges of price or cost information, customer lists, or information regarding future competitive planning).

[412] *See id.* §6(e).

[413] *See, e.g.,* Rosenzweig-Lawfare, *supra* note 388 ("Of course, 'good faith' is a fact bound issue and will generate litigation."); Miccosukee Tribe of Indians of Fla. v. United States Army Corps of Eng'rs, 619 F.3d 1289, 1298 (11th Cir. 2010) (noting the limitations of a "notwithstanding clause").

[414] *See* 6 U.S.C. §143(1).

[415] *See, e.g.,* Gyenes, *supra* note 56, at 295 ("A simpler plan could push 'critical' industry to improve its cybersecurity.... ."); Broggi, *supra* note 31, at 674-75 ("Congress could mandate that the private sector share certain cybersecurity information with the government."); Sales, *supra* note 26, at 1549 ("The government could require firms to gather information about the vulnerabilities in their systems, the type of attacks they have suffered, and the countermeasures they have used to combat malware, and then to disseminate the date to designated recipients.").

Mandatory information sharing could raise several difficult legal questions, however. First, a mandate that companies collect and share cyber-information could be in tension with the Fourth Amendment to the Constitution, which generally prohibits the government from conducting unreasonable searches.[416] While the Fourth Amendment facially only applies to government searches,[417] courts have recognized that searches conducted by ostensibly private parties can constitute government action when the government knew of and acquiesced in the intrusive conduct and the party performing the search intended the search to occur for the benefit of the government.[418] Arguably, a government mandate to collect cyber-intelligence would transform those in the private sector who are now *required* under federal law to share information with the government into government actors, raising the question of whether such a law would violate the Fourth Amendment.[419]

The resolution of that question will likely depend on a number of factors. For example, the Fourth Amendment inquiry will likely depend on the nature of cyber-information being collected in the private sector, as acquisitions of non-content information have generally been found to fall outside of Fourth Amendment protection.[420] Moreover, any Fourth Amendment challenge may fail if the plaintiff consented to the underlying search[421] by, for example, agreeing to a computer-use policy or clicking through a banner on a website that warns of the potential invasion of privacy.[422] Finally, the propriety of a mandatory cyber-information program under the Fourth Amendment may depend on the specifics of a mandatory information sharing program, as the Supreme Court has recognized a "special needs" exception to the Fourth Amendment, whereby when a "special need" beyond the "normal need for law enforcement, make[s] the warrant and probable-cause requirement impracticable"[423]—such as preventing a cyberattack—require balancing the gravity of the public interests, the degree to which an intrusion advances the public interests, and the severity of the interference with individual liberty.[424]

Mandated disclosures of cyber-intelligence may conflict with other provisions in the Constitution. For example, the Supreme Court has recognized that the First Amendment not only protects the "right to speak freely," but also includes "the right to refrain from speaking at all."[425] While much of the Court's compelled speech jurisprudence arises in the context of a speaker being forced to endorse a particular ideological message,[426] the Court has recognized that "compelled statements

[416] *See* U.S. CONST. am. IV.

[417] Burdeau v. McDowell, 256 U.S. 465, 475 (1921).

[418] *See* United States v. Souza, 223 F.3d 1197 (10th Cir. 2009); *see also* United States v. Momoh, 427 F.3d 137, 140-41 (1st Cir. 2005) (using a multi-factor test, as opposed to the *Souza* test, to distinguish private and government action for Fourth Amendment purposes that included the following factors: "the extent of the government's role in instigating or participating in the search, its intent and the degree of control it exercises over the search and the private party, and the extent to which the private party aims primarily to help the government or to serve its own interests."); *see generally* CRS Report WSLG481, *CISPA, Private Actors, and the Fourth Amendment*, by (name redacted) (discussing the Fourth Amendment and its application to private actors engaging in computer searches).

[419] *See* Broggi, *supra* note 31, at 675 ("[A] mandate would render scanning pursuant to the ECS program a government search within the meaning of the Fourth Amendment.").

[420] *See* Smith v. Maryland, 442 U.S. 735, 742 (1979).

[421] *See* Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973).

[422] *See* United States v. Angevine, 281 F.3d 1130, 1134-1135 (10th Cir. 2002).

[423] *See* Griffin v. Wisconsin, 483 U.S. 868, 873 (1987).

[424] *See* Illinois v. Lidster, 540 U.S. 419, 426-27 (2004).

[425] *See* Wooley v. Maynard, 430 U.S. 705, 714 (1977).

[426] *See, e.g., id.; see also* W. Va. State Bd. of Educ. v. Barnette, 319 U.S. 624, 642 (1943) ("If there is any fixed star in (continued...)

of fact ... like compelled statements of opinion, are subject to First Amendment scrutiny."[427] In the context of requiring a private entity to disclose cyber-information, an argument could be made that a private entity has a First Amendment interest in not being required to divulge factual information the entity "would rather avoid."[428] While the Court has upheld compelled disclosure requirements in context of commercial speech cases,[429] it is unclear whether commercial speech case law is relevant to the compelled disclosure of cyber-intelligence.[430] Instead, content-based speech compelled by the government is generally subject to strict scrutiny, requiring the underlying policy to be narrowly tailored to promote a compelling government interest.[431] Given the serious threat potentially posed by cyberattacks and the supposed ability of robust cyber-intelligence to deter such attacks,[432] a narrowly tailored mandate for the disclosure of cyber-threats arguably may be able to survive a First Amendment challenge.[433] Nonetheless, the law on compelled speech is far from clear[434] and may be one of several other constitutional challenges to a mandatory cyber-threat collection and disclosure law.[435]

Beyond the constitutional issues respecting mandatory cyber-information sharing, there may be practical problems with such a proposal. For example, imposing some sort of penalty or liability on a company that did not participate in a mandatory information sharing scheme only induces an entity to share information if the penalties for not participating outweigh costs associated with participation, such as liability risks or risks to a firm's reputation for disclosing the details about a

(...continued)

our constitutional constellation, it is that no official, high or petty, can prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion or force citizens to confess by word or act their faith therein.")

[427] *See* Rumsfeld v. Forum for Academic & Institutional Rights, Inc., 547 U.S. 47, 61 (2006).

[428] *See generally* Riley v. Nat'l Federation of the Blind of North Carolina, Inc., 487 U.S. 781, 797-98 (1988) (holding that a speaker "has the right to tailor the speech, applies not only to expressions of value, opinion, or endorsement, but equally to statements of *fact* the speaker would rather avoid."); *see* James T. O'Reilly, *"Access to Records" Versus "Access to Evil:" Should Disclosure Laws Consider Motives as a Barrier to Records Release?,* 12 KAN. J.L. & PUB. POL'Y 559, 560 & n.6 (2003) (suggesting that compelled disclosure of cyber threat information may implicate First Amendment interests).

[429] *See, e.g.,* Zauderer v. Office of Disciplinary Counsel of the Supreme Court of Ohio, 471 U.S. 626, 650-53 (1985).

[430] *Cf.* Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, 425 U.S. 748, 772 n.24 (1976) (describing commercial speech as speech that "does 'no more than propose a commercial transaction.'") (internal citations omitted).

[431] *See Riley*, 487 U.S. at 797-98.

[432] *See supra* notes 12-35 and accompanying text.

[433] *See generally* Robert Post, *Compelled Subsidization of Speech:* Johanns v. Livestock Marketing Assocation, 2005 Sup. Ct. Rev. 195, 213-14 & n.92-97 ("[T]he First Amendment is not triggered by all government compulsions to speak. In fact we experience such compulsions all the time, and no one regards them as raising constitutional issues. Examples range from compulsory jury service, to compulsory testimony before courts and legislatures, to compulsory reporting of vehicle accidents, to compulsory reporting of potential public health risks like those involving child abuse, to the myriad of public disclosures required by securities regulation, to the labeling requirements routinely required on consumer products.").

[434] *See* Laura J. Hendrickson, *State Government Speech in a Federal System,* 6 CARDOZO PUB. L. POL'Y & ETHICS J. 691, 706 (2008) (noting that "confusing line of cases defines the doctrine on compelled speech.").

[435] For example, one could envision Fifth Amendment interests being implicated if an individual was, under the threat of legal compulsion, forced to reveal facts about a cyberattack that would incriminate them in some criminal activity. *See generally* Doe v. United States, 487 U.S. 201, 212 (1988). Similarly, the Fifth Amendment may be implicated if a law required the disclosure of cyber-intelligence that altered a business's investment-backed expectation of confidentiality in that information, amounting to a taking lacking just compensation. *See* Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002-04 (1984).

cyberattack.[436] Moreover, as one commentator has argued, because of the prevalence of consumer and privacy groups closely watching those that possess cybersecurity information, voluntary cyber-information sharing programs can be better tailored than heavy-handed mandates to ensure that information is shared in a manner that is effective, but not so robust as to allow for "forms of sharing that the public believes are especially intrusive."[437]

Recent cybersecurity legislation has eschewed any mandatory information sharing schemes. For example, CISPA contains an "anti-tasking restriction" that explicitly prevents the bill from being construed to "require a private-sector entity or utility to share information with the Federal Government."[438] Similar provisions exist in the CTSA[439] and CISA.[440] The issue that remains for lawmakers who prefer a voluntary scheme for cyber-information sharing is how to create sufficient incentives that overcome the legal and non-legal disincentives that are currently deterring more robust dissemination of cyber-intelligence.[441] Proposals like CISPA provide two related incentives—liability protections and access to government cyber-intelligence—but other incentives for information sharing could include subsidies,[442] such as "direct payments from the government, tax credits, or deductions" for entities that engage in cyber-information sharing,[443] or other benefits like intellectual property protections.[444] At least one bill has been introduced in Congress that would amend the Internal Revenue Code to create incentives for information sharing.[445] Whether any or all of these incentives would be effective in increasing participation in cyber-intelligence sharing schemes, an issue beyond the scope of this report, will be a critical question for lawmakers to resolve when considering any cybersecurity legislation that aims to increase the amount of cyber-threat information that is available within the private sector.[446]

Preventing Government Misuse of Acquired Cyber-Intelligence

Finally, the last major issue for cybersecurity information sharing legislation is to assuage public fears associated with the government collecting privately held cyber-intelligence, including concerns that the information disclosed to the government could (1) be released through a FOIA request; (2) result in the forfeiting of certain intellectual property rights; (3) be used against a private entity in a subsequent regulatory action; or (4) risk the privacy rights of individuals whose information may be encompassed in disclosed cyber-intelligence.[447] While each of the major

[436] *See* Sales, *supra* note 26, at 1549 ("Imposing such an obligation would not eliminate companies' incentives to withhold cyber-security data. It would simply make it more costly for them to do so, where costs include the sanctions for hoarding discounted by the probability of punishment. Firms will be more likely to collect and share cyber-security data, but some will still find it advantageous to hoard.").

[437] *See* Broggi, *supra* note 31, at 675.

[438] *See* CISPA §3 (enacting §1104(c)(3)).

[439] *See* CTSA §2 (enacting §229(e)(6)).

[440] *See* CISA §8(f)(3).

[441] *See* Bambauer, *supra* note 34, at 1046 (listing various disincentives for information sharing).

[442] *See* Nojeim-Cybersecurity, *supra* note 33, at 128.

[443] *See* Sales, *supra* note 26, at 1550.

[444] *See id.*

[445] *See* Cyber Information Sharing Tax Credit Act, S. 2717, 113th Cong. §2.

[446] *See* Sales, *supra* note 26, at 1550 ("If the subsidies are large enough, firms will have an incentive not just to report the data they have already compiled, but to invest in discovery previously unknown vulnerabilities, threats, and countermeasures.").

[447] *See supra* "*Sharing Cyber -Information with the Government,*" at pp. 32-41.

legislative proposals on cyber-information sharing may differ in substance, there is considerable consensus on the *approach* congressional bills have taken with respect to each of the four major concerns over government control of voluntarily disclosed cyber-intelligence:

- **Public Records Disclosures:** Recent cybersecurity legislation has opted to create a broad FOIA exemption, exempting any covered cyber-information that is shared with the federal government from public disclosure.[448] CISPA, for example, states that "[c]yber threat information shared" in line with the requirements of the bill, if shared with the federal government, "shall be exempt from disclosure" under FOIA,[449] whereas CISA exempts from disclosure "[c]yber threat indicators and countermeasures provided to the" federal government under the bill.[450] In other words, the scope of the FOIA exemptions provided under recent proposals necessarily are a product of what sort of information a particular cyber-information sharing bill covers as an initial matter.[451]
- **Intellectual Property Rights Protection:** To prevent intellectual property rights—such as trade secrets rights—in any shared cyber-intelligence from being forfeited upon disclosure to the government, several proposals contain specific provisions disclaiming any loss of rights as a result of information sharing.[452] CISPA declares that cyber-threat information shared in accordance with the bill must "be considered proprietary information" and restricts disclosure of such material to outsiders unless allowed by the disclosing entity,[453] potentially providing those that share cyber-intelligence with the ability to preserve any trade secret rights in such information. CISA may have the most explicit provisions respecting preservation of intellectual property rights for shared cyber-intelligence, stating that the "provision of cyber threat indicators and countermeasures" to the government "shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection."[454]
- **Regulatory Enforcement Concerns:** To temper fears that cyber-information that is disclosed to the government will be used in later regulatory enforcement actions, two main strategies have been employed in recent cybersecurity legislation. First, several bills have blanket statements that declare that any covered information that is shared with the government will not be used for "regulatory purposes" or a "regulatory enforcement action,"[455] terms of art that are left undefined by the bills. Second, the various legislative proposals will affirmatively limit the federal government from utilizing the shared information

[448] *See* CISPA §3 (enacting §1104(b)(2)(D)(i)); CTSA §2 (enacting §229(d)(2)(A)(i)); CISA §5(d)(3).

[449] *See* CISPA §3 (enacting §1104(b)(2)(D)(i)).

[450] *See* CISA §5(d)(3).

[451] CTSA is the only pending cybersecurity legislation that explicitly amends the CIIA. The bill does this by extending §214 of the Homeland Security Act to cover any "cyber threat indicators" that are submitted by a nonfederal entity to the NCCIC and by excepting from the CIIA's procedural requirements respecting a written statement and acknowledgment of receipt any cyber threat indicators shared under the CTSA. *See* CTSA §2 (enacting §229(d)(2)(B)).

[452] *See* CISPA §3 (enacting §1104(b)(2)(D)(ii)); CISA §5(d)(1)-(2); CTSA §2 (enacting §229(e)(1)(B)(iv).

[453] *See* CISPA §3 (enacting §1104(b)(2)(D)(ii)).

[454] *See* CISA §5(d)(1).

[455] *See* CISPA §3 (enacting §1104(b)(2)(D)(iii)); CISA §§5(d)(5)(D), 8(k); CTSA §2 (enacting §229(d)(3)).

for any purpose other than (1) a "cybersecurity purpose;" (2) to prevent or mitigate an imminent threat of death or serious bodily harm; (3) to respond, prevent or mitigate a serious threat to a minor; or (4) prevent, investigate, or prosecute certain cybercrimes.[456]

- **Privacy Concerns:** In order to assuage more general privacy-based concerns about the implications of the government collecting cyber-information, recent cybersecurity legislation has generally avoided crafting precise rules respecting privacy within the legislation itself in favor of requiring DHS, in conjunction with other federal agencies, to promulgate procedures, policies, and regulations on the federal handling of disclosed information.[457] The guidance the various legislative proposals provide to DHS for the promulgation of privacy rules is general in nature and is centered on the concern that disclosed cyber-intelligence may contain PII.[458] Nonetheless, some proposals do contain specific rules aimed at restricting what types of cyber-information the government can collect and use. CISPA, for example, prevents the government from "us[ing]" particular sensitive documents that contain PII, such as library circulation records or firearm sales records,[459] and prohibits the government from "affirmatively searching" any collected cyber-threat information.[460] CISA affirmatively requires the federal government to protect shared "cyber threat indicators" from unauthorized use or disclosure that may contain PII.[461]

[456] *See* CISPA §3 (enacting §1104(c)(1)(A)-(D)); CISA §5(d)(5)(A)(i)-(iv); CTSA §2 (enacting §229(e)(1)(B)(iii)(I)-(IV)). The CTSA does not use the phrase "cybersecurity purposes," but does restrict the use of a cyber threat indicator by a federal entity for the purpose of protecting "information systems from cyber threats. *See* CTSA §2 (enacting §229(e)(1)(B)(ii)).

[457] *See* CISPA §2(b)(5)(A) (requiring the Secretary of DHS, the Attorney General, the Director of National Intelligence, and the Secretary of Defense to "jointly establish and periodically review policies and procedures governing the receipt, retention, use, and disclosure of non-publicly available cyber threat information shared with the Federal Government" in order to (1) "minimize the impact on privacy and civil liberties," (2) "reasonably limit the receipt, retention, use, and disclosure of cyber threat information associated with specific persons" that is unrelated to a cyber-threat; (3) "safeguard non-publicly available cyber threat information that may be used to identify specific persons from unauthorized access or acquisition;" and (4) protect the "confidentiality of cyber threat information associated with specific persons to the greatest extent practicable"); CISA §3(a) (requiring DNI, DHS, DOD, and DOJ, " in consultation with the heads of the appropriate Federal entities," to jointly promulgate procedures regarding sharing of cyber threat indicators that are "consistent with ... the protection of privacy and civil liberties"); *id.* §3(b) (requiring DOJ to "develop and periodically review guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this Act."); CTSA §2 (enacting §229(d)(3)) (requiring the Secretary of DHS, in consultation with the "Attorney General, the Chief Privacy Officer of the Department, the Chief Privacy and Civil Liberties Officer of the Department of Justice, the Secretary of Commerce, the Director of National Intelligence, the Secretary of Defense, the Director of the Office of Management and Budget, the heads of sector-specific agencies and other appropriate agencies, and the Privacy and Civil Liberties Oversight Board," to "develop and periodically review policies and procedures governing the receipt, retention, use, and disclosure of a cyber threat indicator obtained by a Federal entity.... ").

[458] *See, e.g.,* CISA §5(b)(2) (describing the content of potential privacy regulations, including the need of such rules to include "requirements to safeguard cyber threat indicators containing personal information of or identifying specific persons.").

[459] *See* CISPA §3 (enacting §1104(b)(4) (prohibiting the government from using shared information that includes library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, and medical records).

[460] *See id.* §3 (enacting §1104(b)(2)).

[461] *See* CISA §5(d)(5)(C)(ii).

Given the various restrictions imposed or contemplated in recent cybersecurity information sharing proposals, the issue that remains is how to ensure that such restrictions are complied with by the government. The central enforcement mechanism for any affirmative restrictions on the government's use of shared cyber-information is congressional oversight, in that many of the cyber-information sharing bills require federal agencies to submit regular reports to Congress respecting the government's use of shared cyber-intelligence,[462] including compliance with privacy regulations.[463] Nonetheless, there could be other legal mechanisms available to ensure government compliance with a law's restrictions on the use of shared cyber-intelligence. For example, the CTSA contemplates that any privacy rules promulgated under the proposal would provide for "appropriate penalties for" any government officer, employee, or agent that violates a rule regarding the "receipt, retention, or disclosure of a cyber threat indicator."[464] CISPA perhaps has the most aggressive enforcement mechanism with respect to those government entities that violate the proposal's use restrictions, in that the bill includes a provision that would impose liability on the United States for an intentional or willful violation of any of CISPA's restrictions on how the government can utilize any voluntarily shared cyber-intelligence.[465] Nonetheless, no legislative proposals go as far as current law does with respect to CII, *criminalizing* misconduct with respect to information shared regarding critical infrastructure.[466]

Regardless of the enforceability of a particular restriction on the use of cyber-intelligence by the government, a fundamental question lawmakers may need to contemplate is how restrictions that require close government scrutiny and control over shared cyber-information can be squared with other goals of cyber-information sharing legislation, like requirements that received information be disseminated in an almost instantaneous fashion.[467] Ultimately, because the goals of cyber-information legislation are often diametrically opposed, it may simply be impossible for information sharing legislation to simultaneously promote the rapid and robust collection and dissemination of cyber-intelligence by the federal government, while also ensuring that the government respects the property and privacy interests implicated by such information sharing.[468]

---

[462] *See, e.g.,* CISPA §2(c)(1) (requiring the DHS Inspector General to annually submit to Congress a report reviewing "the use of information shared with the Federal Government under" CISPA); CISA §7(a) (requiring the "heads of the appropriate Federal entities" to biennially submit to Congress a detailed report concerning the implementation of CISA); CTSA §2 (enacting §229(c)(2)(B) (requiring an annual report from DHS be submitted to Congress that reviews cyber threat indicator sharing under CTSA).

[463] *See, e.g.,* CISPA §2(c)(2) (requiring DHS's Officer for Civil Rights and Civil Liberties to annually submit to Congress a report "assessing the privacy and civil liberties impact of the activities conducted by the Federal Government" under CISPA); CISA §7(b) (requiring the Privacy and Civil Liberties Oversight Board and the Inspector Generals of several federal agencies to biennially submit to Congress several detailed report assessing the privacy and civil liberties impact of CISA); CTSA §2 (enacting §229(e)(4) (requiring an annual report from the Chief Privacy of Officer and Chief Privacy and Civil Liberties Officer of DHS be submitted to Congress that assesses "the privacy and civil liberties impact of the governmental activities conducted under" the CTSA).

[464] *See* CTSA (enacting §229(e)(1)(B)(v)).

[465] *See* CISPA §3 (enacting §1104(d)).

[466] *See* 6 U.S.C. §133(f). Moreover, generally where a party wishes to challenge an agency action as violating a federal law or regulation, the Administrative Procedure Act remains as a means to test the legality of the underlying federal agency action. *See* Clouser v. Espy, 42 F.3d 1522, 1528 n.5 (9th Cir. 1994) (citing Lujan v. National Wildlife Federation, 497 U.S. 871(1990)).

[467] *See, e.g.,* CTSA (enacting §229(c)(1) (requiring NCCIC to "receive and disclose cyber threat indicators to Federal and non-Federal entities in as close to real time as practicable.").

[468] *But see* Zheng and Lewis, *supra* note 32, at 8 (arguing that "[s]ecurity and privacy are not mutually exclusive.").

Conclusion

The current legal framework surrounding cyber-information sharing exists at the crossroads of several bodies of law and raises complicated questions respecting how cyber-intelligence can be collected and shared within the private sector and with the public sector. Moreover, as demonstrated by the host of discrepancies and complications raised by various legislative proposals on information sharing, if Congress chooses to alter the current legal framework governing cybersecurity and intelligence sharing, the law will not necessarily be devoid of uncertainty. Instead, new legal questions may arise, likely out of the context of the balance Congress attempts to strike between lowering disincentives for information sharing and ensuring that other interests embodied in privacy, antitrust, tort, or other laws are sufficiently protected under new cybersecurity information sharing legislation. While cybersecurity information sharing is, at most, only one piece of a much larger puzzle regarding how to best protect the United States against potentially debilitating cyberattacks,[469] resolution of the difficult legal questions posed by the regulation of cyber-intelligence sharing may be an important task for the 114th Congress.

Author Contact Information

(name redacted)
Legislative Attorney
[redacted]@crs.loc.gov, 7-....

[469] *See* Howard A. Schmidt, *White House Cybersecurity Coordinator, Legislation to Address the Growing Danger of Cyber-Threats,* (January 26, 2012), *available at* http://www.whitehouse.gov/blog/2012/01/26/legislation-address-growing-danger-cyber-threats ("[O]nly providing incentives for the private sector to share more information will not, in and of itself, adequately address critical infrastructure vulnerabilities.").

EveryCRSReport.com

The Congressional Research Service (CRS) is a federal legislative branch agency, housed inside the Library of Congress, charged with providing the United States Congress non-partisan advice on issues that may come before Congress.

EveryCRSReport.com republishes CRS reports that are available to all Congressional staff. The reports are not classified, and Members of Congress routinely make individual reports available to the public.

Prior to our republication, we redacted names, phone numbers and email addresses of analysts who produced the reports. We also added this page to the report. We have not intentionally made any other changes to any report published on EveryCRSReport.com.

CRS reports, as a work of the United States government, are not subject to copyright protection in the United States. Any CRS report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS report may include copyrighted images or material from a third party, you may need to obtain permission of the copyright holder if you wish to copy or otherwise use copyrighted material.

Information in a CRS report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to members of Congress in connection with CRS' institutional role.

EveryCRSReport.com is not a government website and is not affiliated with CRS. We do not claim copyright on any CRS report we have republished.