Harvard Journal of Law & Technology
Volume 32, Number 2 Spring 2019

BROKEN[1]

Andrea M. Matwyshyn & Stephanie K. Pell***

TABLE OF CONTENTS

---

1. "Broken" is a term of art in computing that refers to a system that is not working properly due to malfunction or problems with design. Eric S. Raymond, *broken*, THE JARGON FILE, VERSION 4.4.8, http://www.catb.org/jargon/html/B/broken.html [https://perma.cc/H88S-BVUW]; Paul Dourish, *The Original Hacker's Dictionary*, PAUL DOURISH, https://www.dourish.com/goodies/jargon.html [https://perma.cc/5H9F-RCEW]. The authors wish to thank Kendra Albert, Steven M. Bellovin, Matt Blaze, Jen Ellis, Jeremy Epstein, Bob Gellman, Jim Green, James Grimmelmann, Marcia Hoffman, Brian Martin, Terrell McSweeny, Alexander Nally, Allison Nixon, Brendan O'Connor, Kurt Opsahl, Jay Radcliffe, Abigail Slater, Mara Tam, Marcia Tiersky, Tarah M. Wheeler, Beau Woods, Chris Wysopal, the Indiana University Center for Applied Cybersecurity Research, and the participants of EstesCon, Narwahlcon, the DEFCON Ethics Village, the 2018 Privacy Law Scholars Conference, and the Data, Technology and Criminal Law Workshop organized by Duke Law School and the University of Wurzburg for their comments and critiques. Any bugs are our own.

* Andrea M. Matwyshyn is a professor of law and professor of computer science (by courtesy) at Northeastern University, an affiliate scholar of the Center for Internet and Society at Stanford Law School, and a Senior Fellow of the Cyber Statecraft Initiative of the Atlantic Council.

** Stephanie K. Pell is an Assistant Professor and Cyber Ethics Fellow at West Point's Army Cyber Institute, with a joint appointment to the Department of English and Philosophy, and an affiliate scholar of the Center for Internet and Society at Stanford Law School. The views expressed are the author's personal views and do not represent the position of West Point, the Army, or the United States Government.

I. INTRODUCTION

Sometimes the "secret ingredient" is a dash of typhoid fever. In an (in)famous moment in the dramatic history of epidemiology, a cook named Mary Mallon, whose hygiene practices were allegedly suboptimal, accidentally transmitted typhoid fever to diners through the meals she prepared. Mallon, better known to history as "Typhoid Mary," was a single carrier of typhoid fever.[2] By the time she was identified as the source of the New York City outbreak, Mallon had allegedly infected approximately a dozen other individuals with typhoid fever between 1900 and 1907.[3] But by doing so, she also spurred the evolution of modern epidemiology as a discipline in the United States.[4]

Just as Mallon's transmissions of typhoid fever revealed the need for a rigorous study of epidemiology in the U.S., so too do the relentless security compromises of public and private sector organizations today signal the need to revisit our current legal paradigms for computer intrusion. Our traditional criminal law paradigms have proven inadequate to stem the tide of computer intrusion crimes in the U.S. In particular, a fatal flaw in the law lies in a conceptual disconnect: our existing approach to computer intrusion and our attempts at encouraging prophylactic security conduct to prevent malware infections are not effectively working in tandem.

Specifically, our definitive computer intrusion statute, the Computer Fraud and Abuse Act ("CFAA"), belies its last-century crafting, as it strains under the new threat vectors leveraged by this century's formidable attackers. Thousands of pages of jurists' opinions and scholars' law review articles have pointed out the CFAA's doctrinal limitations and struggled to interpret the statute's core provisions.[5] The

2. *See Principles of Epidemiology in Public Health Practice*, *Third Edition*, CTRS. FOR DISEASE CONTROL & PREVENTION (May 18, 2012), https://www.cdc.gov/ophss/csels/dsepd/ss1978/lesson1/section10.html [https://perma.cc/A3AS-NUX8]; *see also Typhoid Mary*, ENCYCLOPEDIA BRITANNICA, https://www.britannica.com/biography/Typhoid-Mary [https://perma.cc/X6LN-TMU9].

3. *See Typhoid Mary*, *supra* note 2.

4. *Id.*

5. *See, e.g.*, Mark A. Lemley, *Place and Cyberspace*, 91 CALIF. L. REV. 521, 528–29 (2003) (distinguishing cases where "courts forgot that the information at issue in these cases is a public good to which we have never applied the 'inviolability' rules of real property" from "true cases of unauthorized access, in which crackers exploit software bugs to gain access to a computer system or part thereof that the owner never intended to open to the outside world"); Michael J. Madison, *Rights of Access and the Shape of the Internet*, 44 B.C. L. REV. 433, 436 (2003) (arguing that "CFAA cases so far suggest that courts have failed to appreciate the depth and complexity of the Internet-as-place metaphor, particularly in light of how users actually experience places on the Internet").

CFAA has generated heated policy debate,[6] circuit splits,[7] and much public outcry,[8] but, alas, none of the attempted solutions have successfully remedied its flaws over thirty years' time.

This Article admits defeat. It argues that the CFAA as currently written is unsalvageable and thus requires a rewrite of its core provisions. Then, shifting paradigms to an approach driven by principles from computer security and epidemiology theory, this Article offers an attempted rewrite of the CFAA in a manner more attuned to the current security reality.

Part II explains three core problems plaguing current CFAA interpretation — "double whammy" conduct, doctrinal swapping, and contagion. Part III offers an entirely new paradigm — the Computer Intrusion and Abuse Act ("CIAA"). Borrowing lessons from the field of computer security and epidemiology theory, the CIAA eliminates the CFAA's undefined core terms of "authorized access" and "exceeding authorized access" and replaces them with a three-pronged approach that assesses: (1) the existence of technologically demonstrable harms, i.e., impairment of the computer security properties of confidentiality, integrity, and availability; (2) the intent of the alleged intruder; and (3) the consent of the system or machine owner. The new CIAA approach then further buttresses protection for security research with an affirmative defense. Part III also advocates for the elimination of the current civil provisions of the CFAA, returning the new statute to the CFAA's original exclusively criminal statutory form. Finally, Part III advocates for the creation of three targeted CIAA provisions: one addressing criminal impersonation using a credential, one addressing violations by government employees in positions of trust, and one addressing epidemic malware. It ends with a series of hypotheticals demonstrating how the statute would function in practice. Part IV concludes.

---

6. *Computer Fraud And Abuse Act Reform*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/cfaa [https://perma.cc/5KU7-5YDS]; Kashmir Hill, *Even New York Times Is Oblivious To Fact That Sharing 'HBO Go' Passwords To Watch 'Game Of Thrones' Breaks Law*, FORBES (Apr. 10, 2013, 4:08 PM), https://www.forbes.com/sites/kashmirhill/2013/04/10/news-flash-all-you-people-sharing-hbo-go-passwords-to-watch-game-of-thrones-are-breaking-the-law/#25560e2a413d [https://perma.cc/AA5L-S5KT].

7. *The Computer Fraud and Abuse Act: Circuit Split and Efforts to Amend*, BERKELEY TECH. L.J. BLOG (Mar. 31, 2014), http://btlj.org/2014/03/the-computer-fraud-and-abuse-act-circuit-split-and-efforts-to-amend/ [https://perma.cc/PW2B-NBGD].

8. Justin Peters, *Congress Has a Chance to Fix Its Bad "Internet Crime" Law*, SLATE (Apr. 24, 2015, 5:47 PM), http://www.slate.com/articles/technology/technology/2015/04/aaron_s_law_why_it_s_needed_to_fix_the_horrendously_bad_cfaa.html [https://perma.cc/NV8W-CNEF].

II. DEBUGGING REQUIRED: THE LIMITATIONS OF THE COMPUTER FRAUD AND ABUSE ACT

The first prosecution under the CFAA[9] was the case of Robert Morris Jr. In 1988, Morris, a graduate student at MIT, lost control of a worm[10] he had created as a proof of concept.[11] While Morris intended his worm to self-replicate across systems by exploiting a security vulnerability,[12] he had made an unfortunate mathematical error that resulted in a bug: the worm self-replicated at a disastrously fast rate.[13] Much like Typhoid Mary's infections, Morris' worm caused unintended harm. It substantially slowed down approximately ten percent of the (admittedly few) machines on the Internet at the time — machines whose availability was negatively impacted because the worm usurped their computing power.[14] Thus was born the first known self-replicating malware and the first CFAA prosecution — with an infection and a bug.[15]

During the thirty years since the Morris worm, both the reach of the Internet and the sophistication of attacks have substantially expanded. So too have the types of cases brought under the CFAA. Yet, despite Congress's best intentions, the statute and its subsequent case law have, unfortunately, aged suboptimally. Three problems in particular have arisen: the problem of "double whammy" conduct, the problem of doctrinal swapping, and the problem of contagion.

---

9. The CFAA was originally enacted in 1984 as the Counterfeit Access Device and Computer Fraud and Abuse Act, Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190 (1984). The act was aimed at "hackers who accessed computers to steal information or to disrupt or destroy computer functionality . . . ." LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1130–31 (9th Cir. 2009) (citing H.R. Rep. No. 98-894, at 8–9 (1984), reprinted in 1984 U.S.C.C.A.N. 3689, 3694). The original legislation protected government and financial institution computers and made it a felony to access classified information in a computer "without authorization." Counterfeit Access Device and Computer Fraud and Abuse Act § 2102(a). Two years later in 1986, Congress amended the statute to "deter[] and punish[] certain 'high-tech' crimes," and "to penalize thefts of property via computer that occur as part of a scheme to defraud," S. Rep. No. 99-432, at 4, 9 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2482, 2486–87. The amendment expanded the CFAA's protections to private computers. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 2(g)(4), 100 Stat. 1213.

10. *See* KATIE HAFNER & JOHN MARKOFF, CYBERPUNK: OUTLAWS AND HACKERS ON THE COMPUTER FRONTIER 253–261 (1991).

11. *Id.*; *see also Top 10 worst computer viruses*, TELEGRAPH (July 12, 2018, 11:13 AM), https://www.telegraph.co.uk/technology/5012057/Top-10-worst-computer-viruses-of-all-time.html/ (last visited May 11, 2019).

12. HAFNER & MARKOFF, *supra* note 10.

13. *Id.*

14. *Id.*

15. While the Morris worm was the first documented self-replicating worm, the 1987 Christmas Tree EXEC was the first widely disruptive computer worm, though it required user interaction. *See Christmas Tree EXEC*, WIKIPEDIA, https://en.wikipedia.org/wiki/Christmas_Tree_EXEC/ [https://perma.cc/7LGU-W9J6]. Worms appeared in science fiction in the early 1970's. *See generally* DAVID GERROLD, WHEN HARLIE WAS ONE (1972).

Recurring doctrinal limitations have confused courts, defendants, and legal scholars alike, and the broad scope of the CFAA has begun to erode the traditional boundaries between criminal law and contract[16] — a problem that might be known as the problem of "double whammy" conduct. Moreover, because the statute's civil and criminal case law has been used interchangeably by courts, civil litigants' frivolous CFAA civil claims can cause criminal law doctrine "creep" as courts use CFAA criminal and civil precedent interchangeably. This dynamic of judicial use of CFAA civil and criminal precedent as equally precedential for each other might be called the problem of doctrinal swapping. Doctrinal swapping has begun to impact potentially both innovation and national security negatively. Finally, as attacks and malware are becoming progressively more virulent and contagious, the CFAA does not provide adequate statutory authority and oversight in situations where public-private cooperation is required to stop ongoing attacks — the problem of contagion. These three concerns are discussed in the sections that follow.

A. The Problem of "Double Whammy" Conduct: Doctrinal Limitations

A focal point of the CFAA's interpretational uncertainty involves two primary areas: first, the statute's two core terms of "without authorization" and "exceeding authorized access" — terms that are never expressly defined in the CFAA — and, second, the statute's relationship to contract law. This uncertainty, in turn, has led courts to identify vagueness concerns and has triggered the undesirable blending of criminal law principles with those of contract breach doctrines.

1. Void for Vagueness

One of the main and longstanding criticisms of the CFAA is that, due to a number of amendments added over time, it has become "extraordinarily broad" — so broad that, as applied in certain circumstances, it may violate the void for vagueness doctrine.[17] Rooted in the Due Process Clause, the void for vagueness doctrine addresses two concerns: (1) providing fair notice of what activity the law criminalizes and

16. Andrea M. Matwyshyn, *The Law of the Zebra*, 28 BERKELEY TECH. L.J. 155, 159 (2013).

17. Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1561–62 (2010).

(2) establishing minimum guidelines for law enforcement so that statutes are not applied with discriminatory intent.[18]

Applications of the CFAA can raise void for vagueness concerns due to a combination of vague language meant to define the statute's core concepts of criminality coupled with a jurisdictional reach that essentially covers *any* computer or networked device in the world.[19] Violations of the CFAA often concern accessing a protected computer "without authorization" or accessing a protected computer in a way that "exceed[s] authorized access."[20] As previously noted, the CFAA does not define what it means to access a computer without authorization or to access a computer with authorization. Moreover, the definition of what it means to "excee[d] authorized access" is dependent on an understanding of what it means to access a computer with authorization: "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 accessor is not entitled so to obtain or alter."[21] These undefined or ill-defined core concepts of criminality apply to activity taken on *any* computer "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."[22]

Perhaps the clearest illustration of how the CFAA, as applied, can raise void for vagueness concerns arises when a breach of the terms of service by a consumer — a contract breach — becomes criminalized under the CFAA. The seminal case on point is *United States v. Drew*.[23] In *Drew*, Lori Drew, an adult, created a fictitious profile on Myspace, pretending to be a sixteen-year-old boy, Josh Evans, and communicated

18. *Id.* at 1573. "The void-for-vagueness doctrine has two prongs: 1) a definitional/notice sufficiency requirement and, more importantly, 2) a guideline setting element to govern law enforcement." United States v. Drew, 259 F.R.D. 449, 461 (C.D. Cal. 2009).

19. Kerr, *supra* note 17, at 1571, 1577–78. The statute defines computer as "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 does not include "an automated typewriter or typesetter, a portable hand held calculator, or other similar device." 18 U.S.C. § 1030(e)(1) (2012). Perhaps the only modern device that may be excluded from this definition, Kerr argues, is a calculator — and it would need to be one that does not contain a chip that could connect it to the Internet. Kerr, *supra* note 17, at 1571.

20. 18 U.S.C. § 1030(a)(1).

21. *Id.* § 1030(e)(6).

22. *See id.* § 1030(e)(2)(B) (definition of "protected computer"). As Professor Kerr explains, the phrase "'in or affecting interstate commerce' is a term of art that signals congressional intent to cover as far as the Commerce Clause will allow . . . every computer anywhere in the world that could be regulated under the Commerce Clause is within the purview of the CFAA." Kerr, *supra* note 17, at 1571.

23. 259 F.R.D. 449 (C.D. Cal. 2009).

with a thirteen-year-old girl named Megan Meier, who had been a classmate of Drew's daughter.[24] Following flirtatious communications between Evans and Meier over a number of days, Evans told Meier that he was moving away, that he no longer liked her, and that "the world would be a better place without her."[25] Meier then committed suicide.[26]

The government's theory of prosecution under the CFAA focused on Drew's creation of the Josh Evans profile, which violated the Myspace terms of service. Specifically, the terms required (among other things) that all registration information submitted when setting up a profile must be accurate, that Myspace users not solicit personal information from anyone under the age of eighteen, and that users cannot post and use the photograph of another person without his or her consent.[27] The government argued that because Drew's conduct violated these contract terms, Drew's access was either "without authorization" or "in excess of authorization."[28]

Following the jury's conviction of Drew for two misdemeanor CFAA violations, the district court set aside the jury's verdict, finding violations of both elements of the void for vagueness doctrine: "the conscious violation of a website's terms of service runs afoul of the void-for-vagueness doctrine . . . because of the absence of minimal guidelines to govern law enforcement"[29] and "because of actual notice deficiencies."[30] Indeed, "if every [terms of service] breach qualifies" as a CFAA violation, then there is absolutely no limitation on what kind of breaches should merit criminal prosecution.[31] Moreover, the notice deficiencies would turn otherwise innocent Internet users into criminals[32] — all could be prosecuted and law enforcement entities would be improperly free "to pursue their personal predilections."[33]

Notwithstanding the void for vagueness problem in the *Drew* case, the court did not dismiss the fact that "an intentional breach of the

24. *Id.* at 452.
25. *Id.*
26. *Id.*
27. *Id.* at 454.
28. *Id.* at 461.
29. *Id.* at 464. If the terms of service govern "authorization" and thus whether an individual's access is criminal under the CFAA, the statutory provision "would be unacceptably vague because it is unclear whether any or all violations of terms of service will render the access unauthorized, or whether only certain ones will." *Id.* "If *any* violation of *any* term of service is held to make the access unauthorized," the statutory provision would be overbroad for failing to "set[] guidelines to govern law enforcement." *Id.* at 465.
30. *Id.* at 464 (noting that the CFAA has not "'criminalized breaches of contract' in the context of website terms of service," and that ordinary people "would not expect criminal penalties" for violating contractual provisions (citations omitted)).
31. *Id.* at 466.
32. Kerr, *supra* note 17, at 1581.
33. *Drew*, 259 F.R.D. at 463 (internal citations omitted).

[terms of service] can potentially constitute access without authorization or excess of authorization under the [CFAA]."[34] In other words, a breach of contract could, in other situations where there are no void for vagueness concerns, provide the basis for a prosecution under the CFAA.[35] Concern over this possibility has animated much critique from the technology builder and breaker communities.[36] This undesirable situation where the conduct that constitutes a contract breach morphs into the basis for both a civil claim and criminal charge under the CFAA might be called the problem of "double whammy" conduct.

2. Damaging Contract

The CFAA's problem of "double whammy" conduct arises in part from an open circuit split with respect to whether a mere breach of contract should constitute the basis for a CFAA claim and criminal charge.[37] As explained by one of us in prior work, when pedestrian breach of contract claims potentially become CFAA civil claims and chargeable as criminal offenses under the CFAA, the traditional boundary between contract law and criminal law is violated.[38]

---

34. *Id*. at 461.

35. *See* Facebook v. Power Ventures and Vachani, 844 F.3d 1058, 1062 (9th Cir. 2016) (holding that a continued violation of an end user license agreement can form the basis for a violation of the CFAA after a cease and desist letter is received).

36. Kim Zetter, *The Most Controversial Hacking Cases of the Past Decade*, WIRED (Oct. 26, 2015, 7:00 AM), https://www.wired.com/2015/10/cfaa-computer-fraud-abuse-act-most-controversial-computer-hacking-cases/ [https://perma.cc/72YT-E2CF]; Ted Samson, *CFAA: Where the computer security law is broken*, INFOWORLD (Apr. 10, 2013), https://www.infoworld.com/article/2614067/federal-regulations/cfaa--where-the-computer-security-law-is-broken.html [https://perma.cc/CM3B-KYD8].

37. In both the civil and criminal context, some courts have found that a mere breach of contract can provide the basis for a CFAA violation and some have not. *Compare* Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 418 (7th Cir. 2006) (finding civil liability under the CFAA for an ex-employee arising out of an employment agreement and an implicit duty of loyalty), United States v. Rodriguez, 628 F.3d 1258, 1260 (11th Cir. 2010) (upholding CFAA conviction of employee who accessed social security databases for non-employment purposes), *and* United States v. John, 597 F.3d 263, 271 (5th Cir. 2010) (distinguishing Brekka's interpretation of exceeds authorized access and upholding CFAA conviction of authorized computer user who has "reason to know" that access to data "in furtherance of a criminally fraudulent scheme" is "not authorized access") *with* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009) (declining to follow Citrin where employee had permission to access employer documents), WEC Carolina Energy Solutions v. Miller, 687 F.3d 199, 206 (4th Cir. 2012) (holding no CFAA liability in connection with an alleged violation of an acceptable use policy), *and* United States v. Nosal, 676 F.3d 854, 862 (9th Cir. 2012) (en banc) (identifying danger of using terms of service violations as basis for CFAA claims). *See also Power Ventures and Vachani*, 844 F.3d at 1062 (holding that a continued violation of an end license user agreement can form the basis for a violation of the CFAA after a cease and desist letter is received). The overarching concern is that where a court finds a basis for a meritorious civil claim under the CFAA due to a mere breach of contract, this analysis may then be subsequently used in criminal CFAA caselaw reciprocally.

38. Matwyshyn, *supra* note 16, at 159.

While it could be argued that civil claims under the CFAA in theory conceptually map to contract law damages claims because both potentially result in monetary transfers, such an analysis misunderstands the nuance of contract law and the potential harms to innovation caused by a heavy-handed interpretation of the CFAA.[39] Indeed, turning every technology-mediated contract breach into a possible CFAA claim potentially negates hundreds of years of contract law's doctrinal evolution on matters of public policy unenforceability,[40] adequacy of notice and process in formation,[41] unconscionability,[42] *contra proferentem*,[43] bilateral consent requirements for amendment,[44] and numerous other consumer protection doctrines prominent in contract law.[45]

But when the conversion from a breach of contract results in a criminal CFAA prosecution, the problem of "double whammy" conduct becomes most stark and does violence to traditional contract law principles.[46] Contract claims and criminal charges differ materially in their burden of proof and, perhaps most significantly, in their possible consequences for defendants.[47] Contract law arises from fundamentally different policy drivers than criminal law.[48] It usually reflects a Holmesian "Bad-Man" theory of law — that is, one that in most instances allows room for the violation of contract promises provided the non-breaching party is subsequently made financially whole for losses arising from the breach.[49] Criminal prosecutions address transgressions against the state and violations of social order; contract remedies, by contrast, simply seek to resolve private ordering failures between two

39. *Id.* at 176 (discussing "digital peonage" concerns and the right to exit employment contracts).

40. 5 RICHARD A. LORD, WILLISTON ON CONTRACTS § 12:1–3 (4th ed. Supp. 2018).

41. 1 RICHARD A. LORD, WILLISTON ON CONTRACTS § 4:16 (4th ed. Supp. 2018).

42. 8 RICHARD A. LORD, WILLISTON ON CONTRACTS § 18:1 (4th ed. Supp. 2018).

43. 11 RICHARD A. LORD, WILLISTON ON CONTRACTS § 32:12 (4th ed. Supp. 2018).

44. 30 RICHARD A. LORD, WILLISTON ON CONTRACTS § 75:7 (4th ed. Supp. 2018).

45. Matwyshyn, *supra* note 16, at 171 (discussing gaming in digital contract presentation and content).

46. *Id.* at 178 (discussing how the current CFAA civil provisions impinge on preservation of traditional contract remedies).

47. *Id.* at 177 ("[I]n the Peonage Cases, the U.S. Supreme Court invalidated laws that criminalized breach of employment contracts. As the Peonage Cases attest, threatened criminal prosecution for breach of contract, in particular, chills exit: employees would be worried to leave their employment for fear of losing their liberty in the process.").

48. While criminal law seeks to punish defendants for transgressions with the possibility of incarceration, contract law is driven by a compensatory, not a punitive, ethos. *See* 22 AM. JUR. 2D Damages § 574. ("[P]unitive damages are not ordinarily recoverable in actions for breach of contract because: (1) the damages for breach of contract are generally limited to the pecuniary loss sustained; and (2) the purpose of punitive damages is not to remedy private wrongs but to vindicate public rights.").

49. Matwyshyn, *supra* note 16, at 202 ("[The] economics notion of efficient breach, as well as this Holmesian 'bad man' notion — i.e. one which views breach as a viable option provided one pays damages arising therefrom — view a contractual promise [as] being no more than an option to breach and pay damages.").

parties.[50] In other words, in a world where the breach of an agreement may provide the basis for a criminal charge, the traditional contract theory notion of an "efficient breach" becomes functionally eviscerated.[51] There is no traditional contract law efficiency calculus that involves risking a felony or misdemeanor conviction and an accompanying prison term.[52] Indeed, contract law includes specific doctrines disallowing enforcement of agreements that violate laws and public policy, rendering a "criminal breach" a modern CFAA anachronism.[53] Thus, the two regimes of contract and criminal law sit squarely in conflict on key structural elements, and an undesirable balkanization of contract law around technology contracting situations is developing because of the CFAA and the "double whammy" problem.[54]

Let us analyze a concrete agreement in light of the problem of "double whammy" conduct: the Facebook terms of use. Turning first to contract law, the contract argument in favor of strict enforcement of the Facebook terms of use argues that when consumers click yes on the terms of use of the website, they consent to be governed by those terms, which were reviewable prior to clicking yes. In practice, the situation is decidedly more complicated. Professor Margaret Radin has argued that "the growing modularity of contracts and the waning of consent as the normative basis of legal enforcement" threatens the traditional contract law landscape.[55] Similarly, Professor Woody Hartzog has argued that "website features and design should, in some contexts, be considered enforceable promises."[56] Also, one of us has argued that, as end

---

50. Steven Shavell, *Why Breach of Contract May Not Be Immoral Given the Incompleteness of Contracts*, 107 MICH. L. REV. 1569, 1569 (2009) ("[Although it is a] widely held view that breach of contract is immoral . . . breach may often be seen as moral, once one appreciates that contracts are incompletely detailed agreements and that breach may be committed in problematic contingencies that were not explicitly addressed by the governing contracts.").

51. Matwyshyn, *supra* note 16, at 201–02.

52. *Id.* at 206 ("[A] lone inventor who breaches an agreement may find himself facing computer intrusion charges and potentially prison, but a corporation that breaches an agreement faces no incarceration risk under the CFAA.").

53. Traditionally, courts have sometimes been willing to set aside contracts where the subject matter of the agreement directly violates law or, even if no statute exists on point, courts have been willing to derive policy from statutes related to the topic of the contract and/or formulate policy based on a court's own social/legal norms. *See, e.g.*, Bovard v. Am. Horse Enters., 247 Cal. Rptr. 340, 343–45 (Cal. Ct. App. 1988). Whether a contract is contrary to public policy is a question of law to be determined from the circumstances of the particular case. *Id.* at 343. In *Bovard*, for example, the court explained that "[b]efore labeling a contract as being contrary to public policy, courts must carefully inquire into the nature of the conduct, the extent of public harm which may be involved, and the moral quality of the conduct of the parties." *Id.* at 344. For a discussion of public policy doctrine in contract law, *see generally* David Adam Friedman, *Bringing Order to Contracts Against Public Policy*, 39 FLA. ST. U. L. REV. 563 (2012).

54. Matwyshyn, *supra* note 16, at 165 ("[T]he result of this [CFAA] confusion is a slow but steady balkanization of contract law.").

55. Margaret Jane Radin, *Boilerplate Today: The Rise of Modularity and the Waning of Consent*, 104 MICH. L. REV. 1223, 1223 (2006).

56. Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635, 1638 (2011).

user license agreements ("EULAs") become progressively more one-sided in favor of drafters, the traditional contract law balance between companies and consumers disappears and should be bolstered through statutorily-implied promises.[57] Contracts of adhesion such as today's terms of use have always given contract scholars pause and cause for concern due to their lack of negotiability.[58]

But, aside from these doctrinal contract law concerns, the technological reality of only limited "reviewability" of many terms of use also illustrates the problem of CFAA "double whammy" conduct. Returning to the Facebook terms of use, imagine that a user wishes to create a Facebook account but first attempts to review all the relevant terms of use. While this undertaking may seem a reasonable burden for an average user in theory, the experienced reality of the exercise — time and burden required for this task in practice — is herculean even for legally-trained readers. A review of Facebook's terms plunges the user into a labyrinth of linked sets of terms incorporated by reference, creating an experience that might bring to mind a metaphor of being lost in Borges' fictional library of all books.[59] Even a legally-trained reader will often leave the experience without certainty of having reviewed the complete universe of terms, unclear on whether all links have been followed and confused by whether some text constituted merely precatory guidance or binding terms.[60] Concretely, in order for a consumer to review the entirety of Facebook's terms of use and all policies incorporated by reference[61] that will govern the user's relationship with both Facebook

57. *See generally* Andrea M. Matwyshyn, *Privacy, the Hacker Way*, 87 S. CAL. L. REV. 1 (2013) (arguing in favor of creating a set of nonwaivable statutorily-implied privacy and security promises in all end user license agreements). An implied promise is a promise inferred to exist in any agreement of a certain type, regardless of the expressed language of an agreement. Implied promises may either be waivable or non-waivable as determined by law. For example, it is a statutorily implied term of every lease agreement that a landlord cannot turn the heat off if a tenant is late with rent in most jurisdictions. *See id.* at 57 & n.247.

58. Radin, *supra* note 55, at 1223.

59. Jorge Luis Borges, *The Library of Babel*, *in* LABYRINTHS: SELECTED STORIES AND OTHER WRITINGS 51, 54–55 (Donald A. Yates & James E. Irby eds., trans., 2007) ("it was proclaimed that the Library contained all books").

60. Personal experience of one of the authors.

61. For example, a user who registered on or around to May 7, 2018 seeking to evaluate the terms of Facebook's handling of her data (and seeking to understand how her agreement has been unilaterally amended by Facebook across time) would need to review the following agreements and their incorporated terms: Facebook Advertising Policies, Commerce Product Merchant Agreement, Cookie Consent Guide, Copyright FAQ, CrowdTangle, Inc. Privacy Policy, CrowdTangle, Inc. Terms of Service, Custom Audiences Terms, Customer Support Policy, Facebook Cookies & Other Storage Technologies (current), Facebook Privacy Shield Agreement, Facebook Terms (new), Facebook Terms (old), Facebook U.S. Data Use Policy (new), Facebook Data Policy (old), Facebook Payments International Limited Privacy Policy, Facebook Payments Inc. Privacy Policy, Facebook Payments Terms (new), Facebook Platform Policy, Information for Child-Directed Sites and Services, Instagram Data Policy (new), Instagram Terms of Use (new), Instagram Terms of Use (old), Instagram Privacy Policy (old), Masquerade Privacy Policy, Masquerade Technologies, Inc. Terms of Service, Messenger Brand Guidelines, Moves Terms of Use, Moves App Privacy Policy, Oculus (new) Terms of

and its various affiliated entities (i.e. the entities with whom Facebook reserves the right to share consumer data), an average consumer[62] who reads at a rate of approximately 200 words a minute would likely need to spend approximately *ten hours* reviewing Facebook's user agreements.[63] Putting aside the question of whether an average reader even has the capacity to understand legalistic contract terminology such as notions of indemnification, choice of law, and choice of forum, the length of these documents (and the extent of incorporation by reference) likely renders this contract review an insurmountable burden to an average person. It also raises serious doubts as a matter of traditional contract law analysis regarding the enforceability of this complex lattice of Facebook's EULAs and other similar contracts of adhesion, particularly when drafters allege them to be unilaterally amendable at any time. Thus, the problem of "double whammy" conduct becomes even more troubling. Yet, in some circuits, the unreasonable burden of comprehending (and vigilantly monitoring unilateral amendments to) such lengthy agreements is necessary: without reading the agreements in their entirety, a user may inadvertently breach the contract and potentially trigger criminal consequences under the CFAA.

But, perhaps most notably, "double whammy" conduct is also fundamentally unnecessary: even assuming arguendo that we subscribe to the interpretation that these user agreements are enforceable in whole or in part, contract law already provides recourse for any material breach of such an agreement. The CFAA serves no necessary or unique function in making an allegedly harmed party whole — contract law amply addresses those questions. Indeed, overzealous indirect contract enforcement with the heavy hammer of the civil (and criminal) remedies of CFAA almost always provides merely a redundant bite at the proverbial contract apple, sometimes in ways that contract law has specifically sought to minimize or prohibit. Therefore, the potential impact of this circuit split on whether a mere breach of contract should constitute the basis for a CFAA claim and criminal charge is profound, as almost all private ordering in technology-mediated commerce occurs through contracts.

Service, Current Oculus Privacy Policy (effective until May 20, 2018), New Oculus Privacy Policy (effective until May 20, 2018), Onavo Privacy Policy, Onavo Terms of Service, Promotions Guidelines, Sales Policy, Self-Serve Ad Terms (new), Self-Serve Ad Terms (old), Trademark FAQ, WhatsApp — All Legal Info — Non-European Region.

62. Even Chief Justice Roberts has admitted that he does not read such user agreements. *Chief Justice John Roberts Doesn't Read EULAs Either*, INFO. LAW INST. STUDENT BLOG, (Oct. 24, 2010, 4:01 PM), https://blogs.law.nyu.edu/privacyresearchgroup/2010/10/chief-justice-john-roberts-doesnt-read-eulas-either/ [https://perma.cc/8UJN-TR25].

63. Ten hours is a conservative estimate. Because of the extent of incorporation by reference, linking to other agreements, and the extent of default data sharing among Facebook-owned entities, on or around May 7, 2018, a consumer would need to review at least approximately 125,000 words of contracts.

However, a secondary problem exacerbates the CFAA "double whammy" conduct problem: the judicial practice of interchangeably interpreting civil and criminal CFAA precedents. As Professor Kerr explains, "the usual rule [is] that civil precedents apply to criminal cases . . . [and] these cases threaten a dramatic and potentially unconstitutional expansion of criminal culpability in cyberspace."[64] Thus, this problem of doctrinal swapping amplifies the negative consequences of the problem of CFAA "double whammy" conduct. That is, expansive CFAA use in civil cases simultaneously pushes the boundaries of CFAA application in criminal cases in more aggressive directions. As the next section explains, when these two problems of CFAA, "double whammy" conduct and doctrinal swapping, work in tandem, they threaten to damage not only contract law but also our innovation-based economy and our national security.[65]

B. The Problem of Doctrinal Swapping: Harms to Innovation and National Security

The vast majority of CFAA legal literature has focused on the criminal side of CFAA enforcement. But, an equally important and underexplored set of impacts relates to innovation policy. Indeed, the CFAA problems of "double whammy" conduct and doctrinal swapping raise the specter of hindering employee mobility, limiting technology-mediated business models, and chilling security research, which in turn impacts national security.

Specifically, the impact of CFAA "double whammy" conduct and doctrinal swapping potentially changes the calculus for employees who wish to leave their current employer in favor of a new place of work or in favor of starting their own companies. Fearing retribution in criminal law for an alleged civil transgression of an employee handbook technology use policy or other breach of contract, employees may alter their analysis of a job change decision.[66] Similarly, data aggregation enter-

---

64. Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1599 & n.14 (2003) ("The courts generally apply civil precedents in the criminal context unless there is evidence that Congress did not intend the same standard to govern." (citing United States v. Bigham, 812 F.2d 943, 948 (5th Cir. 1987))).

65. See discussion *infra* Part II.B.

66. Employees may also fear being "blacklisted" among shared contacts and future employers, a phenomenon that some employees and contractors allege to occur. *Employment Blacklists*, THE FORMER AND CURRENT EMPLOYEES (FACE) OF AMAZON, https://sites.google.com/site/thefaceofamazon/home/employment-blacklists [https://perma.cc/77UA-XUV9]. Professor Orly Lobel argues that many companies use aggressive restrictions of their own talent and secrets in a type of "control mentality." *See generally* Orly Lobel, TALENT WANTS TO BE FREE: WHY WE SHOULD LEARN TO LOVE LEAKS, RAIDS, AND FREE RIDING (2013). This control mentality may also encourage litigiousness

prises that scrape publicly-viewable information may hesitate to recombine and present these facts in new and useful ways[67] because of the risk of a contract breach being converted into a criminal CFAA charge.

Even when courts such as the Ninth Circuit craft protective rules to benefit employees, the ability of employees to govern their conduct based on interpretation and analogies between the facts of particular cases and their own future conduct is limited. For example, on this point of employee mobility and new business models, let us briefly examine two cases that illustrate the problems of "double whammy" conduct and doctrinal swapping (and which have triggered countless hours of debate among jurists and legal academics) — the cases known as *Nosal I* and *Nosal II*.

In *Nosal I*,[68] David Nosal, an ex-employee of an executive recruiting firm, was charged with violating the CFAA on the basis of inducing current employees of the firm to use their corporate access credentials to obtain information from a proprietary database (and share the information with him) in violation of the company's computer use policy.[69] The prosecution alleged that the violation of this corporate policy constituted exceeding authorized access and thus provided the basis for a felony charge under the CFAA.[70] However, the Ninth Circuit disagreed with the prosecution's theory and held that inducing someone to access a workplace computer in violation of corporate policy did not constitute a CFAA violation.[71] Nevertheless, in *Nosal II*,[72] the Ninth Circuit decided that when David Nosal or his co-conspirators *themselves* used the login credentials of a current employee to directly gain unauthorized access to proprietary information of their former employer,[73] this act

against employees who have left the company and potentially possess inside knowledge. For example, trade secret disputes might easily morph into CFAA civil disputes if the allegedly protectable information was stored digitally.

67. *See, e.g.*, Feist Commc'ns v. Rural Tel. Serv. Co., 499 U.S. 340 (1991) (balancing interests of copyright holders as aggregators of information and availability of public information generally by establishing a "modicum of creativity" standard). Again, much like contract law, the primary body of law that would cover the permissibility of such aggregation, copyright law, has spent hundreds of years crafting countervailing doctrines to enable fact aggregation and recombination into new presentations that demonstrate a modicum of creativity. For an example of a criminal prosecution of scraping and aggregating data, see United States v. Auernheimer, 748 F.3d 525, 534 n.5 (3d Cir. 2014).

68. United States v. Nosal (*Nosal I*), 676 F.3d 854 (9th Cir. 2012) (en banc).

69. *Id.* at 856.

70. *Id.* at 857.

71. *Id.* at 864.

72. United States v. Nosal (*Nosal II*), 828 F.3d 865 (9th Cir. 2016).

73. Although the court does not explain the distinction between password sharing by an employee and password sharing by a consumer in this manner, a distinction can, in fact, be made based on the intended beneficiary of the password's usage. With a consumer password for a video streaming service, for example, the consumer pays for the password to benefit herself. In the employment situation, the employer pays the employee to use the password to benefit the employer, and an assistant lacks the apparent authority to sublicense a password to a third party on behalf of the company. For a discussion of apparent authority, see

constituted a violation of the CFAA.[74] Affirming Nosal's conviction, the Ninth Circuit found that Nosal, knowingly and with intent to defraud, accessed a protected computer without authorization in violation of the CFAA.[75] The case has led to confusion among observers,[76] particularly as juxtaposed against *Facebook v. Power Ventures, Inc.*,[77] a civil CFAA case involving traffic redirection and shared credentials,[78] and *hiQ Labs, Inc. v. LinkedIn Corp.*,[79] a civil CFAA case seeking to prevent a website from implementing technological protections against scraping.[80] Thus, *Nosal II* potentially further exacerbated the definitional ambiguities of the CFAA because of the problems of "double whammy" conduct and doctrinal swapping.[81]

Finally, the CFAA's problems of "double whammy" conduct and doctrinal swapping can chill security research disclosures. Upon receiving researchers' reports of security vulnerabilities in their products or

---

RESTATEMENT (FIRST) OF AGENCY: APPARENT AUTHORITY § 8 (1933). *See also* Note, *Inherent Power as a Basis of a Corporate Officer's Authority to Contract*, 57 COLUM. L. REV. 868, 868 (1957).

74. *Nosal II*, 828 F.3d at 870.

75. *Id.*

76. Criminal Law — Computer Fraud and Abuse Act — Ninth Circuit Affirms Conviction of a Former Employee Who Used Another Employee's Password, 130 HARV. L. REV. 1265, 1268–69 (2017); Eric Goldman, *Catching Up on Ninth Circuit CFAA Jurisprudence (Internet Law Casebook Excerpt)*, TECHNOLOGY & MARKETING LAW BLOG (Sept. 4, 2017), https://blog.ericgoldman.org/archives/2017/09/catching-up-on-ninth-circuit-cfaa-jurisprudence-internet-law-casebook-excerpt.htm [https://perma.cc/35MW-LDEN] ("[T]he courts' statutory construction remains highly confused and confusing.").

77. 844 F.3d 1058 (9th Cir. 2016). *Facebook v. Power Ventures* appears to rely on an aggressive construction of privity to distinguish between contract breach and cease and desist scenarios. *Id.* at 1068–69. As explained by Professor Eric Goldman, the court said that "Power Ventures might have had implied authorization to access Facebook's service, especially given the users' requests for it to do so. However, 'Facebook expressly rescinded that permission[.]' . . . Interestingly, the court says (in a footnote) that cease-and-desist letters are more consequential than a service's technological self-help via IP address blocks." Goldman, *supra* note 76.

78. Orin Kerr, *Password-sharing case divides Ninth Circuit in* Nosal II, WASH. POST (July 6, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/07/06/password-sharing-case-divides-ninth-circuit-in-nosal-ii/ [https://perma.cc/9BV5-7G2P] (explaining the perceived conflict between *Nosal I* and *II* and *Power Ventures*).

79. 273 F. Supp. 3d 1099 (N.D. Cal. 2017).

80. As explained by Venkat Balasubramani, "[t]he fact that Judge Chen actually prevented LinkedIn from implementing technological measures, and did so relatively casually, is somewhat jaw-dropping. Does this mean that LinkedIn cannot rate-limit hiQ, or decide it wants to implement robots.txt?" Venkat Balasubramani, *LinkedIn Enjoined From Blocking Scraper-hiQ v. LinkedIn*, TECHNOLOGY & MARKETING LAW BLOG (Aug. 15, 2017), https://blog.ericgoldman.org/archives/2017/08/linkedin-enjoined-from-blocking-scraper-hiq-v-linkedin.htm [https://perma.cc/4SJZ-H8EQ]. Balasubramani continued, "[t]he court alludes to the fact that LinkedIn had been 'tolerating' hiQ's access for 'years.' Unfortunately, the ruling does not provide many additional details about this and this fact also does not figure centrally into the ruling, although it undoubtedly influenced the court's view of the equities." *Id.*

81. *Id.*; *see also* Orin Kerr, *9th Circuit: It's a federal crime to visit a website after being told not to visit it*, WASH. POST (July 12, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/07/12/9th-circuit-its-a-federal-crime-to-visit-a-website-after-being-told-not-to-visit-it/?utm_term=.8f6bbdb51585 [https://perma.cc/44NQ-2CW5].

services, companies have sometimes responded with threats of civil and criminal CFAA consequences.[82] While sophisticated companies recognize that this strategy fails in the long term and embrace external reports as a feedback loop,[83] not all companies respond amenably when apprised of unsafe coding flaws by outsiders.[84] Indeed, some particularly aggressive companies have begun to threaten not only security researchers but also the journalists who report on such security vulnerabilities.[85] Yet, the need to (avoid and) remediate security flaws is stark. Uncorrected security vulnerabilities in the private sector often result in national security consequences because of what one of us has called the problem of "reciprocal security vulnerability" — the technological reality that security vulnerabilities in the private sector impact the public sector and vice versa.[86] In other words, when a company wields the CFAA to quash discussion of security issues in lieu of fixing existing security vulnerabilities, it not only harms itself and the researcher but also impairs innovation policy and harms national security interests.

For example, the Mirai[87] botnet[88] took control of webcams, internet-connected DVRs and other Internet of Things ("IoT") products,

---

82. Sean Gallagher, *Man gets threats — not bug bounty — after finding DJI customer data in public view*, ARS TECHNICA (Nov. 17, 2017, 1:30 PM), https://arstechnica.com/information-technology/2017/11/dji-left-private-keys-for-ssl-cloud-storage-in-public-view-and-exposed-customers/ [https://perma.cc/W7DC-NJC4].

83. The international community of technical experts has authored two vulnerability intake and processing ISO standards on point — 29147 and 30111. *See* Int'l Org. for Standardization/Int'l Electrotechnical Comm'n, ISO/IEC 29147:2014 (Feb. 2014) (INT'L STANDARDIZATION ORG., amended Oct. 2018); Int'l Org. for Standardization/Int'l Electrotechnical Comm'n, ISO/IEC 30111:2013 (INT'L STANDARDIZATION ORG. Nov. 2013). For a description of ISO 29147 and 30111, see *Application Security Response: When Hackers Come A-Knockin — Katie Moussouris*, YOUTUBE (May 31, 2013), https://www.youtube.com/watch?v=-L3DNZtK8lc [https://perma.cc/T9PV-JMD6].

84. *See, e.g.*, Gallagher, *supra* note 82.

85. Ms. Smith, *Reporters Threatened with CFAA, Labeled Hackers for Finding Security Hole*, CSO ONLINE (May 20, 2013, 12:20 PM), https://www.csoonline.com/article/2224660/microsoft-subnet/reporters-threatened-with-cfaa--labeled-hackers-for-finding-security-hole.html [https://perma.cc/2G3R-8T27].

86. Andrea M. Matwyshyn, *CYBER!*, 2017 BYU L. REV. 1109, 1109 (2018) ("[T]he two dominant 'cybersecurity' paradigms — information sharing and deterrence — fail to recognize that corporate information security and national 'cybersecurity' concerns are inextricable. This problem of 'reciprocal security vulnerability' means that in practice our current legal paradigms channel us in suboptimal directions.").

87. Brian Krebs, *Hacked Cameras, DVRs Powered Today's Massive Internet Outage*, KREBS ON SECURITY (Oct. 22, 2016, 10:30 AM), https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/ [https://perma.cc/3LD9-QN5X] ("A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked 'Internet of Things' (IoT) devices, such as CCTV video cameras and digital video recorders, new data suggests.").

88. A botnet is a collection of internet-connected devices that is infected by malware and controlled remotely by a single attacker or group. Users are often unaware that their devices have been harnessed as part of a botnet and might be used for a range of criminal activities. Margaret Rouse, *botnet*, TECHTARGET, https://searchsecurity.techtarget.com/definition/botnet [https://perma.cc/PJ4T-3EG2].

harnessing these IoT devices to attack major websites such as Twitter and Reddit in a distributed denial of service ("DDoS") attack[89] that left the internet inaccessible on large parts of the East Coast.[90] The attack was so severe that authorities initially considered it potentially the work of a nation-state.[91] But it was not — it was a botnet of hundreds of thousands of compromised IoT products (that usually shared vulnerable components made in China)[92] carrying out a distributed denial of service attack orchestrated by three college students.[93] The Satori[94] IoT botnet has attacked cryptocurrency mining operations at scale.[95] The Reaper[96] IoT botnet and its progeny have targeted our markets and the financial services industry.[97] Meanwhile, the JenX IoT botnet appears to sell "time-share" increments to would-be attackers to attack the target of their choice for as little as $20.[98] The crisis in IoT security is swiftly escalating, and millions of vulnerable private sector devices are

89. Josh Fruhlinger, *The Mirai Botnet Explained: How Teen Scammers and CCTV Cameras Almost Brought down the Internet*, CSO ONLINE (Mar. 9, 2018, 3:00 AM), https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html [https://perma.cc/X9HX-2AZ5].

90. *Id.*

91. *Id.*

92. Eduard Kovacs, *Over 500,000 IoT Devices Vulnerable to Mirai Botnet*, SECURITY WEEK (Oct. 7, 2016), https://www.securityweek.com/over-500000-iot-devices-vulnerable-mirai-botnet [https://perma.cc/J6CR-7CEG].

93. Garrett M. Graff, *How a Dorm Room Minecraft Scam Brought Down the Internet*, WIRED (Dec. 13, 2017, 3:55 PM), https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/ [https://perma.cc/H6MJ-JT2Q].

94. *New Satori Botnet Variant Enslaves Thousands of Dasan WiFi Routers*, RADWARE (Feb. 12, 2018), https://blog.radware.com/security/botnets/2018/02/new-satori-botnet-variant-enslaves-thousands-dasan-wifi-routers/ [https://perma.cc/K4VY-YYKB].

95. *Id.*

96. Andy Greenberg, *The Reaper IoT Botnet Has Already Infected a Million Networks*, WIRED (Oct. 20, 2017, 5:45 PM), https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/ [https://perma.cc/HU49-DZXB].

97. Priscilla Moriuchi & Sanil Chohan, *Mirai-Variant IoT Botnet Used to Target Financial Sector in January 2018*, RECORDED FUTURE (Apr. 5, 2018), https://www.recordedfuture.com/mirai-botnet-iot/ [https://perma.cc/HLD6-5V7V] ("[A] Mirai botnet variant, possibly linked to the IoTroop or Reaper botnet, was utilized in attacks on at least one company, and probably more, in the financial sector in late January 2018."); Kevin Townsend, *Financial Services DDoS Attacks Tied to Reaper Botnet*, SECURITY WEEK (Apr. 5, 2018), https://www.securityweek.com/financial-services-ddos-attacks-tied-reaper-botnet [https://perma.cc/88K6-J7GA].

98. Dan Goodin, *New IoT Botnet offers DDoSes of once-unimaginable sizes for $20*, ARS TECHNICA (Feb. 1, 2018, 1:25 PM), https://arstechnica.com/information-technology/2018/02/for-sale-ddoses-guaranteed-to-take-down-gaming-servers-just-20/ [https://perma.cc/Z2GY-REYP].

ripe for exploitation. These botnets and malware can target either private sector or public sector targets such as power grids,[99] voting infrastructure,[100] or weapons systems.[101] Thus, overzealous CFAA threats by private parties can chill engagement in and communication about security research. This chilling effect damages the resilience of our economy[102] and national security at a time when the severity of malware and attacks is escalating. These issues of malware and attack escalation bring us to the final CFAA problem — the problem of contagion.

C. The Problem of Contagion: Botnets and Malware

The unfortunate case of Typhoid Mary demonstrated that self-policed hygiene norms have historically proven inadequate to prevent outbreaks of deadly disease. Indeed, without a formalized intervention through infection tracking and quarantine,[103] Mallon likely would have continued to spread infection to hundreds of people. This lesson about the inadequacy of "hygiene" self-policing is equally relevant for digital contexts, and it signals a need for a more robust approach. Indeed, a review of the history of malware reveals that self-policed approaches have proven inadequate. Yet, a more robust strategy has largely been

99. *See* Tim Starks, *U.S. Says Russian Hackers Targeted American Energy Grid*, POLITICO (Mar. 15, 2018, 12:15 PM), https://www.politico.com/story/2018/03/15/dhs-fbi-russia-hackers-targeted-energy-grid-813745 [https://perma.cc/F2FT-VNEC]; David Bond, *Critical Infrastructure Threat as New Malware Is Identified*, FINANCIAL TIMES (Dec. 14, 2017), https://www.ft.com/content/1bbae590-e0df-11e7-a8a4-0a1e63a52f9c (last visited Apr. 13, 2019).

100. *See* Kim Zetter, *The Myth of the Hacker-Proof Voting Machine*, N.Y. TIMES (Feb. 21, 2018), https://www.nytimes.com/2018/02/21/magazine/the-myth-of-the-hacker-proof-voting-machine.html [https://perma.cc/WL5A-MABU]; Bond, *supra* note 99.

101. *See* Noah Schachtman, *Exclusive: Computer Virus Hits U.S. Drone Fleet*, WIRED (Oct. 7, 2011, 1:11 PM), https://www.wired.com/2011/10/virus-hits-drone-fleet/ [https://perma.cc/8NF6-TM2H].

102. If lessons from historical technological market issues hold, a single attack on our market infrastructure might result in billions of dollars of economic loss. *See, e.g.*, Andrea M. Matwyshyn, *Corporate Cyborgs and Technology Risks*, 11 MINN. J.L. SCI. & TECH. 573, 580–85 (2010). Malware and other attacks have already been detected inside market infrastructures. John McCrank, *Cyber Attacks on Stock Exchanges Put Markets at Risk: Report*, REUTERS (Jul. 16, 2013, 6:00 PM), https://www.reuters.com/article/net-us-cybercrime-exchanges-report-idUSBRE96F19A20130716 [https://perma.cc/V5LG-TYUT].

103. The idea of a "quarantine" for individuals who harm others is undoubtedly a familiar one. Indeed, it is a concept that resonates not only with health policy and epidemiology, but with criminal law as well. Incapacitation of offenders has long been a core goal of criminal law, as has the idea of protecting vulnerable populations from the harms that they cause. For a discussion of quarantine, *see* MARTA L. WAYNE & BENJAMIN M. BOLKER, INFECTIOUS DISEASE: A VERY SHORT INTRODUCTION 3 (2015).

absent from the legal,[104] scholarly, and policy conversations of security. Scholars' and policymakers'[105] approaches have often focused on various flavors of "cyber hygiene" initiatives,[106] and "cyber hygiene"[107] remains a popular policy buzzword.

1. Post-Morris Malware and the Need for Security Epidemiology

While the Morris[108] worm was the first worm to self-replicate with the help of a security vulnerability, it was by no means the last malware outbreak. Fifteen years after the Morris worm, the Blaster worm infected potentially millions of machines.[109] The worm exploited a security hole in Microsoft's software to launch a distributed denial of service attack against Microsoft's website.[110] Notable later worms include the 2004 DoomJuice worm, which exploited backdoors left by the MyDoom virus,[111] widely believed to be one of the fastest spreading malware outbreaks in history,[112] and the 2007 worm which allowed the Storm botnet to aggregate victim machines.[113] Another notable outbreak was the worm which facilitated the 2009 DDoS attacks on U.S.

---

104. Meanwhile, the term "cyber hygiene" has, for better or worse, crept into the conversations of even legal practitioners. *See* Chad A. Pittman & Douglas Rapp, *Tips for Good Cyber Hygiene*, ABA (Aug. 9, 2017), https://www.americanbar.org/groups/young_lawyers/publications/tyl/topics/cybersecurity/tips-good-cyber-hygiene.html [https://perma.cc/29Z8-552M]. While this term identifies the need for ongoing maintenance of systems and software, it does not fully capture the dynamics of today's security reality. In particular, a notion of "hygiene" tends to be personal and does not adequately recognize the consequences to third parties of security compromise.

105. Lieutenant Colonel James Coughlin, *Bad Cyber Hygiene Will Cost You More than Your Social Life*, THE HILL (Dec. 28, 2017, 4:30 PM), http://thehill.com/opinion/cybersecurity/366706-bad-cyber-hygiene-will-cost-you-more-than-your-social-life [https://perma.cc/K6WU-CM6L].

106. *See, e.g.*, *National Cybersecurity Assessments and Technical Services (NCATS)*, U.S. COMPUTER EMERGENCY READINESS TEAM, https://www.us-cert.gov/resources/ncats#Cyber%20Hygiene [https://perma.cc/DH39-TJFT].

107. For a discussion of "cyber hygiene" initiatives, *see generally* Scott J. Shackelford & Scott Russell, *Operationalizing Cybersecurity Due Diligence: A Transatlantic Case Study*, 67 S.C. L. REV. 609 (2016).

108. *See* discussion *supra* Part II.

109. Douglas Knowles & Frederic Perriott, *W32.Blaster.Worm*, SYMANTEC (last updated Dec. 9, 2003, 11:50 PM), https://www.symantec.com/security-center/writeup/2003-081113-0229-99 [https://perma.cc/P7VU-DXVD]; John Fontana & Ellen Messmer, *Latest worm puts focus on patch woes*, NETWORK WORLD (Aug. 18, 2003, 1:00 AM), https://www.networkworld.com/article/2336040/latest-worm-puts-focus-on-patch-woes.html [https://perma.cc/UGZ7-VQL2].

110. *Id.*

111. *Doomjuice*, F-SECURE, https://www.f-secure.com/v-descs/doomjuice.shtml [https://perma.cc/Z65Z-YPAD].

112. Jay Munro, *MyDoom.A: Fastest Spreading Virus in History*, PC MAG (Feb. 3, 2004, 1:47 PM), https://www.pcmag.com/article2/0,2817,1485719,00.asp [https://perma.cc/DYL3-ERJR].

113. Cara Garretson, *Storm: The Largest Botnet in the World?*, NETWORK WORLD (Sept. 28, 2007, 1:00 AM), https://www.networkworld.com/article/2286172/lan-wan/storm--the-largest-botnet-in-the-world-.html [https://perma.cc/P4X7-C373].

and South Korean infrastructure — a worm which reused code from MyDoom.[114] Today, as explained above, the Mirai botnet and its progeny further raise the stakes of vulnerable systems by incorporating vulnerable IoT devices.[115] Meanwhile, ransomware such as WannaCry has paralyzed entire hospital networks, exploiting unpatched security vulnerabilities.[116] In other words, malware now presents physical risks of harm not only to critical infrastructure, but also to human lives directly.[117]

As both federal agencies and private sector entities have highlighted, in the last five to ten years some of the most significant security threats have involved the aggregation of victim computers into networks of compromised machines — botnets — in order to execute criminal fraud and other kinds of confidentiality, integrity, and availability attacks at scale.[118] Currently two types of malware are particularly problematic — malware that harnesses user machines into botnets[119] and ransomware that denies access to information and functionality on target machines in order to extort payment.[120] As explained by the DOJ:

> Once a computer is infected with the malware, it can be controlled remotely from another computer with a so-called "command and control" server. Using that control, criminals can steal usernames, passwords, and other personal and financial information from the

114. JM Hipolito, *MYDOOM Code Re-Used in DDoS on U.S. and South Korean Sites*, TREND MICRO: SECURITY INTELLIGENCE BLOG (Jul. 9, 2009, 8:27 PM), https://blog.trendmicro.com/trendlabs-security-intelligence/mydoom-code-re-used-in-ddos-on-u-s-and-south-korean-sites/ [https://perma.cc/R5UJ-EMX9].

115. *See supra* notes 87–93 and accompanying text.

116. Bradley Barth, *WannaCry and Hollywood Hospital Ransomware Attacks Crossed a Line for Some Cybercriminals*, SC MEDIA, (Sept. 20, 2017), https://www.scmagazine.com/wannacry-and-hollywood-hospital-ransomware-attacks-crossed-a-line-for-some-cybercriminals/article/690110/ [https://perma.cc/3UTN-TR6T].

117. *See generally* Andrea M. Matwyshyn, *The Internet of Bodies*, 60 WM. & MARY L. REV. __ (2019) (forthcoming) (discussing the potential for a WannaCry-like ransomware attack on body-embedded medical devices).

118. *See, e.g.*, Tara Seals, *Bad Botnet Growth Skyrockets in 2017*, INFO SECURITY MAGAZINE (Jan. 10, 2018), https://www.infosecurity-magazine.com/news/bad-botnet-growth-skyrockets-in/ [https://perma.cc/3HJ2-DUJF]; *Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices*, U.S. DEP'T OF JUST. (May 23, 2018), https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected [https://perma.cc/JVF6-7BHC].

119. Leslie R. Caldwell, *Assuring Authority for Courts to Shut Down Botnets*, U.S. DEP'T OF JUST. ARCHIVES (Mar. 11, 2015), https://www.justice.gov/archives/opa/blog/assuring-authority-courts-shut-down-botnets [https://perma.cc/C4RH-L8U9].

120. *Definition of Ransomware*, TREND MICRO, https://www.trendmicro.com/vinfo/us/security/definition/ransomware [https://perma.cc/8WX5-FPPN].

> computer user and hold computers and computer systems for ransom. Criminals can also use armies of infected computers to commit other crimes, such as distributed denial of service (DDoS) attacks, or to conceal their identities and locations while perpetrating crimes ranging from drug dealing to online child sexual exploitation.[121]

The ability for attackers to mobilize armies of remote third-party computers and execute additional crimes at scale highlights a need to examine whether our current legal paradigm adequately facilitates the mitigation of onward transfer, outbreaks, and exposure of new targets for the good of *uninfected* machines and systems (and their corresponding impact upon individuals). Much like infectious diseases have challenged patients' ability to prevent and respond due to their invisibility to the naked eye and seeming unavoidability,[122] so too have malware infections raised the specter of involuntary exposure.[123] Indeed, despite taking reasonable precautions, Internet users may still find themselves victimized due to preexisting security vulnerabilities, even when they diligently patch their systems.[124] In this manner, malware infections and outbreaks mirror some of the patterns of infectious diseases.[125]

Hence, we might ask the question, "what strategies exist for addressing infectious disease outbreaks?" For most of human history, avoiding disease transmission was the exclusive method known to combat infectious disease,[126] and quarantine was believed to be the primary method of mitigating disease spread in an outbreak.[127] Indeed, quarantines can be effective at limiting onward transfer, provided that the

---

121. Caldwell, *supra* note 119.

122. WAYNE & BOLKER, *supra* note 103, at 2.

123. Tony Bradley, *Heartbleed: Security Experts Reality-check the Three Most Hysterical Fears*, PCWORLD (Apr. 17, 2014, 3:00 AM), https://www.pcworld.com/article/2144840/heartbleed-3-hysterical-fears-and-what-you-really-need-to-know.html [https://perma.cc/7P8D-8GY9].

124. For example, some vulnerabilities are not known at the time of product launch. *See, e.g.*, Jérôme Segura, *Adobe Reader Zero-day Discovered Alongside Windows Vulnerability*, MALWAREBYTES LABS (May 15, 2018), https://blog.malwarebytes.com/threat-analysis/2018/05/adobe-reader-zero-day-discovered-alongside-windows-vulnerability/ [https://perma.cc/NMR4-VS67]; *Zero-Day Vulnerability*, TREND MICRO, https://www.trendmicro.com/vinfo/us/security/definition/zero-day-vulnerability/ [https://perma.cc/8N88-JMCW].

125. Unlike non-infectious diseases (diseases that are not transmitted from host to host) infectious diseases are influenced by the number of contacts the infected individual experiences, much like malware transmission.

126. WAYNE & BOLKER, *supra* note 103, at 2.

127. For example, in 1665, the English village of Eyam voluntarily quarantined itself to prevent the spread of the plague. However, as a consequence, at least half of the villagers ultimately died. *See id.* Self-quarantine approaches in the absence of a set of broader disease management planning cannot succeed in the long-term. Compulsory isolation does not effec-

mode of transmission of the disease is known, and quarantines balance the interests of the uninfected with the interests of the infected.[128] However, while quarantines block transmission in the short term, they are nevertheless fundamentally reactive and only work once we have become aware of a serious threat of disease or outbreak.[129] Ultimately, the goal of disease prevention offers the long term solution, often addressed through immunization, both individually and for purposes of generating herd immunity.[130] For these reasons, disease control theorists have shifted their focus to population-level thinking in fighting disease.[131] Computer intrusion law should incorporate this population-level thinking as well. In other words, the prosecution of individual bot-herders and bot-masters cannot be the only response to these epidemic malware infections.

Perhaps most importantly, because transmission dynamics of infectious diseases matter in outbreak management, epidemiology has generally analyzed three sets of factors to determine the most effective way to mitigate outbreaks:[132] the specifics of the malicious agent, unique characteristics of the host, and the relevant conditions of the environment which they both inhabit.[133] These three sets of factors as applied to malware outbreaks point to a need for incorporation of a more proactive approach. Such an approach could involve not only prosecuting computer intruders but also involve mitigating the spread of malware infection in real time, based on the specifics of the impacted and at-risk targets. As will be explained in greater detail in Part III, population-level thinking about transmission dynamics may present a key part of the path forward in combatting malware, just as it did in epidemiology. Indeed, as the next section explains, we are already seeing signs of population-level analysis of transmission dynamics in the DOJ's and private litigants' approach to malware infections.

---

tively mitigate an ongoing infection, nor does it prevent an outbreak from returning. For further discussion of quarantine, see *Quarantine and Isolation*, CTRS. FOR DISEASE CONTROL AND PREVENTION (Sept. 27, 2018), https://www.cdc.gov/quarantine/index.html [https://perma.cc/R43H-DWP9]; *History of Quarantine*, CTRS. FOR DISEASE CONTROL AND PREVENTION (July 31, 2014), https://www.cdc.gov/quarantine/historyquarantine.html [https://perma.cc/Z9RA-K7S2].

128. WAYNE & BOLKER, *supra* note 103, at 3.

129. *Id.*

130. However, as with any ecological process, the challenge presented by disease is that new variants arrive and old variants evolve.

131. WAYNE & BOLKER, *supra* note 103, at 15.

132. An outbreak is an increase in the incidence of a disease above expected levels in a particular population. Outbreaks can be common — source, propagated, or both. In the case of a common source outbreak, infected individuals are exposed to a shared source of contamination. In a propagated outbreak the infection is actively transmitted directly from person to person. Propagated outbreaks can arrive in waves of transmission. IBRAHIM ABUBAKAR, HELEN R. STAGG, TED COHEN & LAURA C. RODRIGUES, INFECTIOUS DISEASE EPIDEMIOLOGY 32 (2016). Malware outbreaks comes in both varieties.

133. *See id.* at 4–5.

2. Public-Private Malware Outbreak Management

In 1902, a mathematician named Ronald Ross was awarded a Nobel Prize for his mathematical modeling of malaria transmission.[134] Ross's path-breaking work demonstrated that malaria could be functionally eliminated without completely eradicating mosquitoes, the carriers of the disease.[135] As malware continues to become more aggressive, the internet and software are reaching what might be viewed as a Rossian mosquito-malaria moment of sorts. As the prior section argued, in order to save our code ecosystem, proactive legal approaches are needed to eradicate malware; yet, such approaches, if implemented incorrectly, may result in unintended third-party harms.

Recognizing the need for more proactive, population-level malware enforcement, the DOJ not only prosecutes individuals who use, buy, or sell botnets for criminal computer intrusion purposes but also engages in botnet takedown efforts through the civil injunction process. Under the Federal Rules of Civil Procedure ("FRCP"), federal courts have "the authority to issue injunctions to stop the ongoing commission of specified fraud crimes or illegal wiretapping, by authorizing actions that prevent a continuing and substantial injury."[136] When FRCP 65 is used for botnet takedown efforts, the DOJ will file for a Temporary Restraining Order ("TRO") in district court and, once "granted under seal, the command-and-control servers are either physically or remotely seized."[137] Following this seizure and when working in tandem with "a sophisticated technology company [like Microsoft]," for example, "a software update that commands infected bots to disengage from the network and cease malicious behavior" is issued.[138] The DOJ can also use search warrant authority provided in Federal Rule of Criminal Procedure ("FRCrP") 41 to search computers both infected with, and infecting others with, botnets.[139] These civil and criminal authorities may also be used together in certain operations.[140]

Notwithstanding these criminal and civil authorities, the DOJ warns that, depending on the facts of a particular case, prosecutors may lack the statutory authority to file for an injunction to engage in disruption efforts.[141] Specifically, under current law, two federal statutes[142]

134. RONALD ROSS — BIOGRAPHICAL, THE NOBEL PRIZE, https://www.nobelprize.org/nobel_prizes/medicine/laureates/1902/ross-bio.html [https://perma.cc/S7TH-56EF].

135. WAYNE & BOLKER, *supra* note 103, at 16.

136. Caldwell, *supra* note 119.

137. Aniket Kesari, Chris Hoofnagle & Damon McCoy, *Deterring Cybercrime: Focus on Intermediaries*, 32 BERKELEY TECH. L.J. 1093, 1114 (2018).

138. *Id*.

139. *See id.* at 1117.

140. *See id.* at 1114.

141. Caldwell, *supra* note 119.

142. *See* 18 U.S.C. §§ 1345, 2521 (2012).

provide the Attorney General with the authority to bring civil suits against defendants who are engaging in unlawful wiretapping or specific kinds of fraud.[143] These actions are then further governed by the FRCP.[144] Botnets, of course, may be used for criminal activities such as stealing sensitive information, harvesting email account addresses to hack other computers, and executing DDoS attacks, all of which may not involve fraud or illegal wiretapping.[145] Accordingly, in these kinds of cases, there may be no clear civil statutory authority for botnet takedown.[146]

Similar charging problems may occur when the DOJ seeks to prosecute the trafficking of botnets. While aspects of botnet trafficking may be prohibited by the CFAA, there are certain cases that can "fall through the cracks" for two reasons. First, the CFAA does not expressly cover buying or selling access to botnets; it only expressly prohibits the sale or transfer of "passwords and other information."[147] There are cases where brokers who sell access to botnets are not the criminals who created them.[148] Second, similar to the issue raised with botnet takedown authority, the CFAA's trafficking provision requires an intent to commit a financial fraud.[149] There are several uses for botnets, many of which may not involve financial fraud, and the traffickers may have no knowledge of the intent of use by their customers.[150] The gap in this authority, the DOJ asserts, "has resulted in, and will increasingly

143. *Id.* §§ 1345, 2511, 2521 (2012).

144. *Id.*

145. Caldwell, *supra* note 119.

146. *Id.*

147. David Bitokwer, Principal Deputy Assistant General, Keynote Address at George Washington Law Review Symposium entitled "Hacking into the Computer Fraud and Abuse Act" (Nov. 6, 2015), https://www.justice.gov/opa/speech/principal-deputy-assistant-attorney-general-david-bitkower-delivers-keynote-address [https://perma.cc/D2WU-6CZU]. The DOJ notes that while the law criminalizes creating botnets and using botnets for other crimes, it is not clear that the law criminalizes selling or renting botnets. U.S. DEP'T OF JUST., *Prosecuting the Sale of Botnets and Malicious Software* (Mar. 18, 2015), https://www.justice.gov/archives/opa/blog/prosecuting-sale-botnets-and-malicious-software [https://perma.cc/2A43-6QDD]. For example, in one undercover operation, undercover officers "bought" a botnet "consisting of thousands of victim computers" from a criminal, but this sale "did not result in a prosecutable U.S. offense because there was no evidence that the seller had created the botnet in question, and accordingly the seller was free to continue his activity." *Id.*

148. U.S. DEP'T OF JUST., *Prosecuting the Sale of Botnets and Malicious Software*, *supra* note 147.

149. *See Hearing on Taking Down Botnets Before the Subcomm. on Crime and Terrorism of the Senate Committee on the Judiciary*, 114th Cong. 10 (2014) [hereinafter *Caldwell Testimony*] (written testimony of Leslie Caldwell, Assistant Attorney General, Criminal Division, United States Department of Justice) ("In addition, section 1030(a)(6) presently requires proof of an intent to commit a financial fraud. Such intent is often difficult — if not impossible — to prove because the traffickers of unauthorized access to computers often have a wrongful purpose other than the commission of fraud.").

150. *Id.* ("Indeed, sometimes [traffickers] may not know or care why their customers are seeking unauthorized access to other people's computers.").

result in, the inability to prosecute individuals selling access to thousands of infected computers."[151] The DOJ has therefore urged Congress to amend the CFAA by explicitly expanding its CFAA authority to cover the buying or selling of access to botnets and for an expansion of the list of offenses eligible for injunctive relief.[152]

While the DOJ and other federal agencies manage some botnet takedown operations,[153] the impetus or driving force for other botnet takedowns comes from the private sector.[154] Through the FRCP 65 civil injunction process, private entities are now cooperating with public sector entities in self-structured ways to interrupt malware infections that negatively impact their clients and their financial interests.[155] For example, Microsoft has played a pivotal role[156] in what might be characterized as a functional public-private partnership[157] to disrupt and take

151. U.S. DEP'T OF JUST., *Prosecuting the Sale of Botnets and Malicious Software*, *supra* note 147.

152. *See Caldwell Testimony*, *supra* note 149, at 10–11.

153. For example, in April 2013, the FBI spearheaded a public/private botnet takedown operation named Operation Clean Slate, designed to "eliminate the most significant botnets jeopardizing U.S. interests by targeting the criminal coders who create them." *Hearing on Taking Down Botnets Before the Subcomm. on Crime and Terrorism of the Senate Committee on the Judiciary*, 114th Cong. 3 (2014) [hereinafter *Demarest Testimony*] (written statement of Joseph Demarest, Assistant Director, Cyber Division, Federal Bureau of Investigation).

154. *See* Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 Tex. L. Rev. 467, 480 (2017) (describing how "in June 2013, Microsoft and financial institutions worked with the FBI to disrupt botnets that infected computers with 'Citadel' malware and, according to the FBI, caused over $500 million in financial fraud by stealing and using banking credentials").

155. As explained by Richard Boscovich, Assistant General Counsel for the Digital Crimes Unit at Microsoft Corporation, Microsoft, the current process of botnet takedowns involves working with law enforcement and other industry partners and using both "legal and technical tactics" in an ongoing effort to disrupt botnets. In general terms, the legal and technical tactics involve Microsoft "ask[ing] a court for permission to sever the command-and-control structures of the most destructive botnets, breaking communication lines to either the domains or Internet protocol (IP) addresses that cybercriminals use to control the botnet." More specifically, (and putting the legal theory/authority aside for the moment), once receiving permission from a court to takedown a botnet: "Microsoft severs the connection between a cybercriminal and an infected computer, [and] traffic generated by infected computers is either disabled or routed to domains controlled by Microsoft," which allows it to "collect valuable evidence and intelligence used to help notify victims that their computers are infected, as well as clean computers to remove the malicious software." *Hearing on Taking Down Botnets Before the Subcomm. on Crime and Terrorism of the Senate Committee on the Judiciary*, 114th Cong. 6 (2014) [hereinafter *Boscovich Testimony*] (written statement of Richard Boscovich, Assistant General Counsel, Digital Crimes Unit, Microsoft).

156. Mark Mermelstein, Mary Kelly Persyn & Harry J. Moren, *Strategic Remedies for Cybercrime Victims*, 16 J. INTERNET L. 20, 28 (2013).

157. *See* Eichensehr, *supra* note 154, at 475 (describing botnet takedowns as a "manifestation[] of public-private cybersecurity"); Zach Lerner, *Microsoft the Botnet Hunter: The Role of Public-Private Partnerships In Mitigating Botnets*, 28 HARV. J.L. & TECH. 237, 246 (2014) ("The takedown of the Citadel botnet . . . demonstrates the potential role for public-private partnerships in locating and mitigating botnets."); *Boscovich Testimony*, *supra* note 155, at 2 ("For more than a decade, Microsoft has partnered with other companies and global law enforcement agencies to battle such malicious cybercriminals.").

down botnets and to "quarantine" malware with epidemic potential.[158] From the corporate perspective, the primary goal is not to recover assets, but to disable the botnet.[159] As Microsoft explains, their philosophy is that by "aim[ing] for their wallets[,][160] [w]e [can] disrupt botnets by undermining cybercriminals' ability to profit from malicious attacks."[161]

While a number of these operations — both led by the DOJ and the private sector — have resulted in successful public safety outcomes, the lack of a more formalized process around these efforts raises concerns for all involved parties and for consumers. A group of scholars has noted a potential for overbreadth in remedies and the limited transparency and notice mechanisms of the *ex parte* process.[162] Other concerns include lack of oversight regarding takedown operations,[163] which can lead to negative downstream effects for innocent consumers.[164]

Moreover, at certain times, interests of corporate parties and government agents working on particular cases are not always aligned in these malware interventions. More specifically, while the goals of participants from the private sector such as Microsoft are likely aligned with customer protection and speedy take down, the goals of law enforcement in a particular case, at times, are potentially more aligned with a slower approach driven by evidence maximization in order to secure a conviction of the individuals running the botnet.[165] Mean-

158. *See Caldwell Testimony*, *supra* note 149, at 8 (Because private-sector companies "serve a critical function when they notify victims that their computers have been compromised and supply the tools needed to clean up those computers," and because "the vast majority of the internet is owned and operated by the private sector, we simply could not conduct anti-botnet operations without the firm commitment of network service providers to protecting their customers.").

159. *Id.*

160. In one botnet takedown operation, for example, "financial partners reported between [an] 86% and 98% reduction in fraud after [Microsoft's] action against the Citadel botnet." *RSA 2014: Microsoft and Partners Defend Botnet Disruption*, COMPUTER WEEKLY (Mar. 3, 2014), https://www.computerweekly.com/news/2240215443/RSA-2014-Microsoft-and-partners-defend-botnet-disruption [https://perma.cc/9K8Z-4TW8].

161. *Boscovich Testimony*, *supra* note 155, at 4. Some, however, have analogized takedown efforts to the game "Whack-A-Mole." In response to this argument, Boscovich asserted that "[a]t the very minimum, the disruptive approach eliminates the less sophisticated cyber criminals, reducing the noise, which enables us to concentrate on the bigger threats." *RSA 2014*, *supra* note 160.

162. *See* Kesari et al., *supra* note 137, at 1118–19.

163. *See* Lerner, *supra* note 157, at 254–56.

164. *See* discussion *infra* notes 172–175 and accompanying text.

165. *See* Army Cyber Institute, *CyCON US 2018 - Botnet Takedowns*, YOUTUBE (Jan. 7, 2019), https://youtu.be/SAn8ZpgJiKs [https://perma.cc/7UHH-E754] (Attorney Gabriel Ramsey, Partner, Crowell & Moring, and outside counsel for Microsoft, at a conference in November 2018, explains a time when a botnet takedown effort "bumped up" against a government investigation involving an ongoing wiretap. If or when a situation arises that a private party is being asked by the government to "stand down" with respect to the private entity's

while, it is reasonable to presume that intelligence services may, in certain circumstances, also prefer to delay a botnet intervention for a period of time to benefit intelligence collection.[166]

Further, because of the lack of formalization of the current process, there is no established mechanism to document and learn from the successes and imperfections of past takedown efforts. To the extent we know about botnet takedown operations, this information emerges from corporate[167] or DOJ press releases[168] and occasional litigation.[169] For example, as described in Congressional testimony, Microsoft has indicated that when it engages in a botnet takedown, the company "work[s] hard to avoid disrupting legitimate Internet traffic and, where necessary, we will take steps during or after implementation of a court order to achieve that goal."[170] Microsoft, however, has not always been successful at preventing collateral damage during botnet takedowns.[171] It has been reported that during the takedown of the Zeus botnet, a joint operation between Microsoft, the FBI and the DOJ,[172] "Microsoft . . . knocked out many servers that belonged to security researchers . . . [who] provided a valuable service to the public by notifying system administrators that they had infected computers on their network."[173] In another instance, a researcher discussing the fallout from Microsoft's takedown of 3322.org to disrupt the Nitol botnet noted that a "public cloud has been disrupted for potentially millions of legitimate users, none of whose traffic goes anywhere at all near microsoft.com or is any way related to Nitol or other botnets."[174] In yet another botnet

---

efforts to takedown or disrupt a botnet, Mr. Ramsey suggested that it would be useful for the government to provide more information about what they need so everyone's equities could be addressed: "If I'm being asked to stand down, can I trust you?" This particular discussion by Mr. Ramsey can be found at 36:07-42:19 and 54:39-55:50 in the video).

166. *Demarest Testimony*, *supra* note 153, at 1 ("Botnets can also be used for covert intelligence collection . . . .").

167. Juan Hardoy, *Breaking Up a Botnet – How Ramnit was Foiled*, MICROSOFT EU POLICY BLOG (Oct. 22, 2015), https://blogs.microsoft.com/eupolicy/2015/10/22/breaking-up-a-botnet-how-ramnit-was-foiled/ [https://perma.cc/DM5E-ABBK].

168. *See, e.g.*, U.S. DEP'T OF JUST., *Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices* (May 23, 2018), https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected [https://perma.cc/MW43-WV4B].

169. For a discussion of botnet takedown efforts, *see generally* Kesari et al., *supra* note 137, at 1106–21.

170. *Boscovich Testimony*, *supra* note 155, at 6.

171. For a detailed discussion of some kinds of the collateral damage that can occur during botnet takedowns, *see* Lerner, *supra* note 157, at 250–52.

172. *Id.* at 249.

173. James Wyke, *Was Microsoft's Takedown of Citadel Effective?*, NAKED SECURITY (June 12, 2013), https://nakedsecurity.sophos.com/2013/06/12/microsoft-citadel-takedown/ [https://perma.cc/G764-GTRS].

174. Suresh Ramasubramanian, *Microsoft's Takedown of 3322.org - A Gigantic Self Goal?*, CIRCLEID (Sept. 17, 2012, 6:53 AM), http://www.circleid.com/posts/20120917_microsoft_takedown_of_3322_org_a_gigantic_self_goal/ [https://perma.cc/EYA8-U993].

takedown operation where Microsoft received court authorization to seize 23 domains from No-IP, a provider of dynamic DNS services, service for ordinary users who were not botnet victims was interrupted.[175] Similarly, caselaw appears to indicate at least one other botnet takedown by a federal agency ended in complications and third-party harm.[176]

Meanwhile, the risks of serious collateral damage are increasing. With the existence of what one of us has termed the "Internet of Bodies" ("IoB") — the use of the human body as a technology platform[177] — the possibility of botnets and botnet takedowns directly affecting human safety is upon us. Indeed, one commentator has envisioned a highly problematic scenario: "with particularly sensitive systems and devices like hospital networks and medical equipment becoming frequent targets of malicious hacking, what happens if the government attempts to clean a device (such as an infusion pump controlling a patient's medication) without permission?"[178] Accordingly, when thinking about what elements should be included in legislation to formalize a botnet takedown process, the potential for these kinds of downstream harms must be considered, to include how a statute should address mitigation efforts by appropriate parties when a court grants authorization for a botnet takedown operation.[179]

---

175. Microsoft acknowledged that "[d]ue to a technical error . . . some customers whose devices were not infected by the malware experienced a temporary loss of service." Alex Wilhelm, *Microsoft Goes After Botnet, Tanking No-IP's Dynamic DNS Service for Regular Users in the Process*, TECHCRUNCH (July 2, 2014), https://techcrunch.com/2014/07/02/microsoft-goes-after-botnet-tanking-no-ips-dynamic-dns-service-for-regular-users-in-the-process/ [https://perma.cc/BXY4-CGXS]. Given these issues, one group of scholars, while acknowledging Microsoft's understandable role in "implementing the software that disrupt[s] botnets," have cautioned that "this also means that Microsoft . . . can cause unintended harms by pursuing an overbroad TRO." Kesari et al., *supra* note 137, at 1119. Accordingly, "[w]ithout any way to raise concerns before implementation, potential victims must rely on Microsoft's and a court's foresight of potential harms to innocent parties." *Id.*

176. FTC v. Pricewert LLC, No. C-09-2407 RMW, 2009 WL 1689598, at *1–2 (N.D. Cal. June 15, 2009); FTC v. Pricewert LLC, No. C-09-2407 RMW, 2010 WL 329913, at *1 (N.D. Cal. Jan. 20, 2010) (relying on Part 5 of the FTC Act, botherder's hardware was disconnected from the internet and a receivership created, but the temporary restraining order allegedly caused harm to innocent third parties because of defendant's servers being disconnected from the internet).

177. *See generally* Matwyshyn, *supra* note 117.

178. Gabe Rottman, *All Bots Must Die: How a Senate Bill to Combat Botnets Could Put Privacy at Risk*, CDT (Aug. 8, 2016), https://cdt.org/blog/all-bots-must-die-how-a-new-senate-bill-to-combat-botnets-could-put-privacy-at-risk/ [https://perma.cc/K65S-PDXT]. "Cleaning" in this context refers to removing malware from the medical device, not physical cleansing, e.g., scrubbing it with alcohol.

179. Anticipating what can go wrong, in the current botnet takedown process, courts have required Microsoft to post bonds in the hundreds of thousands of dollars. *See* Eichensehr, *supra* note 157, at 523; *see also* Kesari et al., *supra* note 137, at 1106 (arguing that one protection in Rule 65 procedures not found in other private sector remedial schemes is the requirement that "movants file a security bond to pay the costs and damages of any party 'wrongfully enjoined or restrained'" (quoting FED. R. CIV. P. 65(c))).

In additions to concern over gaps in the current CFAA framework with respect to government botnet disruption, we also question whether the current framework can successfully evolve to address next generation security threats. On the private-sector side, as illustrated by Microsoft's efforts to take down the Citadel botnet, private sector entities employ a patchwork of laws to establish actionable[180] harms that provide basis for their takedown efforts under FRCP 65.[181] As botnet activity and other forms of infectious malware are a continuing and increasing threat, a modern computer intrusion statute should directly provide takedown authority and incorporate appropriate privacy and security protections for innocent victims and third parties affected by these malware interventions. Indeed, the challenges presented by these malware scenarios remind us that, much like Typhoid Mary, today's malware problems cannot be solved through legal approaches that rely on individualized duties of "cyber-hygiene" alone. Instead, a more robust security epidemiology approach with attention to population-level transmission dynamics offers the better path forward. Applying these lessons from epidemiology theory, the next Part offers a more robust approach to computer intrusion that recognizes these insights.

III. THE NEXT RELEASE: A SECURITY EPIDEMIOLOGY MODEL AND THE NEW COMPUTER INTRUSION AND ABUSE ACT ("CIAA")

In Soho today sits the John Snow,[182] a pub eponymously named for a doctor who successfully analyzed the source of a London cholera outbreak in 1854. In perhaps the first case of "big data" health analytics, Dr. John Snow demonstrated that a cholera[183] outbreak in Soho[184] that

180. Essentially, Microsoft asserted that the botnet caused the Windows operating system to stop functioning normally, converting it into a "tool of deception and theft while still bearing Microsoft's trademarks." The botnet also damaged Microsoft's reputation due to customer frustration, and Microsoft incurred costs associated with instituting necessary security features. Lerner, *supra* note 157, at 247 (citing Brief for Petitioner at 1, *Microsoft Corp. v. John Doe*, No. 3:13-CV-319, 2013 WL 2728614 (W.D.N.C. June 10, 2013)).

181. In its *ex parte* complaint filed with a district court in Western North Carolina, Microsoft argued that the botnet "violated a number of state and federal laws, including [the CFAA, the CANSPAM Act, the Electronic Communications Privacy Act, the Lanham Act, the Racketeer Influenced and Corrupt Organizations Act, and the North Carolina Computer Trespass law], as well as the common law torts of conversion, unjust enrichment, and nuisance." *Boscovich testimony*, *supra* note 155, at 6.

182. *John Snow*, LONDONIST, https://londonist.com/pubs/john-snow [https://perma.cc/FR4U-XWZN].

183. *John Snow: A Legacy of Disease Detectives*, CTRS. FOR DISEASE CONTROL AND PREVENTION (Mar. 14, 2017), https://blogs.cdc.gov/publichealthmatters/2017/03/a-legacy-of-disease-detectives/ [https://perma.cc/6HL3-SY6W].

184 . Kathleen Tuhill, *John Snow and the Broad Street Pump*, UCLA DEP'T OF EPIDEMIOLOGY, http://www.ph.ucla.edu/epi/snow/snowcricketarticle.html [https://perma.cc/V3L8-UVLZ].

killed 616 people arose from water supplies contaminated by raw sewage.[185] While conventional medical wisdom asserted that cholera was spread by "vapors" or a "miasma," five years prior, Snow had published a (then) controversial article arguing his water contamination theory.[186] After 500 instances of cholera in ten days clustered around a particular intersection in Soho — the intersection where the John Snow pub sits today — Snow suspected that the source of the outbreak was a particular contaminated street water pump.[187] He plotted the deaths from the outbreak on a geographical grid and examined each case for possible sources of contamination.[188] Ultimately, he successfully correlated each case of cholera with the use of the suspect pump.[189] John Snow's work demonstrates the importance of both tracking infection in real time and adopting mitigation strategies that operate on both an individual level and in the aggregate, targeting groups and societies.

In much the same way as the United Kingdom and the United States crafted the field of epidemiology by learning from disease outbreaks in the 19th and 20th centuries, in the early 21st century, we face a parallel challenge in learning how to curb outbreaks of security "diseases" — malware, ransomware, botnets and other types of attacks. Indeed, these attacks are swiftly reaching epidemic proportions.[190]

As a consequence, we advocate a re-framing of security, legal, and policy discussions away from a primary focus on individual "cyber-hygiene" efforts[191] and towards incorporation of a broader approach through a study of "security epidemiology." A new legal and policy approach driven by a model of security epidemiology should explicitly connect individual level security with the broader consumer protection and national security questions raised by malware and computer intrusion. In particular, a security epidemiology approach recognizes the importance of population-level analysis and dynamic malware infection.

---

185. *Id.*

186. His peers discounted his theory, finding the cause to likely be breathing vapors or a "miasma in the atmosphere." Snow had noted that most homes and businesses dumped untreated sewage and animal waste directly into the Thames River, and that water companies often bottled that same water and delivered it to businesses for use. *Id.*

187. *Id.*

188. *Id.*

189. Contamination of the pump allegedly occurred due to a parent's washing a baby's diaper in a town well. *Id.*

190. As explained by the Center for Disease Control, "Epidemic refers to an increase, often sudden, in the number of cases of a disease above what is normally expected in that population in that area." *Principles of Epidemiology in Public Health Practice*, *Third Edition*, CTRS. FOR DISEASE CONTROL AND PREVENTION (May 18, 2012), https://www.cdc.gov/ophss/csels/dsepd/ss1978/lesson1/section11.html [https://perma.cc/VB9N-PASL].

191. Self-policed practices and individual level initiatives alone, unfortunately, have already proven inadequate to stem the security problems arising from today's malware epidemics. For example, a new strain of ransomware is shutting down key services in cities, and the authors are not currently known. Matt Burgess, *The Rise of SamSam, the Hacker Group Shutting Down Entire Cities*, WIRED (Aug. 1, 2018), https://www.wired.co.uk/article/samsam-ransomware [https://perma.cc/H3KY-DF7X].

In other words, security paradigms informed by insights from epidemiology theory recognize that computer intrusion (as currently defined by the CFAA) and prophylactic questions of aggregate infection tracking, incident response, and mitigation are deeply interrelated and interdependent constructs. Stated another way, computer intrusion enforcement should reinforce technical security defense efforts and vice versa, across both the public and private sector. Thus, an important step toward crafting a new security epidemiology approach involves addressing the shortcomings of the CFAA introduced in Part II. Consequently, we propose a new statutory approach — the Computer Intrusion and Abuse Act ("CIAA").

A. The CIAA

As described in Part I, interpreting the CFAA has often confounded both scholars and jurists. With ill or undefined core terms and dated technological constructs, the statute has aged poorly. As such, let us return to first principles and the underlying concern that Congress sought to address: the creation of a workable legal framework for criminal computer intrusion.[192]

1. The Trespass Fixation

The dominant mental model for computer intrusion visible in both the legal scholarship on the CFAA, as well as in the legislative history of the CFAA, is one driven by trespass. It is perhaps intuitive that trespass would offer a natural model for "entering" into a computer system without permission. Indeed, much legal scholarship has diligently attempted to apply this paradigm to the CFAA.[193] Yet, perhaps indicative of the limits of a trespass approach in digital contexts, courts have never crafted a robust independent tort of "internet trespass."[194]

---

192. *See* S. Rep. No. 104-357, at 3 (1996) ("The [bill] would strengthen the [CFAA] by closing gaps in the law to protect better the confidentiality, integrity, and security of computer data and networks . . . . The [CFAA] was originally enacted in 1984 to provide a clear statement of proscribed activity concerning computers . . . .").

193. *See* Orin S. Kerr, *Trespass, Not Fraud: The Need for New Sentencing Guidelines in CFAA Cases*, 84 GEO. WASH. L. REV. 1544, 1544 (2016) ("Most CFAA crimes are rooted in trespass . . . ."). *But see* Catherine M. Sharkey, *Trespass Torts and Self-Help for an Electronic Age*, 44 TULSA L. REV. 677, 700 (2009) ("There is a real concern that unqualified enforcement of trespass to chattels would in effect amount to a *sub rosa* intellectual property right in non-protectable subject matter."); Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass and Privacy*, 62 BUS. LAW. 1395, 1396 (2007) ("The use of trespass doctrine has, in turn, resulted in a remarkable series of decisions, which have taken the meaning of unauthorized access far beyond simple computer hacking.").

194. For a discussion of internet trespass, see, for example, Jane K. Winn, *Crafting a License to Know from a Privilege to Access*, 79 WASH. L. REV. 285, 285 (2004) (explaining that "trespass to chattels has been derided as an anachronism ill-suited to the Internet," but some cases have found "that its application gives appropriate recognition to the rights of owners of

With the benefit of 30 years' hindsight, it is now clear that a trespass paradigm — the mental model used by both the drafters of the CFAA and most legal scholarship — offers a poor choice for a federal computer intrusion statute. Indeed, the somewhat single-minded devotion (obsession?) of jurists and scholars to trespass as the appropriate model for the CFAA has arguably hindered the arrival of a better intrusion paradigm. A trespass model of computer intrusion can account for neither the legal nuances of trespass nor the technical realities of computer intrusion. Similarly, the harms that arise from acts of computer intrusion often do not map well onto the harms that a trespass model seeks to address. Thus, the first step of addressing the shortcomings of the CFAA involves breaking the unhelpful mental constraints of this "trespass fixation."

The reasons that trespass offers a poor model for a federal computer intrusion statute are ample. First, trespass is generally a construct of state law, and comparatively very few federal trespass statutes exist.[195] Indeed, looking to the substance of trespass law, state trespass laws vary dramatically. Trespass comes in various forms.[196] Most broadly, trespass is divided into trespass to chattels[197] and trespass to land.[198] Some states criminalize certain types of trespass conduct that other states deem only worthy of civil redress at best.[199] Some states create subsidiary trespass offenses based on particular industries present in the state,[200] while other states' laws do not reflect identical idiosyncrasies in trespass concepts.[201] As a consequence, the same set of facts might result in significantly different trespass analyses in different jurisdictions. Further, this variation has not resulted in calls for federal harmonization of trespass law. In contrast, because computer intrusion

---

computer equipment connected to the Internet"). *See generally* Michael R. Siebecker, *Cookies and the Common Law: Are Internet Advertisers Trespassing on Our Computers?*, 76 S. CAL. L. REV. 893 (2003); Brett M. Frischmann, *The Prospect of Reconciling Internet and Cyberspace*, 35 LOY. U. CHI. L.J. 205 (2003).

195. Federal trespass law includes 18 U.S.C. § 1382 (2012) (trespass on military bases); 18 U.S.C. § 1863 (2012) (trespass in national forests); and 25 C.F.R. § 163.29 (2018) (trespass on Native American lands).

196. Trespass to the person also exists as a conceptual framing. Trespass to the person historically involves six separate tort concepts: threats, assault, battery, wounding, mayhem (or maiming), and false imprisonment. ARTHUR UNDERHILL, J. GERALD PEASE & W. J. TREMEEAR, THE LAW OF TORTS 250 (9th English and 3rd Canadian ed. 1912).

197 . *Trespass to Chattels vs. Conversion*, FINDLAW, https://injury.findlaw.com/torts-and-personal-injuries/trespass-to-chattels-vs-conversion.html [https://perma.cc/W7B6-WZ7Q].

198. For a discussion comparing various propertization models in the context of the CFAA, see generally Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164 (2004).

199. *Compare* IDAHO CODE § 36-1603 (2018) *with* 18 PA. CONS. STAT. § 3503 (2018).

200. 18 PA. CONS. STAT. § 3503 (2018).

201. NEV. REV. STAT. § 207.200 (2017).

directly implicates population-level risks to innovation and national security, a primarily federal approach[202] is a more logical choice than a state-level approach with significant variation.[203] A true trespass-based model for computer intrusion law — one that accurately reflects the various definitions and flavors of trespass across states — would undesirably exacerbate jurisdictional inconsistency and legal unpredictability. Jurisdictional variation both in substance and in overzealous or inconsistent enforcement of computer intrusion would damage both innovation and national security.

But perhaps more importantly, a trespass model — assuming that we can even agree on which version of trespass law is appropriate — is a poor fit for describing the technical reality of the various known categories of computer intrusion. Depending on the type of attack, there are other criminal law models that will often provide a substantially better conceptual fit for the harm caused by the particular technical intrusion conduct at issue. For example, an intentional and deadly computer intrusion into the pacemaker of a patient is better framed as an act of first-degree murder[204] than a trespass. The compromise and manipulation of financial documentation in a bank is potentially an act of larceny[205] or, perhaps, burglary,[206] money laundering,[207] theft,[208] or breaking and entering.[209] The notion of a "trespass" is both imprecise and significantly undersells the severity of these crimes.

The intrusion caused by a denial-of-service attack[210] potentially prevents the operator of a website from making content externally viewable to third parties because of an unusually high volume of queries.[211] Since websites are open to the public, these queries are all implicitly or explicitly invited — it is the unreasonable volume of the

202. While some state enforcement may be desirable, a homogeneous conceptual approach to defining what constitutes impermissible criminal conduct is essential and should be crafted on the federal level.

203. Recent state efforts to outlaw certain conduct have threatened to materially harm security research. J.M. Porup, *Georgia Governor Vetoes Bill That Would Criminalize Good-Faith Security Research, Permit Vigilante Action*, CSO (May 8, 2018, 1:25 PM), https://www.csoonline.com/article/3269206/legal/new-georgia-law-criminalizes-good-faith-security-research-permits-vigilante-action.html [https://perma.cc/SH5B-7N7P].

204. *See, e.g.*, WASH. REV. CODE § 9A.32.030 (2018).

205. *See, e.g.*, MICH. COMP. LAWS § 750.356 (2017).

206. *See, e.g.*, 720 ILL. COMP. STAT. 5/19-1 (2018).

207. 18 U.S.C. § 1956 (2012 & Supp. IV 2016).

208. CAL. PENAL CODE § 484 (West 2018).

209. MASS. GEN. LAWS ch. 266, § 16 (2018).

210. NCCIC, *Security Tip (ST04-015): Understanding Denial-of-Service Attacks*, US-CERT (June 28, 2018), https://www.us-cert.gov/ncas/tips/ST04-015 [https://perma.cc/ZC3R-YDVT].

211. *Id.*

queries that results in the harm, not the existence of the queries themselves.[212] Thus, technically, it can be argued that no trespass has occurred. This type of harm could easily and more appropriately be described instead through the lens of vandalism,[213] theft,[214] fraud,[215] battery,[216] tortious interference with contract,[217] or loitering.[218]

A "man-in-the-middle" attack[219] is more conceptually parallel to a theft,[220] fraud such as forgery, [221] or stolen corporate opportunity[222] than a trespass — it involves an interception of traffic in transit.[223] A SQL injection[224] might be more akin to breaking and entering[225] or a fraud perpetrated by deceit and trickery[226] than it is to a trespass — it involves injecting code into a dialog box that tricks the site into disclosing additional information because of a vulnerability in its structure.[227] A website defacement[228] is much like spraying graffiti on a building wall[229] or on a locker inside a school in an act of vandalism,[230] littering,[231] and loitering.[232] It is fixable by restoring from a backup, just as one might remove graffiti. A trespass generally cannot be "restored" in a conceptually parallel manner. Scholars, jurists, and legislators do not attempt to recast or unify various traditional bodies of criminal law (and the harms they address) as merely forms of trespass.

By falling prey to the trespass fixation, legal scholars, jurists, and policymakers lose sight of the technical nuances and variations in harms caused by different categories of attacks. Indeed, we theorize that

---

212. *Id.*

213. MINN. STAT. § 609.595 (2018).

214. IOWA CODE § 714.1 (2018).

215. COLO. REV. STAT. § 18-5-102 (2018).

216. WIS. STAT. § 940.19 (2017–2018).

217. Fernandez v. Haber & Ganguzza, LLP, 30 So. 3d 644, 646 (Fla. Dist. Ct. App. 2010). A DoS causes a lack of availability which means that the entity – say a bank – can't fulfill its contractual obligations to its customers because its systems are down.

218. SOUTH GATE, CAL., CODE ch. 7.74 (2018).

219 . Neil DuPaul, *MAN IN THE MIDDLE (MITM) ATTACK*, VERACODE, https://www.veracode.com/security/man-middle-attack [https://perma.cc/3QAX-ZJSA].

220. VA. CODE ANN. § 18.2-96 (2018).

221. COLO. REV. STAT. § 18-5-102 (2018).

222. Eric Talley & Mira Hashmall, *The Corporate Opportunity Doctrine*, U.S.C. INST. FOR CORP. COUNSEL (Feb. 2001), https://weblaw.usc.edu/why/academics/cle/icc/assets/docs/articles/iccfinal.pdf [https://perma.cc/F8TS-P5DV].

223. *See* DuPaul, *supra* note 219.

224 . *SQL Injection*, TREND MICRO, https://www.trendmicro.com/vinfo/us/security/definition/sql-injection [https://perma.cc/W2Y6-3K6R].

225. N.C. GEN. STAT. ANN. § 14-51 (West 2018).

226. *See* MD. CODE ANN., CRIM. LAW § 8-301 (West 2017).

227. *See SQL Injection*, *supra* note 224.

228 . *Website Defacement*, TREND MICRO, https://www.trendmicro.com/vinfo/us/security/definition/website-defacement [https://perma.cc/ER2J-LLV9].

229. *Id.*

230. CAL. PENAL CODE § 594 (West 2018).

231. GA. CODE ANN. § 16-7-43 (2018).

232. INDIANAPOLIS, IND., CODE § 407-103 (2019).

the trespass fixation has substantially contributed to the current stymied state of CFAA reform. For these reasons, the time has come for a reboot of the overall conceptual approach to computer intrusion through a lens that more rigorously analyzes legal and technical reality.

Thus, we offer an entirely different approach to computer intrusion that is inspired by lessons from epidemiology theory and that recognizes the insights from current computer security principles — the Computer Intrusion and Abuse Act ("CIAA"). Among other things, the CIAA avoids the trespass fixation[233] and explicitly considers population-level dynamics of security. It blends traditional criminal computer intrusion discourse with modern concerns over malware and preventative security measures. Specifically, the core computer intrusion provision of the CIAA frames its approach through three elements: (1) the technical notion of harm, as defined in the field of computer science; (2) defendant intent; and (3) the consent of the owner or operator of the protected computer.

2. Technical Harms + Intent + Consent

The traditional epidemiologic triad model explains that infectious diseases result from the interaction of the three elements: the environment,[234] the agent,[235] and the host.[236] Transmission of infection occurs when the agent is conveyed into a particular environment by some mode of transmission and enters through an appropriate portal of entry to infect a susceptible host.[237] Borrowing the spirit of these insights offers an initial model for conceptualizing the next generation of computer intrusion and security harms for purposes of re-writing the CFAA. The environment dictates the severity of the outbreak and speed of spread of the infection.[238] For this reason, we start with a technological construction of intrusion harms around *impairment to system settings*, rather than a legal one. An agent is the infection itself.[239] Agents in the case of security are the attackers themselves — the people whose code causes technical changes to machines and systems. Just as a vaccine and a virus both contain versions of the same infection but infect a host with two diametrically opposed expected outcomes,[240] the intent behind causing the infection matters. A vaccine involves an injection of a

233. It also does not wade into the inevitable policy battles over the proportionality of criminal consequences when compared with other kinds of felony violations.

234. ABUBAKAR ET AL., *supra* note 132, at 7.

235. *Id.*

236. *Id.*

237. *Id.*

238. *Id.*

239. *Id.*

240. *Vaccines (Immunizations) - Overview*, MEDLINEPLUS, https://medlineplus.gov/ency/article/002024.htm [https://perma.cc/5KSM-APA4].

small quantity of the virus designed to be non-harmful, which creates a protective response within the recipient.[241] Hosts are usually the unwilling infection targets of agents;[242] thus, the consent of the potential host is a dispositive indicator of whether a particular instance of infection constitutes an epidemiologically significant event. We consider each of these three elements — technical harm, intent, and consent — in turn.

a. Technical harms

In the security research and vulnerability indexing community, the classic paradigm for analysis of the harms generated by a computer intrusion often focuses on three core constructs — the technical properties of confidentiality,[243] integrity,[244] and availability[245] of systems. The distinctions among these three properties and the reason why their analysis should craft the over-arching paradigm for technical and legal discussions of security has been elaborated at length in prior work by one of us.[246] Here, building on that scholarship, we explain how these three technical elements of security offer one important aspect of the definitional solution to the current CFAA impasse. We replace the confused language of "authorized access" and "exceeding authorized access" in part with a technical, forensically-demonstrable construct.

By reframing the CFAA around the demonstrable technical harms experienced by a "protected computer"[247] at the hands of an alleged intruder, we inject a new level of definitional precision into determining whether an intrusion has occurred. Specifically, a computer intrusion causes harm to the confidentiality of a protected computer when that protected computer can no longer maintain the set of technical properties that were set *a priori* regarding the system's limitations of third-

241. Security researcher Tarah Wheeler has compared a vaccine to the actions taken as part of a "red team assessment." She describes the activity of "injecting a small amount of poison to build our immunity." Email exchange between Tarah Wheeler and Stephanie Pell (March 30, 2019) (on file with authors).

242. *Id.*

243. *See* COMPUT. SEC. RES. CTR., *Glossary of Computer Security Acronyms*, NAT'L INST. OF STANDARDS & TECH., http://csrc.nist.gov/publications/secpubs/rainbow/tg004.txt [https://perma.cc/XMW6-Q4KY] (defining "confidentiality" as "[t]he concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations").

244. *Id.* (defining "integrity" as "[s]ound, unimpaired or perfect condition").

245. Availability has classically referred to preservation of the technical property set *a priori* regarding the ability of a user to access data in the system. *See id.* (defining "availability of data" as "[t]he state when data are in the place needed by the user, at the time the user needs them, and in the form needed by the user.").

246. *See* Matwyshyn, *supra* note 86, at 1140–44.

247. For a definition of protected computer, *see infra* Section III.A.3.

party data access.[248] As described by the National Institute of Standards and Technology ("NIST"), confidentiality refers to the concept of a machine or system holding sensitive data in confidence and limiting access to a previously designated set of individuals or organizations.[249] An intrusion into the integrity of a protected computer relates to any change in the state of the system or the state of information in the system as such data or properties were set *a priori*, free from manipulation or impairment.[250] Finally, availability harms relate to intrusions where the technical property set *a priori* with respect to the ability of particular users to see and access data in the system is damaged. In other words, as explained by NIST, availability relates to the state when data is in the place needed by the user, at the time the user needs it, and in the form needed by the user.[251]

By connecting legal notions of a computer intrusion to these basic security properties, a substantial degree of the current uncertainty in interpretation disappears: immediately one of the two CFAA circuit splits is resolved. The question of whether a contract breach alone should constitute adequate basis for a CFAA claim or criminal charge due to "unauthorized" access or "exceeding authorized access" disappears entirely.[252] Clearly, under a technically constructed definition of intrusion, it does not. Contract harms are not technical harms — they are purely creatures of law arising out of a reciprocally-induced exchange.[253] Thus, the operative initial analysis in a prosecution under the CIAA begins with a purely technical inquiry. The configuration choices as set by the system's or machine's owner set the baseline, and only impairment of that technical baseline constitutes possible harm.[254]

The CIAA next couples this technical construction of harm with two traditional legal constructs — intent and consent. While intent is an element under the CFAA, the CFAA's intent elements, *knowingly*

248. Confidentiality has classically been defined as the maintenance of technical properties set *a priori* regarding a system's limitations of data access. *See* COMPUT. SEC. RES. CTR., *supra* note 243.

249. *Id.*

250. Integrity has classically been defined as the preservation of data or system properties set *a priori*, free from manipulation or impairment. *See id.* (defining "system integrity" as "[t]he quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system"); *id.* (defining "data integrity" as "[t]he property that data meet an *a priori* expectation of quality"); *id.* (defining "integrity" as "[s]ound, unimpaired or perfect condition").

251. *See supra* note 245.

252. The second circuit split relates to whether a plaintiff must plead both damage and loss for a civil recovery under the CFAA. Because we advocate the elimination of all civil claims under the CFAA, our approach also resolves the second circuit split.

253. A contract breach is inapposite and does not inform the technical question of whether a forensically demonstrable technical change has occurred in the system.

254. These configuration choices define the scope of implicit consent of the system owner to a certain level of interaction with third parties.

or *intentionally* accessing a computer without authorization or by exceeding authorization, together with the other elements of the statute, do not offer adequate consideration of the innovation and national security concerns discussed in Part II. For this reason, we buttress the CIAA's technical harm requirement and intent requirement with an explicit affirmative defense for security research.

b. Defendant intent

Apart from concerns over definitional imprecision described in Part II,[255] ill-guided prosecutorial discretion,[256] and the innovation and national security policy concerns described in Part II,[257] the CFAA has been criticized for its inadequate consideration of the intent that motivated an alleged intruder's conduct.[258]

In particular, the current language of the CFAA has raised serious concerns regarding the chilling of security research among both the security research community[259] and among policy experts generally.[260] Researchers regularly state that the lack of CFAA enforcement predictability damages their ability to conform their research conduct to the requirements of the law with certainty.[261] Attorneys who counsel security researchers express similar concerns.[262] In particular, because of

255. *See* discussion *supra* Part II.

256. *See* Jeremy D. Mishkin, *Prosecutorial Discretion Under the CFAA Gets More Discretionary: US v. Nosal*, WHITE COLLAR ALERT (July 18, 2016), https://whitecollarblog.mmwr.com/2016/07/18/prosecutorial-discretion-cfaa-gets-discretionary-us-v-nosal [https://perma.cc/K4Z8-HMDT]; Tor Ekeland, *How To Reform the Outdated Federal Anti-Hacking Law*, CHRISTIAN SCI. MONITOR (Mar. 24, 2017), https://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0324/How-to-reform-the-outdated-federal-anti-hacking-law [https://perma.cc/GSD9-EUW5].

257. *See* discussion *supra* Part II.

258. For a discussion of the CFAA's intent requirements, see David Thaw, *Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement*, 103 J. CRIM. L. & CRIMINOLOGY 907, 914 (2013).

259. *See* Jen Ellis, *How Do We De-Criminalize Security Research? AKA What's Next for the CFAA?*, RAPID 7 BLOG (Jan. 26, 2015), https://blog.rapid7.com/2015/01/26/how-do-we-de-criminalize-security-research-aka-what-s-next-for-the-cfaa [https://perma.cc/8D7N-VKML].

260. *See* Jack Detsch, *Influencers: Antihacking Law Obstructs Security Research*, CHRISTIAN SCI. MONITOR (July 14, 2016), https://www.csmonitor.com/World/Passcode/Passcode-Influencers/2016/0714/Influencers-Antihacking-law-obstructs-security-research [https://perma.cc/9YPG-GX4A].

261. *See* Kate Conger, *New Study Makes Clear Just How Risky It Is to Be a Security Researcher*, GIZMODO (Apr. 10, 2018, 08:30 AM), https://gizmodo.com/new-study-makes-clear-just-how-risky-it-is-to-be-a-secu-1825116053 [https://perma.cc/Z5X2-HTD4].

262. *The Computer Fraud and Abuse Act Hampers Security Research*, ELEC. FRONTIER FOUND., https://www.eff.org/document/cfaa-and-security-researchers [https://perma.cc/NA55-MKVQ].

jurisdictional variation in prosecution and judicial interpretation,[263] researchers and their counsel fear that in the course of performing security research intended to bolster consumer protection and national security, researchers may unintentionally run afoul of prosecutors' potentially evolving interpretations of the meaning of "authorized access" and "exceeding authorized access."[264] Because the possible consequences of such an unintentional transgression include a felony conviction, researchers have repeatedly asked Congress and the DOJ for clarification of how the CFAA's core terms (accessing a computer without authorization and exceeding authorized access) apply to various kinds of security research.[265] Similarly, because of the problems of "double whammy" conduct and doctrinal swapping, researchers fear that a vindictive company may bring a frivolous civil CFAA claim for an end user license agreement violation (in lieu of a contract claim), which may then also be deemed an adequate basis for a criminal charge. Moreover, researchers sometimes receive frivolous threats of litigation from companies displeased with the public disclosure that their products contain code flaws and errors.[266]

As such, the CIAA explicitly proposes an affirmative defense for security research, when those who are engaging in security research knowingly cause an impairment in the confidentiality, integrity, or availability of a protected computer in the course of conducting security research, provided that the researcher (defendant) can prove that her conduct aligns with the generally accepted practices of the security research community.[267] The need for consideration of intent in a more granular manner with respect to security research (through the creation of a security research affirmative defense) is also driven by national security considerations. Because of the current national work force shortage among top-tier security researchers, affirmative mitigation

263. For a discussion of the doctrinal swapping problem that exacerbates these dynamics, see discussion *supra* Part II.

264. *See* Joseph Lorenzo Hall & Stan Adams, *Taking the Pulse of Hacking: A Risk Basis for Security Research*, CTR. FOR DEMOCRACY & TECH. 9 (Mar. 2018), https://cdt.org/files/2018/04/2018-03-27-Risk-Basis-for-Security-Research-FNL.pdf [https://perma.cc/2RN6-YNPK] (describing how the CFAA's broad terms, coupled with "the practical realities of many research methods, creates uncertainty," and how "[u]ncertainty potentially resulting in steep criminal penalties creates a significant chilling effect for researchers").

265. *See* Ellis, *supra* note 259.

266. *See* Hall & Adams, *supra* note 264, at 12 ("For researchers, publicly disclosing research results creates different kinds of risk. Depending on the circumstances and the method of disclosure, a researcher may face risks of harm to their reputation, employment, or legal standing.").

267. This model of expert-driven assessment might be viewed as parallel to the manner in which professions such as medicine and law self-police through malpractice statutes. For a discussion of current medical malpractice cases, see *Medical Malpractice*, PERS. INJ. VERDICT REVIEWS (Thomson Reuters), May 2018.

measures are needed in order to encourage existing security professionals to continue their work for the benefit of public safety without fear of unexpected prosecution.[268]

Next, for the CIAA's consent inquiry, we build on Professor James Grimmelmann's reframing of the CFAA's "access without authorization" and "exceeds authorized access" language through the lens of consent.

c. Consent: Kerr's Paradox and Grimmelmann's Resolution

As previously noted, the CFAA fails to define "access," "authorization," or "authorized access," and this lack of definitional clarity has caused a host of problems, including but not limited to: void for vagueness problems,[269] shifting of the traditional boundaries between civil and criminal responsibility,[270] detrimental impacts on innovation, and a chilling effect on security researchers that harms national security.[271] Scholars have responded by trying to find an interpretive solution under the CFAA's current language that provides a logical, constitutional, and workable theory for computer intrusion crimes.[272] We are therefore not the first to suggest that the CFAA is a problematic statute in need of reform or greater interpretive clarification from courts.[273] In this Part, we discuss two scholars' attempts to resolve perhaps the most problematic element of the CFAA — the meaning of "unauthorized access" or "access without authorization." Specifically, we focus upon the work of Professors Orin Kerr and James Grimmelmann. Each offers a particular view of how courts should interpret unauthorized access and of the implications of such interpretations. Kerr argues that authorization to access a computer is contingent upon trespass norms, which he defines as "shared understandings of what kind of access invades another person's private space."[274] Grimmelmann challenges Kerr's analysis, arguing that "authorization under the CFAA is best understood as

268. *See* Matwyshyn, *supra* note 86, at 1114 (explaining the problem of "reciprocal security vulnerability," that is, how public sector/national security concerns and private sector/consumer protection concerns are inextricably interwoven).

269. *See* discussion *supra* Section II.A.

270. *See* discussion *supra* Section II.B.

271. *See* discussion *supra* Section II.B.

272. *See, e.g.*, Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1599–1600 (2003); Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2272–73 (2004); *see generally* Patricia L. Bellia, *A Code-Based Approach to Unauthorized Access Under the Computer Fraud and Abuse Act*, 84 GEO. WASH. L. REV. 1442 (2016); Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143 (2016); Michael J. Madison, *Authority and Authors and Codes*, 84 GEO. WASH. L. REV. 1616 (2016); Josh Goldfoot & Aditya Bamzai, *A Trespass Framework for the Crime of Hacking*, 84 GEO. WASH. L. REV. 1477 (2016).

273. *See supra* note 272.

274. Kerr, *Norms of Computer Trespass*, *supra* note 272, at 1143.

incorporating the traditional legal understanding of consent."[275] Grimmelmann's analysis provides the more useful foundation for our own CFAA revision project.

i. Kerr's Trespass Norms and Grimmelmann's Consent

Drawing some support from legislative history,[276] Kerr has, for over two decades, essentially argued that trespass is the appropriate paradigm to employ in construing and interpreting prohibitions on "unauthorized access" in state and federal computer abuse and intrusion statutes.[277] In his most recent essay, *Norms of Computer Trespass*, he articulates his trespass theory in its most refined form: "authorization to access a computer is contingent on trespass norms — shared understandings of what kind of access invades another person's private space."[278] When discerning online trespass norms, an apparent tension exists between the openness of the Web and the impediments to access website owners often impose, such as "speed bumps, barriers, and caveats to access that range from hidden addresses to limiting cookies and banning IP addresses."[279] Kerr argues that these kinds of permeable roadblocks or obstacles raise difficult questions about when access to or use of a website should be considered unauthorized access.[280] Recognizing the open nature of the Web, he claims that computer trespass law must strike an appropriate balance between protecting security and privacy, while also "creating public rights to use the Internet free from fear of prosecution."[281] Accordingly, Kerr argues for "presumptively open norms" as the necessary context for determining if a computer trespass has occurred on the Web.[282]

With open norms as a foundation for his trespass theory, Kerr asserts that the principle of *authentication* — that is, the verification of the user as the person with access rights — "provides the most desirable basis" for determining whether a trespass has occurred online.[283] He contends that activity that does not involve bypassing an authentication

275. James Grimmelmann, *Consenting to Computer Use*, 84 GEO. WASH. L. REV. 1500, 1519–22 (2016).

276. *See, e.g.*, S. Rep. No. 104-357, at 11 (1996) (stating that "section 1030(a)(5) criminalizes all computer trespass, as well as intentional damage by insiders, albeit at different levels of severity"); S. Rep. No. 99-432, at 9 (1986), reprinted in 1.986 U.S.C.C.A.N. 2479, 2487 ("In intentionally trespassing into someone else's computer files, the offender obtains at the very least information as to how to break into that computer system. If that is all he obtains, the offense should properly be treated as a simple trespass.").

277. Kerr, *Cybercrime's Scope*, *supra* note 272, at 1605–40; Kerr, *Norms of Computer Trespass*, *supra* note 272, at 1143.

278. Kerr, *Norms of Computer Trespass*, *supra* note 272, at 1143.

279. *Id.* at 1161.

280. *Id.*

281. *Id.*

282. *Id.*

283. *Id.* at 1147.

barrier — such as the blocking of IP addresses, using a webscraper to query website addresses that a computer owner did not expect people to find, or a violation of a terms of service — would not trigger CFAA liability.[284] For Kerr, "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,"[285] and thus insufficient to trigger computer trespass liability.

Enter Grimmelmann. In *Consenting to Computer Use*, Professor Grimmelmann approaches the "mystery" of unauthorized access from a different perspective — one which looks to whether the computer owner has given consent to computer use(s). Grimmelmann argues that the term without authorization "does not refer to what a *computer user does*; it refers to what a *computer owner says* about those uses."[286] Accordingly, "[t]he issue is not whether X is allowed, but whether X is allowed by the computer's owner."[287] Indeed, the current CFAA does not define a class of conduct that is per se unlawful; whether or not any specific conduct in relation to a computer would be unlawful depends on whether the conduct is authorized or unauthorized.[288] He explains that authorization under the CFAA is a "defense in the same way that consent is a defense to torts and crimes including trespass, battery, and rape."[289] That is, to access a computer with authorization is to access and use a computer in a manner that is consistent with the consent given by the computer's owner.[290]

But, as Grimmelmann argues, in our modern online environment, the determination of whether a computer owner has given her consent must be assessed though characteristics that are distinctive to computer use: "[c]omputer use is technically and temporally intermediated, so an owner cannot approve or reject proposed uses as they happen. Instead, she will typically need to give prospective consent, leaving it to users and courts to interpret the scope of that consent and to apply it to conduct the owner may not have anticipated."[291]

In addition to prospective consent, Grimmelmann explains that there is a second distinctive feature of computer use cases:

> "Software is *plastic*: Programmers can implement almost any system they can imagine and describe precisely." This fact vastly increases the complexity of

284. *Id.* at 1163–64.
285. *Id.* at 1164.
286. Grimmelmann, *supra* note 275, at 1501.
287. *Id.*
288. *Id.*
289. *Id.* at 1502 (citing to discussions of consent found in 86 C.J.S. *Torts* § 38 (2016) and 6 AM. JUR. 2D *Assault and Battery* § 7 (2016)).
290. *Id.* at 1502.
291. *Id.*

> people's interactions with software. In particular, it means there will almost always be cases in which software behaves in a way its programmers neither expected nor intended. Software is buggy, and automation plus bugginess makes software hackable.[292]

This "plasticity," Grimmelmann argues, recommends two principles to guide any computer use theory of consent. First, courts applying the CFAA must make allowances for difficulties facing computer owners insofar as they are vulnerable to the "distinctive risk of opportunism" from "ill-intentioned computer users" who can "observe in detail how software works and then arrange their interactions with it for maximum benefit" at the "owner's expense."[293] Second, courts applying the CFAA must be cognizant of the risks facing computer users, specifically a risk of "arbitrary enforcement" from computer owners who may "behave opportunistically either by arguing after the fact that they were deceived about some relevant fact" or, in advance, "setting out a disingenuously broad statement of what constitutes unauthorized use."[294] For such fairness concerns, as well as to avoid constitutional void for vagueness problems,[295] computer users must be given fair notice of what activity the law will treat as unauthorized conduct.[296]

With this background, Grimmelmann analyzes how two distinct consent regimes, factual consent and legal consent, manifest and interact in computer use/misuse cases. Recognition of these two kinds of consent and how they interact with one another is, we believe, essential to arriving at a reasonable and workable modern computer intrusion statute.

ii. Consent Dualism: Factual versus Legal Consent

Factual consent concerns computer use authorized by the computer owner. Both words and code are relevant to determining the scope of the computer owner's factual consent. If Alice tells Bob he is welcome to use her computer, Alice's statement to Bob is a form of factual consent.[297] When Eve uses her own laptop to check a weather website that Carlos has designed,[298] Carlos has communicated factual consent insofar as he has "created a website . . . intended for public use."[299]

---

292. *Id.* at 1505 (internal citations omitted).
293. *Id.* at 1506.
294. *Id.*
295. *See* discussion *supra* Section II.A.
296. Grimmelmann, *supra* note 275, at 1507.
297. *Id.* at 1508.
298. *Id.*
299. *Id.*

Even when a computer owner's words may be perfectly clear, code also matters.[300] Consider a scenario where eight-year-old Alice creates an account on a build-your-own emoji website.[301] The website, as part of its terms of service, requires all users to be at least ten years old and Alice is required to acknowledge this fact when she clicks "I agree" to the terms of service.[302] Notwithstanding this requirement, Alice enters her correct year of birth during the sign-up process and the website allows her to create an account.[303] The website owner does not, however, delete her account.[304]

While factual consent concerns computer use authorized by the computer owner, legal consent is the determination, *as a matter of law*, that Alice consented to a particular use of her computer.[305] As Grimmelmann explains, "legal consent is based on factual consent," but it can differ in two important ways: (1) the law may not treat factual consent as sufficient to constitute legal consent because, as a matter of policy, there may be reasons to treat Alice's factual consent as defective; or (2) the law may treat factual consent as unnecessary for legal consent because there are good reasons, as a matter of policy, to treat Alice as if she had factually consented, even if she did not.[306]

As a matter of policy, we would not want to recognize Alice's factual consent as sufficient for legal consent if her factual consent was the product of "coercion, deception, or incapacity."[307] But to say, as a matter of law, that legal consent is not present because factual consent was the product of fraud requires policy choices identifying what kinds of actions constitute "culpable fraud."[308]

Conversely, there are situations where, as a matter of policy, it may be preferable to recognize the existence of legal consent, even if Bob did not give factual consent.[309] As Grimmelmann notes, in the CFAA context, the *Craigslist Inc. v. 3Taps Inc.*[310] case illustrates the principle of imputed consent and the policy choices at issue.[311] Drawing from the facts of this case, Alice runs a website where people purchase classified ads.[312] Eve uses a program to scrape publicly available information on

300. *Id.* at 1512.
301. *Id.*
302. *Id.*
303. *Id.*
304. *Id.*
305. *Id.* at 1512–13.
306. *Id.* at 1512.
307. *Id.* at 1513.
308. *Id.*
309. *Id.* at 1514–15.
310. 942 F. Supp. 2d 962 (N.D. Cal. 2013).
311. Grimmelmann, *supra* note 275, at 1516.
312. *Craigslist*, 942 F. Supp. 2d at 966.

Alice's website.[313] Alice sends Eve a letter telling her to cease and desist her scraping activities.[314] Eve ignores the letter and continues to scrape.[315] Here, it is clear through Alice's words that she has not given factual consent to the continued scraping.[316] But, as a matter of law, should legal consent be imputed? That is, should making information publicly available on a website constitute constructive consent for scraping or other uses of that information that don't cause loss of data or the website to crash? One might argue that when information is made available to the public, "allowing website owners to selectively exclude individual users would chill speech and innovation."[317] This choice — whether or not to impute legal consent and deem the scraping to be authorized access — is a policy choice.[318]

iii. Why the Consent Dualism Distinction Matters

What then does Grimmelmann's consent theory offer that Kerr's norms of computer trespass approach does not? Grimmelmann identifies a paradox that can only be resolved by distinguishing factual from legal consent. He begins by suggesting that although factual and legal consent are distinct concepts, most academic literature and judicial analysis of the CFAA collapses the two forms of consent.[319]

To illustrate the collapse of these two forms of consent — and the resulting paradox — Grimmelmann cites from Kerr's decades-long work on social norms theory under the CFAA, and specifically cites Kerr's most recent *Norms of Computer Trespass* essay.[320] He notes that Kerr's descriptions of offline trespass norms are often "appropriate when speaking of factual consent," such as when Kerr describes how "an open window isn't an invitation to jump through the window and go inside."[321] Grimmelmann observes, however, that in other places in *Norms of Computer Trespass*, Kerr describes how social norms operate in ways that are consistent with legal, not factual, consent.[322] Specifically, Grimmelmann identifies a passage where Kerr argues that "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

313. *Id.*
314. *Id*. at 967.
315. *Id.*
316. Grimmelmann, *supra* note 275, at 1516.
317. *Id.*
318. *Id.*
319. *Id.* at 1519.
320. *Id.*
321. *Id.*
322. *Id.* at 1520.

publishing a newspaper but then forbidding someone to read it. Publishing on the Web means publishing to all."[323] Grimmelmann identifies this statement as "a normative argument about the proper scope of legal consent."[324] That is, Kerr's appeal and reliance on the open norms of the Web imputes (legal) consent to individual users who visit a public website.[325]

While not disagreeing with the policy informing Kerr's normative argument, Grimmelmann explains that "there are cases where Kerr's descriptive and normative claims cut in opposite directions."[326] Specifically, in *3Taps*-like cases where a website owner allows the general public to access his website but expressly forbids a particular individual from access, Kerr might argue that "common social practices create shared understandings" such that, if specifically told not to access the website, you don't have permission to visit it.[327] But, Kerr's assertion that "[p]ublishing on the Web means publishing to all" seems to mean that *everyone* has to access the website.[328] This collapse of factual consent and legal consent results in a situation where Kerr seems to be arguing that the owner both did and did not consent to access.[329] This "paradox resolves itself," however, with the recognition that "Kerr is shifting between factual and legal consent."[330] Moreover, "Kerr's equivocation between factual and legal consent undermines his appeal to social norms" of trespass as an interpretive theory for unauthorized access under the CFAA.[331] More specifically, Grimmelmann writes:

> If social norms are used descriptively, to inform computer users and courts about the scope of factual consent (as in *Weather Website* and Kerr's chimney example), they are incapable of resolving hard policy questions about the proper scope of the CFAA. But if social norms are used normatively, to tell courts when they ought to find legal consent (as in *Nosal* and *3Taps*), their use is highly problematic for precisely the reason Kerr himself pinpointed in a different paper: the *contestability of online norms* creates a substantial vagueness problem.[332]

---

323. *Id.* (quoting Kerr, *supra* note 274, at 1169).
324. *Id.*
325. *Id.*
326. *Id.*
327. *Id.*
328. *Id.*
329. *Id.*
330. *Id.*
331. *Id.*
332. *Id.* at 1520–21.

Having exposed the problems of using social norms of computer trespass as an interpretive theory for unauthorized access under the CFAA, Grimmelmann reminds us that in many areas of criminal law — trespass, theft, battery and rape — "consent is a complex bundle of doctrines built around factual consent but incorporating a variety of legal fictions [i.e. created legal consent]."[333] Not all of the "bundles" are the same; what is sufficient to confer consent in one area may not be in another.[334] Computer misuse law or, as we argue, a modern *computer intrusion* statute will, among other things, need its own bundle.

3. The New Language

In this Part, we propose language for the CIAA. First, our proposal incorporates the elements of consent of the owner of the "protected computer,"[335] and the intent of the alleged intruder, but only criminalizes the alleged intruder's conduct if an impairment of confidentiality, integrity, or availability occurs on a protected computer. Consistent with the perspective that protecting a robust security research ecosystem is a pivotal component of national security policy, we include a security research affirmative defense as part of the first provision of our proposal. Second, we provide a provision for the prosecution of an individual who criminally impersonates another by accessing a protected computer with a password or other unique credential. This provision incorporates the DOJ's current ability to prosecute the trafficking of passwords. Third, we seek to address computer misuse by the special population of "trusted individuals" who have a duty of confidentiality to the government as a condition of employment and who, by accessing a government computer for a non-government purpose, would violate the proscribed terms of that duty. Fourth, we seek to create a specific statutory mechanism that will allow the government or a private party (under certain circumstances and with the agreement and cooperation of the DHS and the DOJ and oversight of a federal district court) to "takedown" botnets (or what we define as epidemic malware) for the purpose of stopping the spread of the malware in order to prevent additional computer intrusion harms from occurring. Fifth, we seek to provide a more solid legal foundation for the DOJ to prosecute the creation and trafficking of botnets, which we address in a new provision criminalizing the trafficking of epidemic malware.

Finally, in drafting the criminal statutory provisions below (all of which are criminal provisions but for the aforementioned epidemic malware provision) we have chosen not to include a "companion" civil

333. *Id.*

334. *Id.*

335. For our definition of "protected computer," which is adapted from the current definition in the CFAA, see *infra* Section III.A.3.a.

provision that, like the current CFAA, allows a private party to sue another private party "to obtain compensatory damages and injunctive relief or other equitable relief" if the first party "suffers damage or loss" due to a CFAA violation and the offending conduct meets at least one of five enumerated kinds of harms.[336] In Part II, we explained many of the problems caused by the current civil provision. As we previously noted, much of the conduct charged under the current CFAA by private parties could be addressed by other areas of law, such as intellectual property law, contract law, and other traditional statutory frameworks such as theft and vandalism.[337] We are therefore not convinced that a companion civil provision is a necessary or even normatively appropriate element of a new computer intrusion statute. Indeed, eliminating the civil provision eliminates the circuit split regarding whether contract breach can provide the basis for a CFAA violation (and consequently what we have described as the double whammy conduct and doctrinal swapping problems disappear),[338] as well as the split on whether a plaintiff must plead both damage and loss for a civil recovery under the CFAA (because the civil provision has been eliminated, this issue becomes moot).[339] Thus, we advocate restoring the CFAA to its original purely criminal form.[340]

The rest of this Part provides a description and explanation of our proposed changes, accompanied by model statutory language. We also provide a series of hypotheticals that illustrate how our proposed statutory provisions in the CIAA would operate in context of many of the challenges and controversial applications of the CFAA.

a. Change 1: 1030(a)(1) - Criminal Computer Intrusion

We begin by expressly abandoning the concepts of "access without authorization" and "exceeding authorized access." Consistent with the three-part paradigm introduced in Part III, we replace the language of

336. 18 U.S.C. § 1030(g) (2012). The five harms are enumerated in 18 U.S.C. § 1030 (c)(4)(A)(i)(I)–(V).

337. *See* discussion *supra* Section III.A.1.

338. *See* discussion *supra* Section II.A.2.

339. Interpretation of 18 U.S.C. § 1030(a)(4). For further discussion of this circuit split, *see* Matwyshyn, *supra* note 16, at 185 n.114. *Compare* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 585 (1st Cir. 2011) ("As we move into increasingly electronic world, the instances of physical damage will likely be fewer while the value to the victim or what has been stolen and the victim's costs in shoring up its security features undoubtedly will loom ever-larger.") *with* Garelli Wong & Assocs. v. Nichols, 551 F. Supp. 2d 704, 708 (N.D. Ill. 2008) (holding that a plaintiff under the CFAA must plead both "damage" and "loss.").

340. Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, § 290001(d), 108 Stat. 1796, 2098 (codified as amended at 18 U.S.C. § 1030(g) (2000 & Supp. I 2001)). Congress should also consider that because computer intrusion statutes parallel to the CFAA exist on the state level, the proposed CIAA approach requires that the new statute preempt state computer intrusion statutes that conflict with its limited scope. A more expansive discussion of this preemption issue is beyond the scope of this article.

authorization in section 1030(a)(1) with the concepts of demonstrable technical harms, intent, and consent:

> Whoever intentionally accesses a protected computer and without the express or implied consent from the owner or operator of the protected computer
>
> (A) knowingly engages in conduct that impairs the confidentiality, integrity, or availability of the protected computer or information contained in the protected computer; or
>
> (B) intentionally engages in conduct that impairs the confidentiality, integrity, or availability of the protected computer or information contained in the protected computer
>
> shall be punished as provided in . . . [341]
>
> Whoever conspires to commit or attempts to commit an offense under this subsection shall be punished as provided in . . . [342]

In the first three lines of this provision, we incorporate the concept of consent by the computer owner, which can be communicated *expressly* through words or *implicitly* through code or some combination of both.[343] The beginning of this provision also requires that the alleged intruder intentionally access a protected computer. But, as conveyed in sections (A) and (B), whether or not consent is given by the computer owner, there is no violation of this provision unless an impairment of confidentiality, integrity, or availability ("CIA"), of a protected computer or the information contained on a protected computer occurs. These harms are objectively testable and forensically discoverable on the protected computer.[344] Moreover, the conduct that causes the impairment of CIA must be either knowing or intentional on the part of the alleged intruder — that is, the alleged intruder is not responsible for actions taken in ignorance or by mistake. She is responsible when she

---

341. It is beyond the scope of this Article to propose a statutory sentencing framework for the CIAA.

342. *Id.*

343. *See* discussion *supra* Section III.A.2.c.

344. When a defendant is charged with an attempt under this provision, the government would offer evidence to prove the defendant's specific intent to commit a CIA harm (i.e. knowing what the outcome may be), which will likely include specific actions he takes towards the completion of the crime. The ability to detect an intrusion may be impaired because of the lack of adequate security measures in place by the target of the alleged intrusion.

is aware that her activities could or would result in certain consequences. As previously discussed, we believe the construction of criminal culpability around the security harms defined by the "CIA triad" is the appropriate focus for a computer intrusion statute.[345] If there is no CIA impairment, conspiracy to impair the CIA of a protected computer or an attempt to impair the CIA of a protected computer, then our statute does not criminalize the conduct in question under this provision.

The current CFAA contains a scheme that both criminalizes and raises statutory penalties for violations that implicate other kinds of harms, like the transmission of national security information or an intent to defraud, which motivate a defendant's criminal activity or follow from the unauthorized access or access that exceeds authorization from a computer or protected computer.[346] We do not disagree with the idea that certain kinds of "criminal purpose" or violations that also involve "follow-on" criminal conduct may deserve a higher statutory maximum or greater exposure under the Federal Sentencing Guidelines. It is beyond the scope of this Article, however, to propose a holistic statutory and sentencing guidelines framework that both addresses problems with sentencing under the current CFAA[347] and accounts for the new substantive CIAA provisions that we propose. That said, we would incorporate a misdemeanor charging option into this provision to give prosecutors discretion for addressing, for example, first time offenses by minors that do not cause significant damage or other instances where a misdemeanor "warning" may be appropriate.[348]

---

345. This provision is meant to replace all of the substantive violations contained in 18 U.S.C. § 1030(a)(1)–(4), (a)(5)(A)–(C), and (a)(7). This provision also replaces 18 U.S.C. § 1030(b), which incorporates a conspiracy to commit or attempt to commit the substantive provisions.

346. *See generally* 18 U.S.C. §§ 1030(a)–(c) (2012). For example, the current CFAA both specifically criminalizes and provides for higher statutory maximums for criminal conduct that involves obtaining information pertaining to the "national defense" or "foreign relations" of the United States when the perpetrator "has reason to believe that such information . . . could be used to the injury of the United States or to the advantage of any foreign nation." 18 U.S.C. §§ 1030(a)(1), (c)(1)(A)–(B).

347. *See* Kerr, *supra* note 193, at 1544 (arguing that "the existing regime for sentencing violations of the Computer Fraud and Abuse Act . . . is based on a conceptual error that consistently leads to improper sentencing recommendations").

348. The CFAA also contains a misdemeanor charging provision. *See* 18 U.S.C. § 1030 (c)(4)(G). In 2014 Attorney General Holder issued a memorandum that provided general policy guidance to prosecutors charging violations under the CFAA. Holder acknowledged that "[a]s technology and criminal behavior continue to evolve . . . it remains important that the CFAA be applied consistently by attorneys for the government and that the public better understand how the Department applies the law." OFFICE OF THE ATTORNEY GENERAL, MEMORANDUM TO THE UNITED STATES ATTORNEYS AND ASSISTANT ATTORNEY GENERALS FOR THE CRIMINAL AND NATIONAL SECURITY DIVISIONS: INTAKE AND CHARGING POLICY FOR COMPUTER CRIMES MATTERS 1 (Sept. 11, 2014). In this article, we are only offering statutory charging provisions but acknowledge the necessity for more nuanced policy guidance to assist prosecutors with making sure a statute is applied consistently.

In light of national shortages in the information security workforce,[349] heavy-handed prosecutions of minors for computer intrusion offenses are likely to result in counterproductive results.[350] If security past is security prologue, it is perhaps precisely the most curious minors who will simultaneously both most often risk running afoul of computer intrusion law as teens and grow into the most gifted, seasoned information security professionals.[351] Although they may lack the judgment of an adult in governing their own code-breaking conduct, erring on the side of offering second chances and constructive rehabilitation opportunities to these minors affords them the chance to use their security talents for the good of society rather than for destructive or criminal purposes.[352]

While we apply this provision of the CIAA to several different scenarios in this Part, it is worth noting now that a violation of the terms of service as the sole piece of "offending" conduct would not result in criminal responsibility under our statute because there has been no CIA impairment to a protected computer. If, however, a CIA impairment did occur to a protected computer, the terms of service may be evidence relevant to understanding the computer owner's consent and whether the conduct was within the scope of the contractual relationship. Similarly, if a security researcher is participating in a bug bounty program and a CIA impairment occurs, the determination of whether the computer owner consented to the researcher's use of the computer will at least partially turn on the terms and scope of the agreement governing the bug bounty program.[353] But, if an individual scrapes information from a publicly available website, there can be no criminal liability unless the scraping causes some impairment of the CIA of the protected computer — the issue of consent does not come into play unless and until there is an impairment of CIA.

---

349. Press Release, (ISC)^2, Global Cybersecurity Workforce Shortage to Reach 1.8 Million as Threats Loom Larger and Stakes Rise Higher (June 7, 2017), https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/06/07/2017-06-07-Workforce-Shortage [https://perma.cc/2GS3-RYPP]; *see also* Tarah Wheeler, *In Cyberwar, There are No Rules*, FOREIGN POLICY (Sept. 12, 2018, 8:00 AM) https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense [https://perma.cc/6UFP-9PRZ].

350. *See, e.g.*, Andrea M. Matwyshyn, *Generation C: Childhood, Code, and Creativity*, 87 NOTRE DAME L. REV. 1979 (2013).

351. *Id.* at 2025–26.

352. *Id.* at 2028–29.

353. In 2017, the Department of Justice issued a document entitled "A Framework for a Vulnerability Disclosure Program for Online Systems." Authored by the Criminal Division's Cybersecurity Unit, the framework "outlines a process for designing a vulnerability disclosure program that will clearly describe authorized vulnerability disclosure and discovery conduct, thereby substantially reducing the likelihood that such described activities will result in a civil or criminal violation of law under the Computer Fraud and Abuse Act (18 U.S.C. § 1030)." U.S. DEP'T OF JUSTICE, A FRAMEWORK FOR A VULNERABILITY DISCLOSURE PROGRAM FOR ONLINE SYSTEMS 1–2 (2017), https://www.justice.gov/criminal-ccips/page/file/983996/download [https://perma.cc/FT4T-H8C9].

This provision of the statute also protects a user from being prosecuted due to a mistake she may make, because the user must either "knowingly" or "intentionally" impair the CIA of a protected computer or information contained in a protected computer. That is, if your cat walks across your keyboard and causes a website to crash, neither your cat[354] nor[355] you will be culpable for a computer intrusion crime.[356] The relevant statutory definitions for aforementioned parts of this provision are as follows:

> **Knowingly**: A person commits an act knowingly if he or she is aware of the act, does not commit the act through ignorance, mistake, or accident, and is aware that his or her conduct could or would result in a confidentiality, integrity, or availability impairment to a protected computer. The government is not required to prove that a person knew his or her acts or omissions were unlawful. Evidence of a person's words, acts, or omissions, along with all other evidence, may be relevant to determining whether that person acted knowingly.[357]
>
> **Intentionally**: A person commits an act intentionally if he or she acts purposefully with the intent that his or her conduct will cause a confidentiality, integrity, or availability impairment to a protected computer. In other words, the person undertakes his or her conduct either intending for, or hoping that, a confidentiality, integrity, or availability impairment to a protected computer will follow. The government is not required to prove that a person knew his or her acts or omissions were unlawful. Evidence of a person's words, acts, or omissions, along with all other evidence, may be relevant to determining whether that person acted intentionally.

---

354. Animals have on occasion been prosecuted for crimes. *See* Francisco Macías, *Animals on Trial: Formal Legal Proceedings, Criminal Acts, and Torts of Animals*, THE LIBRARY OF CONGRESS (Feb. 9, 2016), https://blogs.loc.gov/law/2016/02/animals-on-trial [https://perma.cc/VC6U-YZR9].

355. For a discussion of a hypothetical feline computer intrusion and consequences therefrom, see Matwyshyn, *supra* note 16, at 165–66.

356. *Id.* at 166.

357. This definition is adapted from the Ninth Circuit's model criminal jury instructions. NINTH CIRCUIT JURY INSTRUCTIONS COMM., MANUAL OF MODEL CRIMINAL JURY INSTRUCTIONS FOR THE DISTRICT COURTS OF THE NINTH CIRCUIT § 5.6 (2010).

Confidentiality: the maintenance of technical properties set a priori regarding a system's limitations of data access; the concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations.[358]

Integrity: the preservation of data or system properties set a priori, free from alteration, manipulation, or destruction.[359]

Availability: the preservation of the technical property set a priori regarding the ability of a user to access data in the system; the state when data are in the place needed by the user, at the time the user needs them, and in the form needed by the user.[360]

Impairment: a technologically demonstrable deterioration. The impairment can be temporary or permanent.

Computer (adapted from current CFAA language):[361] 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, unless such device is capable of remote information transmission.

Protected computer (identical to current CFAA language):[362] 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

358. *See* COMPUT. SEC. RES. CTR., *supra* note 243.
359. *See id.*
360. *See id.*
361. *See* 18 U.S.C. § 1030(e)(1) (2012) (adapted from current CFAA language).
362. *See* 18 U.S.C. § 1030(e)(2)(A)–(B) (identical to current CFAA language).

> that use by or for the financial institution or the Government; or
>
> (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.

As we previously discussed, the CFAA is having a chilling effect on security research.[363] In lieu of correcting vulnerabilities discovered by researchers, unsophisticated vendors of vulnerable products sometimes attempt to use the CFAA to threaten researchers into silence. Meanwhile, security researchers face the transaction costs of hiring counsel to defend them not only against frivolous litigation by deep-pocketed plaintiffs, but also against uncertainty of outcome under various jurisdictions' interpretations of the CFAA. Together the forces of litigation and vagueness surrounding the CFAA's core definitions combine to render a legal climate that is inhospitable for security research, despite its benefits to our national security.

The challenge, of course, is to prevent chilling security research while protecting consumers from computer intrusion harms caused by criminals posing as security researchers — either before or after the fact — or by careless researchers who do not put reasonable protections and controls in place in the course of their research. The model language we offer below attempts to strike the appropriate balance between these two objectives and give security researchers more guidance about the circumstances and kind of conduct that could place them in legal jeopardy. More specifically, we attempt to give researchers that engage in good-faith security research and take reasonable precautions to prevent impairment to the CIA of protected computers in the course of conducting that research a "fallback" defense if unintended consequences occur in the course of their research.

As an initial matter, we draft this provision as an affirmative defense, which places the burden on the defendant to prove the defense. That is, while the prosecution has the burden to prove, beyond a reasonable doubt, that the defendant knowingly caused an impairment of CIA to a protected computer and did not have the computer owner's express or implied consent to so do, if the defendant wants to "be excused" from criminal culpability for her activity, the burden shifts to

363. *See* discussion *supra* Section III.A.2.c; *see also Data Security and Bug Bounty Programs: Hearing Before the Subcomm. on Consumer Prot., Prod. Safety, Ins., & Data Sec. of the S. Comm. on Commerce, Sci., & Transp.* 115th Cong. 2 (2018) (statement of Katie Moussouris, founder and CEO, Luta Security) (noting that the CFAA "has caused a chilling effect on security research for defensive purposes").

her to prove that the elements of the security research defense have been met.[364] The language in sections (i)–(iii) below is adapted from the security research exemption granted by the U.S. Copyright Office and Librarian of Congress during the 2015 Digital Millennium Copyright Act Triennial Rulemaking.[365]

In practice, a defendant will have to prove that her actions complied with each element of this provision. That proof may require expert testimony about whether or not the defendant's activities occurred in a controlled environment that was designed to avoid impairment to the CIA of protected computers and harm to the public, as reflected in section (ii) below. A "controlled environment" refers to the exercise of reasonable care in line with the generally accepted standards of the security research community, as such standards evolve from time to time. In other words, this provision sets up a battle of the experts[366] akin to those used during liability determinations in legal or medical malpractice cases. The inquiry into a "controlled environment" asks whether the conduct of a security researcher reflects standard risk minimization practices in light of the potential foreseeable technical damage. More specifically, and likely aided by expert witness testimony, the finder of fact must determine whether, in planning and executing the security research that caused technically cognizable harm, the researcher exercised the care, skill, and diligence that are commonly exercised by other security researchers in similar conditions and circumstances.

A security researcher can never guarantee a particular outcome, and a failure to choose the best research strategy does not necessarily amount to a violation of maintaining a controlled environment. The question, instead, is whether the security researcher crafted and executed a research strategy in good faith that, at the time this strategy is chosen, was reasonable in light of known risks. However, if a reasonably prudent security researcher with the skill and competence level necessary to engage in the undertaken research would not take the same or

---

364. An affirmative defense is "[a] defense in which the defendant introduces evidence, which, if found to be credible, will negate criminal or civil liability, even if it is proven that the defendant committed the alleged acts. Self-defense, entrapment, insanity, necessity, and *respondeat superior* are some examples of affirmative defenses." *Affirmative Defense*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/affirmative_defense [https://perma.cc/SJ7W-EXRC].

365. Exemption to the Prohibition Against Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 208, 65963 (Oct. 28, 2015). Indeed, because of the language of the granted exemption, which references the CFAA expressly, maintaining a harmonized legal approach between these two statutory regimes is paramount. *Id.*

366. An expert witness would, of course, need to be appropriately qualified and accepted by a court before giving testimony. Any evidence or testimony presented to the jury would have to satisfy both *Daubert* and Federal Rule of Evidence 702. *See* United States v. Daubert, 509 U.S. 579, 589–90 (1993) (describing the requirements of expert testimony under Rule 702 as requiring the judge to "ensure that any and all scientific testimony or evidence admitted is not only relevant, but reliable").

similar course of action as that taken by the researcher, there may be a violation of the controlled environment requirement. The government can, of course, offer its own expert testimony to rebut the testimony of the defense expert. In light of courts' extensive experience with legal and medical malpractice claims, they are likely to be comfortable supervising and making evidentiary rulings regarding expert testimony about degree of care in security research design, and juries will be able to make findings of fact about degree of care in security research design, with the assistance of evidence derived from expert testimony.

Moreover, as our model language indicates, the security research affirmative defense can only be raised when a defendant is charged with *knowingly* violating this provision of the statute and not if she is charged with *intentionally* violating the statute — there can be no "good faith security research" if the defendant intentionally caused a CIA harm without the express or implied consent of the computer owner. We apply the security research affirmative defense to a number of scenarios at the end of this Part.

> **Security Research and Testing Affirmative Defense**
>
> (C) An affirmative defense to knowingly impairing the confidentiality, integrity, or availability of a protected computer or information contained in a protected computer, without the express or implied consent of the owner or operator of the protected computer, shall be established if a defendant proves that:
>
> (i) the actions taken by the defendant constituted good-faith testing, investigation, or correction of a security flaw or vulnerability;
>
> (ii) such activity is carried out in a controlled environment[367] designed to avoid impairments to the CIA of protected computers or harm to the public; and
>
> (iii) the information derived from the activity is used primarily to promote the security or safety of the class

367. The language of this section is modeled on the security research exemption granted by the Librarian of Congress and the U.S. Copyright Office in the 2015 DMCA Rulemaking Process. U.S. Exemption to the Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, *supra* note 365, at 65963.

> of devices or machines on which the computer program operates, or the security or safety of the individuals who use such devices or machines.
>
> **Controlled environment**: a controlled environment refers to a planned and executed research design demonstrating the exercise of reasonable care in line with the generally accepted standards of the security research community, as such standards evolve from time to time.

b. Change 2: 1030(a)(2) - Criminal Impersonation with a Credential

In the first provision of our model statute, criminal culpability does not attach unless an objectively testable impairment to the CIA occurs to or on a protected computer, or a defendant engages in an attempt or conspiracy to impair the CIA of a protected computer without the express or implied consent of the owner or operator of the protected computer. But, if Eve guesses Alice's password and logs into Alice's email account, that intrusion is generally not forensically discoverable on the protected computer, as defined in section 1030(a)(1) of our proposal. Eve has tricked the computer into believing she is Alice, and therefore possibly gained access that she was not intended to have. We therefore need a provision that will make Eve criminally responsible for using a credential that does not belong to her to access a protected computer without the express or implied consent of the owner of the credential.

However, the question of "who is the 'owner' of the credential?" should be viewed as a context-dependent analysis. Specifically, one should ask "who is the primary beneficiary of the use of the credential?" In an employer-employee context, the primary beneficiary is the employer. That is, when an employer issues a credential to an employee, it is for the purpose of the employee's performance of work for the employer. In a consumer subscription service context, the primary beneficiary is the consumer. Even with respect to "free" services where a consumer pays with her information, the information is the thing of value that is conveyed in exchange for the services. As such, the consumer is the "owner" of the credential.

By implementing an analysis driven by the concept of criminal impersonation of a credential, we resolve an issue that has long plagued the courts. Courts looking at cases involving the misuse of credentials under the CFAA have, at times, struggled to find the right "hook" under the CFAA. As the confusion raised by *Nosal I, Nosal II,* and *Facebook v. Power Ventures* cases demonstrates,[368] courts and legal scholars

368. *See* discussion *supra* Section II.B.

alike have struggled to fit cases addressing credential abuse within the existing CFAA framework.[369] The CIAA model's analysis of these facts would instead rely on a new theory of "criminal impersonation with a credential," which is built upon the contract and corporate law concept of apparent authority. Ultimately, analysis of the *Nosal* facts with the CIAA model statute would reach the same conclusions as both the *Nosal I* and *Nosal II* courts, but through substantially different analytic paths than those followed by either the *Nosal I or Nosal II* courts.

In *Nosal I*, Nosal and his co-conspirators asked an employee to use active credentials to research certain information. The *Nosal I* court found that an employee does not exceed authorized access under the CFAA by using authorized credentials. Similarly, there would also be no criminal culpability under the CIAA for an employee using credentials issued by an employer to him. Because the employee ran queries that were technologically consistent with his use of the password in the way intended by his employer, the CIAA would find no impersonation. The designated user of the credentials used the credentials as intended. The secondary repurposing of the information is not a computer intrusion question. It is a question better addressed by other bodies of law, such as trade secret law.

In *Nosal II*, Nosal instructed his collaborator, Christian, to obtain source lists from his former employer's proprietary database without the authorization of the employer.[370] Christian, in turn, obtained the login credentials of an administrative assistant who was still an employee of the former employer. As a matter of contract and corporate law, an assistant will rarely if ever possess the requisite level of corporate authority to sublicense a corporate password to a third party. The assistant holds no rights personal to her in that password — the assistant's right to use the password is only a limited-purpose license granted by the employer for its own benefit. The employer is the "owner" of the credential. A corporate login credential is not purchased, created, or terminated by an administrative assistant; instead it is provided to the assistant by the employer solely to perform services on the employer's behalf during a period of employment. The only possessory interest in that credential remains at all times with the assistant's employer, as does the right to issue any sublicenses.

For this reason, Nosal's only potentially viable legal argument would be that he reasonably believed himself to have authority to possess and use the third-party credentials. However, this argument would in part rely on the contract and corporate law doctrine of apparent authority. As used in contract and corporate law, apparent authority refers

369. To avoid these problems, the government and the court in *Nosal II* distinguished exceeding authorized access from lack of authorization.

370. *See* United States v. Nosal (*Nosal II*), 828 F.3d 865, 1031 (9th Cir. 2016).

to the situation where an employee or agent is reasonably judged to have the ability to bind a principal to a promise.[371] In other words, "apparent authority" refers to an agent's semblance of authority where "a principal, through his own acts or inadvertences, causes or allows third persons to believe his agent possesses" that authority.[372] Apparent authority, unlike express or implied authority, derives from the conduct of a principal, communicated or manifested to a third party, which reasonably leads the third party to rely on an agent's authority.[373] To determine an agent's apparent authority, courts ask (1) whether the principal held the agent out as possessing sufficient authority to encompass the act in question, or knowingly permitted the agent to act as having such authority; and (2) whether a party dealing with the agent acted in good faith, reasonably believing under all the circumstances that the agent had necessary authority to bind the principal to the agent's action.[374] An administrative assistant lacks even the patina of apparent authority, and no evidence existed that the employer acted in any manner to the contrary. No reasonable third party would believe that an administrative assistant possessed the authority to contractually bind her employer in credential licensing agreements.[375] And certainly a former employee of the same company should recognize that an administrative assistant does not have the authority to license credentials to third parties on behalf of their shared former employer. Thus, if anyone other than the assistant uses the credential, he "tricks" the system into giving him access to information through an act of impersonation, although this kind of confidentiality harm will not be forensically demonstrable on the system. Our CIAA's provision for criminal impersonation with a credential accounts for this lack of demonstrable forensic evidence.

Thus, under the CIAA's provision for criminal impersonation with a credential (see (A) below), the *Nosal II* facts would expose Nosal to criminal culpability for criminally impersonating the assistant with a credential. Additionally, this provision addresses the issue of trafficking in credentials.

---

371. *See* New England Educ. Training Serv., Inc. v. Silver St. P'ship, 528 A.2d 1117, 1120 (Vt. 1987); Pamperin v. Trinity Mem'l Hosp., 423 N.W.2d 848, 853–54 (Wis. 1988) (noting that under apparent authority, a principal may be liable "for the acts of one who reasonably appears to a third person, through acts by the principal or acts by the agent if the principal had knowledge of those acts and acquiesced in them, to be authorized to act as an agent for the principal").

372. Gordon v. Tobias, 817 A.2d 683 (Conn. 2003).

373. *Silver St. P'ship*, 528 A.2d at 1120.

374. *Gordon*, 817 A.2d at 689.

375. This apparent authority analysis would not apply to the situation where a consumer shares a password to, for example, a video streaming service. A consumer who purchases contract rights to use a password possesses the power to both create and terminate it, and the consumer pays for this privilege. A consumer's sharing of a password after purchasing a license to access content or services constitutes, at best, a contract breach for which adequate remedy is available through contract law.

> Whoever —
>
> (A) intentionally uses a credential without the express or implied consent of the owner of the credential to access a protected computer and intentionally views or uses information that is not viewable on the protected computer without the credential, shall be punished as provided in…; or
>
> (B) knowingly and with intent to defraud traffics (as defined in 18 U.S.C. § 1029) in any credential or similar information through which a computer may be accessed without the express or implied consent of the rightful owner of the credential, if —
>
> (i) such trafficking affects interstate or foreign commerce; or
>
> (ii) such credential is used by or for the Government of the United States;
>
> shall be punished as provided in . . .
>
> Whoever conspires to commit or attempts to commit an offense under this subsection shall be punished as provided in . . .
>
> **Credential**: any symbol, sound, object, process, or other indicator logically associated with or adopted by a person and used for the purpose of verifying the identity of a user as a prerequisite to allowing access to a protected computer or resources in a protected computer.
>
> **Owner of a credential**: the person or entity who is the primary beneficiary of the use of the credential.
>
> **Traffic**: (as defined in 18 U.S.C. 1029) transfer, or otherwise dispose of, to another, or obtain control of with the intent to transfer or dispose of.[376]

376. *See* 18 U.S.C. § 1029(e)(5) (2012 & Supp. II 2015). This provision replaces the substantive provisions in 18 U.S.C § 1030(a)(6)(A)–(B) (2012).

> As we previously noted, this article does not attempt to provide a holistic statutory and sentencing guidelines framework. We would, however, provide a misdemeanor charging provision to give prosecutors the discretion to address first-time violations by minors or others when a "warning notice" is appropriate.

c. Change 3: 1030(a)(3) - Abuse of Government Position of Trust

The CFAA criminalizes the act of intentionally accessing a protected computer and obtaining information in a way that exceeds authorized access.[377] As noted in the DOJ intake and charging policy document, "in several circuits, violation of the statute under the exceeds-authorized-access theory might occur where an employee accesses sensitive corporate information in violation of the company's access policy or where a law enforcement officer accesses the National Crime Information Center ('NCIC') computers to obtain information in order to stalk a former romantic partner, which would violate NCIC's access restrictions."[378] Our criminal computer intrusion provision eliminates the exceeds-authorized-access prohibition and replaces it with a theory of computer intrusion requiring that a defendant, without the express or implied consent of a computer owner, knowingly or intentionally impairs the confidentiality, integrity, or availability of the protected computer or information contained in the protected computer. Accordingly, the CIAA criminal computer intrusion provision would not criminalize the aforementioned exceeds-authorized-access conduct *unless* an impairment to the CIA of a protected computer has occurred.

We understand that the current exceeds-authorized-access theory serves the important function of deterring (and punishing) government employees or contractors serving in positions of trust from accessing or using sensitive or classified information for non-governmental purposes.[379] This new provision addresses those policy objectives. It does not, however, change current law with respect to existing whistleblower protections.

> Whoever, having signed an agreement imposing a duty of confidentiality, which may include restrictions on the access and use of non-public information contained in a government computer, as a requirement for

377. 18 U.S.C. § 1030(a)(2)(C).

378. Intake and Charging Policy for Computer Crimes Matters, *supra* note 348, at 4.

379. *See id.* at 3 ("Many types of offenses under the CFAA can have an impact far beyond the particular computer that is directly affected by the actions of the offender. Unauthorized access [or exceeding authorized access] to a computer containing classified information, for example, can harm national security.").

> government employment, or for permission to access a government computer or information contained in government computers not otherwise available to the public, and —
>
> (A) intentionally accesses any nonpublic computer owed or used by a department or agency of the United States for a non-governmental purpose that would violate the proscribed duty of confidentiality; or
>
> (B) intentionally obtains, transmits, or uses information contained in any nonpublic computer owned or used by a department or agency of the United States for a non-governmental purpose that would violate the proscribed duty of confidentiality —
>
> shall be punished as provided in . . .
>
> Whoever conspires to commit or attempts to commit an offense under this subsection shall be punished as provided in . . .
>
> (C) Rule of Construction — Nothing in this provision may be construed as limiting whistleblower protections provided by state or federal laws.

d. Change 4: 1030(a)(4) - Epidemic Malware

While placing a contagious individual in quarantine may protect a population from further infection through contact with that particular individual, this isolation of infected carriers is still not enough to prevent future outbreaks. Instead, the target of modern epidemiology is the creation of "herd immunity." In other words, the goal of epidemiology is not merely containment of outbreaks; it equally targets the prevention of epidemics.

In July of 2014, the Senate Judiciary Subcommittee on Crime and Terrorism held a hearing entitled, "Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks."[380] In Senator Whitehouse's opening statement, he highlighted the need for

380. *See Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks: Hearing Before the Subcomm. on Crime & Terrorism of the S. Comm. on the Judiciary* 113th Cong. 2 (2014) (opening statement of Rep. Sheldon Whitehouse, Chairman, Judiciary Subcomm. on Crime and Terrorism).

an approach to botnet takedowns that is grounded in a solid legal foundation and protects consumer privacy, with the understanding that Congress should not dictate tactics for botnet disruption.[381]

In addition to the need to ensure there is a "solid legal foundation" for botnet takedown efforts, it is important to recognize that a few cases of botnet takedowns have resulted in suboptimal outcomes, potentially due to unforeseen consequences of the particular take down method selected.[382] Currently, no outside technical expertise is required in the initial structuring of the remediation strategy and the determination of an appropriately harm-minimizing response. Particularly because of the challenge of understanding the technical minutiae of malware for a judge or even public and private litigants, the use of outside technical experts would add a valuable buffer to the process currently in use. Similarly, just as courts came to recognize the benefits of a formalized bankruptcy process with a written, documented plan of liquidation or re-structuring[383] and state corporate law formalized the process of corporate dissolution through a plan of dissolution,[384] the same sort of formal written documentation would create a valuable feedback loop to learn from successes and errors. Thus, we propose a more formalized botnet[385] dissolution process. This process is expressly inspired by the idea of disclosure plans in bankruptcy and corporate law, buttressed by the idea of outside experts — another concept borrowed from bankruptcy law.[386]

While the problem of botnets specifically has been highlighted by the DOJ in their requests for additional authority under the CFAA, the issues of malware that self-propagates is broader than simply the problem of botnets. A tight botnet focus does not consider past self-propagating malware such as the Morris worm, nor does it address the

---

381. Rep. Whitehouse noted that "Congress . . . cannot and should not dictate tactics for fighting botnets," but it should make sure that "there is a solid legal foundation for enforcement actions against botnets and clear standards governing when they can occur," that "botnet takedowns and other actions are carried out in a way that protects consumers' privacy," and that "our laws respond to a threat that is constantly evolving, and encourage, rather than stifle, innovative efforts to disrupt cyber criminal networks." *Id.*

382. *See* discussion *supra* Section II.C.2.

383. For a discussion of plans of liquidation in bankruptcy proceedings, see U.S. COURTS, *Chapter 7 - Bankruptcy Basics*, http://www.uscourts.gov/services-forms/bankruptcy/bankruptcy-basics/chapter-7-bankruptcy-basics [https://perma.cc/7UBZ-CATP]; *see also* Richard L. Epling, *Proposal for Equality of Treatment for Claims in Chapter 7 and Claims in A Liquidating Chapter 11 Case*, 4 BANKR. DEV. J. 399, 401 (1987) ("a significant minority of courts has required liquidation through the vehicle of a plan").

384. *See* Bob Eisenbach, *You Say You Want A Dissolution: An Overview Of The Formal Corporate Wind Down*, IN THE (RED) (Feb. 24, 2015), https://bankruptcy.cooley.com/2015/02/articles/the-financially-troubled-company/you-say-you-want-a-dissolution-an-overview-of-a-formal-corporate-wind-down [https://perma.cc/E5VA-WDH3].

385. Our proposal extends beyond merely botnets to a broader category of "epidemic malware."

386. The Bankruptcy Act explicitly refers to a "privacy ombudsman" who assists the court in bankruptcies with sensitive data assets. 11 U.S.C. § 332 (2012).

inevitable future attacks akin to WannaCry.[387] For these reasons, the CIAA adopts a forward-looking statutory framework with a broader approach to malware, encompassing not only botnets but also the entire family of malware that impacts machines for purposes of criminal remote command and control or self-propagation.

Accordingly, we offer a new statutory construct — epidemic malware — with a structured, public-private cooperative-takedown framework again inspired by epidemiology theory. The general idea of applying an epidemiological lens to questions of security has been previously introduced. For example, professors Santiago Gil, Alexander Kott, and Albert-Laszlo Barabasi have advocated a genetic epidemiology approach to cybersecurity and proposed "a methodology to associate services to threats inspired by the tools used in genetics to identify statistical associations between mutations and diseases."[388] Their approach also allowed for determination of "probabilities of infection directly from observation, offering an automated high-throughput strategy" for developing comprehensive metrics for security.[389] Professor Stefan Savage has also conceptually applied epidemiology-like concepts to the analysis of effective vulnerability notifications.[390] Stuart Staniford, Vern Paxson, and Nicholas Weaver have argued for the need to develop a "'Center for Disease Control' analog for virus- and worm-based threats to national cybersecurity."[391] This article is, however, the first legal scholarship to advocate for drawing upon an epidemiology-based approach to questions of security[392] and reforming aspects of the CFAA in line with these insights.

---

387. *See generally* Santiago Gil et al., *A Genetic Epidemiology Approach to Cyber-Security*, 4 SCI. REPS. 5659 (2014).

388. *Id.*

389. *Id.*

390. *See generally* Frank Li, Zakir Durumeric, Jakub Czyz, Mohammad Karami, Michael Bailey, Damon McCoy, Stefan Savage, & Vern Paxson, *You've Got Vulnerability: Exploring Effective Vulnerability Notifications*, 25 USENIX SEC. SYMP. (2016), http://cseweb.ucsd.edu/~savage/papers/USESEC16.pdf [https://perma.cc/F66Q-623F].

391. Stuart Staniford, Vern Paxson, & Nicholas Weaver, *How to 0wn the Internet in Your Spare Time*, 11 USENIX SEC. SYMP. 16 (2002), https://www.usenix.org/legacy/event/sec02/full_papers/staniford/staniford.pdf [https://perma.cc/3JUD-HDT4].

392. Prior law review literature has examined questions of health security, meaning access to medical care and prevention of disease, through the lens of epidemiology, but this type of security is outside the scope of this inquiry. *See, e.g.* David P. Fidler, *Return of the Fourth Horseman: Emerging Infectious Diseases and International Law*, 81 MINN. L. REV. 771, 775 (1997) (arguing that examining infectious diseases in connection with the nature of international relations clarifies that the emergence and reemergence of infectious diseases pose threats of the most serious magnitude). Physical security, social epidemiology, and international law has also been considered by one article. Sevgi Aral et al., *Health and the Governance of Security: A Tale of Two Systems*, 30 J.L. MED. & ETHICS 632 (2002) ("Research in social epidemiology suggests that a shared sense of security from physical violence and interference with property can contribute to better community health.").

This new "epidemic malware" provision creates a structure for public-private takedown operations in situations where self-propagating malicious code threatens the safety of protected computers *en masse.* Through independent DHS epidemic malware designation, the creation of a dissolution plan, the involvement of an independent technical expert in approval of the dissolution plan, and annual congressional reporting requirements, we offer a structure to frame existing botnet takedown efforts and future public-private mass incident response and remediation efforts. Moreover, while litigants might be inclined to use any epidemic malware provision for intellectual property enforcement, intellectual property theft does not fall within the definition and corresponding scope of activity addressed through the epidemic malware provision.

Because experts agree that the hardest part of these epidemic malware interventions are technical, rather than legal,[393] we would recommend that Congress add a sunset provision for the purpose of "forcing" a congressional-level evaluation of how the statute actually worked in practice and the consideration of any needed reforms for reauthorization.

> Procedure for the takedown of epidemic malware by the Government or by a private entity in partnership with the Government:
>
> (1) A private entity whose systems, networks, or computers are infected with epidemic malware or whose customers' systems, networks, or computers are infected, or likely to be infected, by epidemic malware may make an application to a federal district court for an order authorizing the takedown of the epidemic malware. The Government may also independently make an application to a federal district court, which must be signed by the Attorney General, the Deputy Attorney General, or an Assistant Attorney General from either the Criminal Division or the National Security Division, authorizing the takedown of epidemic malware.[394] Each application shall include the following information —

393. *See generally* CyCon US 2018 Botnet Takedown Panel, *supra* note 165.

394. The DOJ should ensure that the notice process used in connection with this epidemic malware provision comports with minimum constitutional standards of notice. In addition, when the government is making an application for a takedown of epidemic malware, it still has the obligation to seek applications for additional orders to address Fourth Amendment concerns that may be implicated in takedown efforts.

(a) An epidemic malware designation: a written certification by an official at the Undersecretary level, to be designated by the Secretary of DHS, that the malware identified by the private party or the government is epidemic malware;

When making an epidemic malware designation, the certifying official shall consider but not be limited to the following factors and shall document the analysis and factors considered in making the certification:

(A) a recent increase in amount or virulence of the malware;

(B) the recent introduction of the malware into a setting where it has not been seen before;

(C) an enhanced mode of transmission so that more susceptible machines and systems are exposed;

(D) a change in the susceptibility of the targeted systems, or factors that increase target exposure or involve introduction through new methods of transmission.

(b) An explanation of how the epidemic malware is affecting the products, services, networks, computers, or systems of the private entity or its customers or, when the application is being made by the government, an explanation of harms being caused by the epidemic malware;

(c) A plan of dissolution and notice, approved by a technical advisor from a court-appointed list, that contains —

(i) an assessment of the harm or potential harms to the private entity, its customers, other members of the public, or other networks or systems if the epidemic malware at issue is not disrupted;

(ii) an assessment of the harm or potential harm to members of the public or other networks or systems if the epidemic malware takedown is allowed;

(iii) a description of how the private party or the Government plans to execute the takedown of the epidemic malware, to include any cooperation or assistance to be provided to the private entity by the Government or other third parties assisting the private entity or the Government;

(iv) a description of how the Government or the private entity making the application and any Government agencies or third parties assisting in the takedown effort will protect personally identifiable information of affected members of the public;

(v) a description of steps or processes that will be taken to minimize foreseeable harms identified in (ii), along with remediation and escalation processes that will be put in place to remediate any unintended impact on a private entity's customers, the security of other members of the public, or other networks or systems;

(vi) a description of how notice will be provided to all reasonably foreseeable impacted parties, to include any cooperation or assistance to be provided by the Government or other third parties; and

(vii) when a private entity is making an application, a proposed bond amount that will be posted to cover potential damages to third parties during the takedown effort.

(2) Upon such application, the judge may issue an order granting the application for takedown of epidemic malware, as represented in the plan of dissolution and notice or as modified by the court, if the judge determines on the basis of facts contained in the application that the proposed takedown is primarily for the purpose of mitigating a DHS-designated epidemic malware outbreak or the potential for such an outbreak and that the applicant is taking reasonable steps to protect personally identifiable information of affected members of the public, to minimize foreseeable harms, and to provide notice to all reasonably foreseeable impacted parties. When a private entity is making an application for takedown of epidemic malware, the

court must also find that either the private entity or its customers are infected with or are likely to be infected with epidemic malware.

(3) Prior to granting the application, the court may schedule an ex parte hearing to obtain additional testimony or other evidence from the private entity making the application, the Government, or the technical advisor. If the technical advisor does not approve the applicant's plan of dissolution and notice, the applicant may request a hearing to resolve any deficiencies raised by the technical advisor. If a hearing is scheduled, the private party making the application or the Government may make a motion to seal the courtroom, which the court shall grant if it finds that a public hearing could result in any of the factors described in paragraph (5).

(4) Upon certification by the Attorney General that a takedown effort will disrupt a serious criminal or national security investigation, and no condition or combination of conditions in the dissolution plan can mitigate the disruption, the court may delay the granting of the application for takedown for a reasonable time to accommodate the legitimate needs of the investigation.

(5) Upon such application, either the private entity making the application or the Government may make a motion to seal the application, which the court shall grant if the court determines that disclosure of the application could result in the following —

(A) endangering the life or physical safety of an individual;

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) thwarting or disrupting the takedown plan proposed in the application; or

(E) otherwise seriously jeopardizing an investigation.

(6) Following the completion of any epidemic malware takedown effort authorized by the court, the application, order, and other related filings shall be unsealed. The party making the application or the Government can make a motion to delay the unsealing for up to 30 days if the court finds that unsealing could result in one of the factors described in paragraph (5). The private party making the application or the Government can make a motion to continue the delay on or before the expiration of any previous order granting a delay.

(7) Technical Advisor — the technical advisor referenced in paragraph (1)(c) is a neutral party with the appropriate technical expertise to review and approve plans for dissolution and notice, and to advise the court on technical matters arising in the course of assessing and granting the Government's or a private entity's application to take down epidemic malware. The DHS shall assist the Administrative Office of the Courts in recruiting a group of individuals who are not full-time Government employees who can serve as technical advisors for courts around the country. The Administrative Office of the Courts shall publish and keep an up-to-date list of approved technical advisors on its website. Private entities or Government agencies that are preparing applications to take down epidemic malware should contact the Administrative Office of the Courts about making arrangements for a technical advisor to become engaged in the pre-application preparation process with the private entity. At the end of the engagement of the technical advisor, the Government agency or private entity making the application or who utilized the services of a technical advisor for the purpose of making an application, shall reimburse the Administrative Office of the Courts for the services performed by the technical advisor. The DHS shall complete an annual review of the technical advisor list to ensure that an appropriate number of technical advisors with the appropriate skill level are available.

(8) Guidance — the Secretary of Homeland Security, in consultation with the Attorney General and the Federal Trade Commission, shall create and publish on

the DHS website guidance and rules for the epidemic malware designation process and best practices and procedures for notice to parties that may be impacted by takedown efforts.

(9) Annual report — beginning one year after the enactment of the epidemic malware provision, the DHS, in conjunction with the Administrative Office of the Courts, shall publish an annual report containing the following information —

(a) How many applications for takedown of epidemic malware were made, and how many were granted;

(b) How long each individual takedown effort took with respect to each application;

(c) For each individual takedown effort:

(i) an approximation of how may individual third-party or consumer computers, devices, or systems were defended;

(ii) how many individual consumer or third-party computers, devices, systems, or networks experienced confidentiality, integrity, or availability harms in the course of the takedown effort that were anticipated and discussed by the plan of dissolution approved by the technical advisor;

(iii) how many individual consumer or third-party computers, devices, systems, or networks experienced confidentiality, integrity, or availability harms in the course of the takedown effort that were not anticipated or discussed by the plan of dissolution approved by the technical advisor;

(d) Any other information — which can be presented in the form of a summary, if appropriate — that will educate Congress and the public on benefits, risks, and lessons learned from the year's takedown efforts. The DHS should consult with the technical advisors involved in the year's takedown efforts and relevant Government agencies, to include the DOJ and the

FTC. The DHS may also consult with any other experts, affected third parties, or foreign partners that assisted with or were impacted by the takedown efforts.

(e) Both the DHS and the Administrative Office of the Courts shall assist with the collection of information necessary for the DHS to complete the analysis in (a)–(d) above. Private entities that receive court authorization to take down epidemic malware shall provide the DHS or the Administrative Office of the Courts with information necessary for the DHS to complete the analysis in (a)–(d) above.

(9) Definitions. As used in this chapter —

(a) **Epidemic malware** means software whose primary function is to:

(1) cause an impairment in confidentiality, integrity, or availability of multiple protected computers without the express or implied consent of the owners[395] of the protected computers and;

(2) take partial or complete control over the protected computers' operation without the consent of the owner for purposes of using the protected computers in (i) criminal activity coordinated through technical means or (ii) self-propagation and infection of additional protected computers.

(b) **Personally identifiable information** ("PII"), as defined in OMB Memorandum M-07-1616, refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for a private entity or government agency to recognize that non-PII can become PII whenever

395. This lack of consent prevents the misclassification of voluntarily-downloaded peer-to-peer networking software as epidemic malware. Again, the epidemic malware provision is not intended to be used by intellectual property holders for policing infringing behavior.

additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual.[396]

1030(a)(5) Trafficking Epidemic Malware

Whoever —

(a) knowingly and with the intent to commit a CIA impairment to a protected computer traffics (as defined in 18 U.S.C. 1029) in any epidemic malware; or

(b) intentionally acquires access to a protected computer infected with epidemic malware with the intent to commit a CIA impairment to a protected computer shall be punished as provided in . . .

Whoever conspires to commit or attempts to commit an offense under this subsection shall be punished as provided in . . .

Traffic: (as defined in 18 U.S.C. 1029) means transfer, or otherwise dispose of, to another, or obtain control of with the intent to transfer or dispose of.[397]

Epidemic malware means software whose primary function is to:

(1) cause an impairment in confidentiality, integrity, or availability of multiple protected computers without the express or implied consent of the owners of the protected computers; and

(2) take partial or complete control over the protected computers' operation without the consent of the owner for purposes of using the protected computers in (i) criminal activity coordinated through technical

396. *Rules and Policies - Protecting PII - Privacy Act*, U.S. GEN. SERVS. ADMIN., https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act [https://perma.cc/S4GL-33LA].

397. *See* 18 U.S.C § 1029(e)(5) (2012). This provision replaces the substantive provisions in 18 U.S.C. § 1030(a)(6)(A)–(B) (2012).

means or (ii) self-propagation and infection of additional protected computers.

e. Change 5: Elimination of the Civil Provisions

The proposed language above intentionally eliminates civil claims under the CFAA. To estimate the potential impact of this proposed elimination, we conducted an analysis of CFAA cases in calendar year 2018. As the findings of the study set forth below suggest, the removal of the CFAA civil provision appears unlikely to limit current plaintiffs' ability to obtain recourse materially because other adequate avenues appear to exist under existing non-CFAA statutory frameworks and common law actions. Instead, our findings suggest that removal may prove to be desirable for reasons of innovation policy and prevention of potentially retributive use of the CFAA.

(1) The inquiry in brief: To query the possible effect that eliminating the civil provisions of the CFAA may have on common CFAA fact patterns, we conducted an analysis of 80 civil CFAA cases decided between January 1, 2018 and December 31, 2018.[398] Coding these cases based on pled claims for civil recourse and legal merit as determined by the court, we sought to identify the extent to which harmed parties would have been deprived of recourse had the CFAA civil provision not existed. We also sought to identify cases arising from competition-related disputes, i.e. those with the greatest likelihood of negatively impacting future innovation. If employers and competitors use the CFAA as a sword to limit employee mobility, startup creation and competitive enterprise development, this anti-competitive behavior will result in economy-wide harms, hindering the next generation of technology innovation and the free-flow of competitive goods and services.[399]

(2) Hypothesis: Specifically, we hypothesized that (1) a majority of the civil CFAA disputes would involve matters of competition (companies suing employees, contractors or competitors, or business partners suing each other); and (2) in a majority of the substantively-resolved civil CFAA competition cases,[400] the CFAA civil claim would be dismissed or

398. *See infra* note 403.

399. For a discussion of "digital peonage" and anti-competitive CFAA usage, see Andrea M. Matwyshyn, The Law of the Zebra, *supra* note 16.

400. *See* discussion of epidemic malware, *supra* Section III.A.

functionally redundant because alternative means of statutory or common law redress were alleged by the plaintiff and the claims are deemed potentially valid by the court.[401]

(3) Sample: The initial sample pulled from Westlaw[402] consisted of the 205 CFAA cases[403] — the set of all CFAA cases our query yielded that were decided between January 1, 2018 and December 31, 2018 . We discarded criminal CFAA cases and civil CFAA cases that only tangentially referenced CFAA claims or were procedural dispositions without adequate facts for analysis. In other words, we eliminated cases whether the merits of the CFAA claim were not evaluated by or decided by the court. This left a final sample of 80 civil CFAA cases. (N=80).[404]

(4) Methodology:[405] We read all cases in the final sample, coding them based on the claims asserted by each party, the nature of the relationship between the plaintiff and the defendant, and whether the CFAA claim was deemed potentially meritorious by the court.

In particular, we sought to identify any cases where plaintiff's only claim was under the CFAA's civil recourse provisions. Additionally, we sought to identify cases that might harm innovation: cases involving the CFAA and competition (employers, contractors and competitors) implicate contravening public policy concerns regarding innovation that are central to other bodies of law, such as employment law and antitrust regulation. As such, it is these more established bodies of law which arguably should provide the dispositive guidance in determining whether an actionable harm has occurred. Permitting CFAA claims to negate the carefully-constructed balance between innovation and sanction created by these other bodies of law would arguably undercut generations of established doctrine and damage innovation interests. Similarly, a high rate of non-meritorious CFAA civil

401. Specifically, the CFAA claims were plead alongside other civil claims arising out of the same nexus of facts.

402. The Westlaw query was last run on April 15, 2019, in the ALL-FEDS database using the query "computer fraud and abuse act" or "CFAA" or (("18 USCA" /2 1030) or ("18 U.S.C.A." /2 1030) or ("Computer Fraud #and Abuse Act")).

403. Cases on file with authors.

404. This study should be replicated with a larger sample.

405. The analysis conducted in this study reflects a hybrid methodology driven by caselaw and doctrinal analysis.

claims may signal the functional use of the CFAA civil provisions as a type of transaction cost sanction, as would potentially the use of a CFAA civil claim as a counterclaim.

(5) Data:

Table 1: 2018 Civil CFAA Cases (N=80)

	Competition-related	Other	Total
Civil CFAA cases	64	16	80
CFAA claim dismissed (with or without prejudice)	33	12	45
CFAA claim survives	31	4	35
Presence of non-CFAA basis for recourse in surviving claims	29	4	33
CFAA counterclaims	6	1	7
CFAA counterclaim survives	4	0	4

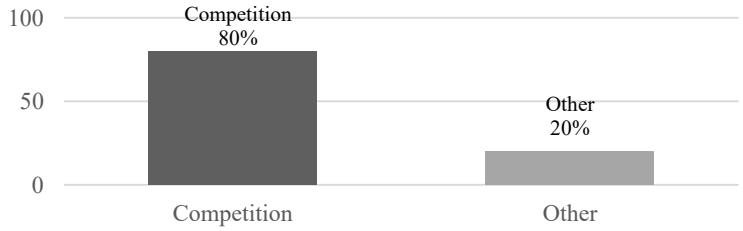

Figure 1: 2018 Civil CFAA Claims by Litigant Relationship (%)

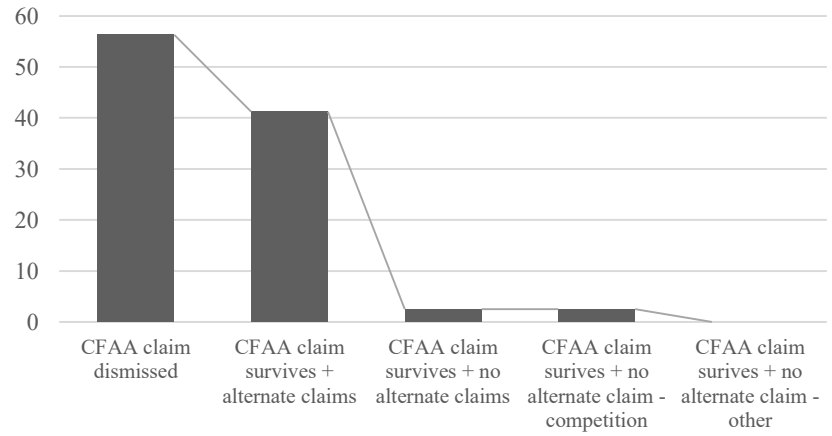

Figure 2: 2018 Civil CFAA Claim Dismissals (%)

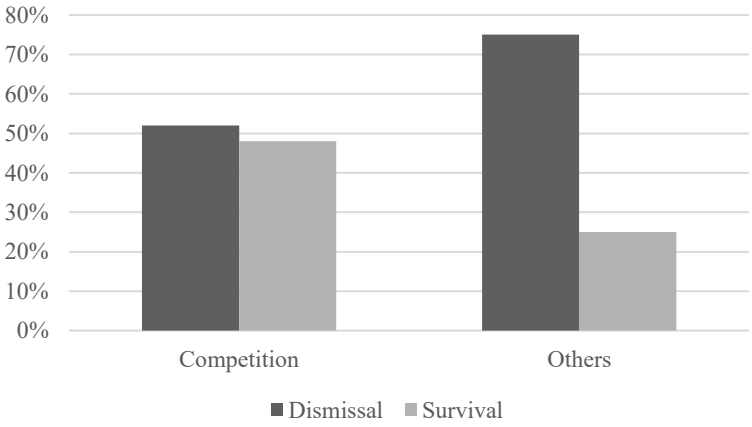

Figure 3: 2018 CFAA Civil Claims Rate of Dismissal (%)
by Litigant Relationship (N=80)

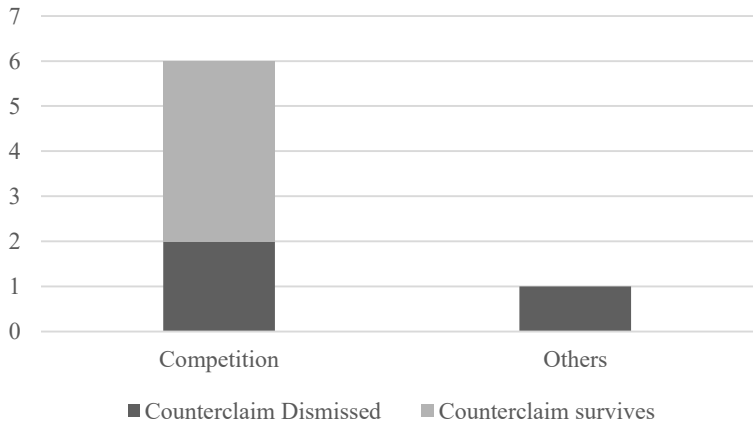

Figure 4: 2018 CFAA Civil Counterclaims Rate of Dismissal (%) by Litigant Relationship (N=7)

(6) Analysis: We found that 64 out of 80 (80%) of the civil CFAA disputes in the sample involved disputes over competition (alleged computer intrusion by employees, contractors, competitors or business partners). The remaining 16 cases civil cases involved various other fact patterns, only 4 (25%) of which were deemed to present a potentially meritorious CFAA claim. In contrast, among the competition cases, 31 (48%) were deemed potentially meritorious under the CFAA. In other words, the dismissal rate in civil CFAA cases for competition cases was approximately 52%, while the dismissal rate for other CFAA civil cases was substantially higher -75%. In the surviving competition claims, 29 out of 31 (94%) included other viable legal avenues for redress other than the CFAA. Among the other surviving CFAA civil claims, 4 out of 4 (100%) included other viable legal avenues for redress outside the CFAA. Seven cases presented counterclaims (9%). Six involved competition; one involved other matters. Among these CFAA counterclaim cases, the only counterclaims which survived (4 out of 6), were all competition-related. Based on this data, competition-related civil CFAA cases appear to demonstrate different dynamics than non-competition related civil CFAA cases. Because the competition-related CFAA civil cases directly implicate innovation policy concerns and threaten to potentially recalibrate the legal balance set by other bodies

of law, these results raise concern about the practical dynamics of CFAA usage by civil litigants for potentially anti-competitive reasons.

(7) Conclusions: The study appeared to support both of our hypotheses. A majority of the civil CFAA disputes in our sample involved matters of competition (companies suing employees, contractors, or competitors, or business partners suing each other). In a majority of these substantively-analyzed civil CFAA competition cases in our sample, the CFAA civil claim appears to have been nonviable and was dismissed or dismissed without prejudice. Among the cases where the CFAA civil claim was potentially meritorious, alternative means of statutory or common law redress appeared to exist to compensate the claimant for any compensable harms in almost all cases. Thus, based on the analysis of our sample of CFAA civil cases from 2018,[406] we conclude that returning the CFAA to its original form as a solely criminal statute is unlikely to significantly correlate with foreclosing civil redress for most plaintiffs currently including CFAA civil claims in their pleadings.

In summary, we believe that elimination of the civil provisions of the CFAA is both a feasible and desirable approach. It would eliminate both the CFAA "double whammy" problem and the CFAA doctrinal swapping problem, likely resolving both existing CFAA circuit splits.[407] Despite our strong belief that elimination of the civil provisions is the preferable approach, if Congress is unwilling to reform the CFAA without including a civil provision, two issues must be highlighted. First, all CFAA caselaw prior to the enactment of the CIAA relating to provisions or terms replaced by the CIAA should be viewed as non-precedential for interpretation of the CIAA. Second, legislators should reevaluate the current conceptions of loss and damages requirements.[408] Because of the CIAA's dramatically revised framework focused on demonstrable technical harms, we expect that the new strands of civil claims would reflect a materially diminished set of innovation

406. As with every study, this study embodies certain methodological limitations. In particular, it should be replicated with a larger sample that is drawn over a longer period of time to ensure that the sample used in our study is, in fact, representative of CFAA civil cases broadly. Because we only looked at cases from 2018, our data does not reflect whether those claims dismissed without prejudice were ever refiled and re-adjudicated meritoriously.

407. For further discussion of the circuit splits, see *supra* note 37 and accompanying text.

408. For example, in light of the time value of money, even the statutory minimum amount of $5000 required by 18 U.S.C. 1030(g) translates to at least $8000 in 2018 dollars. *See Inflation Calculator*, CPI INFLATION CALCULATOR, http://www.in2013dollars.com/1996-dollars-in-2018?amount=5000 [https://perma.cc/L9TJ-3ZTT].

policy concerns. Thus, even if a civil provision that allows private parties to sue for CIAA violations remains, its interpretation will be significantly transformed going forward due to the CIAA's new framework. However, as stated above, we believe that elimination of the civil provision is the preferable approach.

B. How the CIAA Would Work in Practice

In this section, we apply our model CIAA language to several different hypotheticals. These hypotheticals are modeled after litigated CFAA scenarios wherever possible.

1. Hypothetical #1: The Malicious Third-Party Intruder

Mallory decides to rob a bank. Mallory runs tools to identify unpatched vulnerabilities in the bank's networks and exploits a vulnerability to gain access to the accounts and siphon off funds. She withdraws $500,000.00 from a corporate account and manipulates the system logs to hide her tracks.

Analysis:

(1) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a protected computer? Yes, both confidentiality and integrity impairments exist. A confidentiality impairment occurred because Mallory caused the system to grant her access to information that the system was not *a priori* configured to permit. An integrity change occurred because she changed the files in the system in a way that the system was not *a priori* configured to permit.

(2) Was there express or implied consent? No.

(3) Was there knowledge or intent to harm? Yes, both knowledge and intent to harm.

Criminal culpability is possible for Mallory under the CIAA.

(b) Sybil, a foreign operative, finds a non-public Pentagon military purchase order system and generates an order. Based on the number, she enumerates the purchase order ID, which allows her to read additional orders that she did not create. She then deletes her order.

Analysis:

(1) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a protected computer? Yes, an integrity impairment exists because Sybil created a false

purchase order on a non-public system[409] and a confidentiality impairment exists because she accessed purchase orders that the system, as *a priori* configured, did not permit her to read. It could also be argued that there was an availability impairment due to the fact that a previously created purchase order is no longer viewable.

(2) Was there express or implied consent? No. The system was not publicly-viewable and no express or implied consent was provided.

(3) Was there knowledge or intent to harm? Yes, both knowledge and intent to harm.

Criminal culpability is possible under the CIAA.

2. Hypothetical #2: The Infrastructure Disrupter

An organized criminal enterprise exploits a security vulnerability in a stock exchange quote relay system. This enterprise transposes two digits in some of the stock prices which are pushed out to all market participants. These erroneous prices result in high-frequency trading platforms executing millions of trades based on the faulty information. A flash crash in the market results.

Analysis:

(1) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a protected computer? Yes, an impairment of integrity occurred with the transposing of digits.

(2) Was there consent by the owner of the protected computer? No.

(3) Was there knowledge and intent to harm? Yes.

Criminal culpability is possible under the CIAA.

3. Hypothetical #3: The Security Researcher

Alice, a security researcher, runs a port scan and determines that a port that should be secured is vulnerable to an attacker. She incorporates this information in an anonymized form in a conference presentation.

Analysis:

409. The analysis is dependent on the non-public nature of the system. For an analysis of an enumeration on a public system, see *infra* Hypothetical #10.

(1) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a protected computer? No. Alice's actions did not change any of the *a priori* system settings. There is no impairment to the CIA of a protected computer.

No criminal culpability is possible under the CIAA.[410]

(b) Faythe, a security researcher, is hired by the owner of a company to perform a security audit and to penetration test the company's network. The company, via a typo communicated in an email, provides Faythe with the wrong IP address related to the company's system. Using the IP address provided by the company, Faythe accesses the IP address and uses a security vulnerability to pivot into a system where she sees proprietary information belonging to a company that did not employ her. Faythe realizes her error, stops in place, and immediately reports her mistake to the owner of the harmed system.

Analysis:

(1) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a protected computer? Yes, a confidentiality and/or integrity impairment. By accessing the system as she did, Faythe was able to view information not available based on the system's *a priori* settings. She may also have impaired the integrity of the system because as she pivoted into the system, she may have changed some of the information in the system.

(2) Was there express or implied consent? No, not by the owner of the damaged system.

(3) Was there knowledge or intent to harm? While there is no intent to harm on Faythe's part, there is possible knowledge. The security research defense may be appropriate. Expert testimony will establish whether Faythe took reasonable precautions before executing her security audit. For example, should she have tested to confirm the company's IP address range, rather than relying on information provided by the company itself?

There is possible criminal culpability under the CIAA for Faythe. However, even if the prosecutor determines that there was knowledge on Faythe's part, it may be appropriate not to charge Faythe or, at best,

410. It is noteworthy that the DOJ has stated publicly that port scans do not constitute unauthorized access under the CFAA. Aaron Boyd, *More from Black Hat: DOJ Official Draws Line Between Cyber Crime, Legitimate Research*, FED. TIMES (Aug. 5, 2015), https://www.federaltimes.com/2015/08/05/more-from-black-hat-doj-official-draws-line-between-cyber-crime-legitimate-research [https://perma.cc/8CZ5-DEZF].

to charge her with a misdemeanor, particularly if this is Faythe's first offense. The fact that she immediately reported her mistake to the owner of the damaged system should serve as a mitigating factor.

4. Hypothetical #4: The Scared Consumer

(a) Erin, a security researcher, builds a tool to test for Heartbleed, a vulnerability that can disclose sensitive information from the memory of a remote system. Erin publishes her tool on her security research website with a statement indicating that it can be used to test for the Heartbleed vulnerability on websites. Erin is not aware, however, that her tool has a flaw that can cause a system to disclose memory contents and subsequently crash.

(b) Bob, a consumer, googles Heartbleed and finds Erin's tool on her website. Bob is worried that his online bank account may be vulnerable to Heartbleed and runs Erin's tool against his online banking website. Erin's tool causes the site to disclose memory contents and crash.

Analysis:

(1) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a protected computer? Yes, an availability and a confidentiality impairment. The system crashing is an impairment in availability. An impairment in confidentiality occurs because the tool caused the system to display information not otherwise available based on *a priori* settings.

(2) Was there express or implied consent? No.

(3) Was there knowledge or intent to harm? There was no knowledge or intent to harm on Bob's part. But, there is possible knowledge on Erin's part. Erin posted the tool on her public website, indicating it could be used (and she could clearly foresee it would be used) by consumers to check for Heartbleed on third-party websites. If charged, the security researcher affirmative defense could be appropriate. Expert testimony would be used to determine whether Erin crafted and executed a research strategy in good faith, and, that at the time this strategy was chosen and executed, was reasonable in light of known risks. For example, did Erin take appropriate steps to test her tool before releasing it publicly and otherwise minimize risk of possible harm?

There is possible criminal culpability for Erin under the CIAA.

5. Hypothetical #5: The Script Kiddie

Oscar, a fourteen-year-old, finds a script on the Internet that, when executed, causes websites with a certain kind of vulnerability to crash. Oscar runs the script against his school's website and the website crashes. A forensic investigation conducted by local authorities reveals that the script originated from Oscar's home computer. When Oscar is interviewed about the matter by school personnel, Oscar indicates that he was "trying to learn how to be a security researcher and messed up." A kid on Oscar's chess team, however, tells school authorities that Oscar said to him "I wanted to hurt my school because they are morons who can't build a website well." Oscar has beaten this other student in the past four chess competitions.

Analysis:

(1) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a protected computer? Yes, there was an impairment in availability when the school's website crashed.

(2) Was there express or implied consent? No.

(3) Was there knowledge or intent to harm? Depending on which of Oscar's statements is credible, either knowledge, or intent to harm, or both were present.

There is possible criminal culpability for Oscar. However, in light of Oscar's age and assuming this is a first offense, the prosecutor should consider a misdemeanor charge or an alternative sanction.

(b) Oscar's cat, Script Kitty, walks across his keyboard, deleting text in a URL that functionally results in an enumeration attack.

Analysis:

(1) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a protected computer? No. The website was coded to render this URL publicly viewable.

(2) Was there express or implied consent? Yes, implied consent existed because the enumerated website page was publicly viewable.

(3) Was there knowledge or intent to harm? No. Cats cannot form intent for criminal law purposes, and Oscar viewed a site set *a priori* to be publicly viewable.

No culpability is possible for Oscar (or Script Kitty[411]) under the CIAA.

6. Hypothetical #6: The DDoS Participants

Two individuals, Dan and Chuck, each participate in a distributed denial-of-service (DDoS) attack. Dan is unaware of his participation in the DDoS, as his computer, without his knowledge, is infected with malware and becomes part of a large botnet on which strangers rent time. Chuck, on the other hand, agrees to participate in a political protest organized by the hacktivist group Anonymous aimed at Facebook, with a goal of rendering Facebook "mute" for a period of time. He joins thousands of others in downloading Ion Cannon and committing a DDoS attack. Facebook is knocked offline for several hours.

Analysis:

(1) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a system or machine? Yes, an impairment to availability occurred when Facebook was knocked offline.

(2) Was there express or implied consent? No.

(3) Was there knowledge or intent to harm? Dan had no knowledge or intent to harm. Chuck had both knowledge and intent to harm.

Chuck faces criminal culpability under the CIAA, but there is no possible culpability for Dan.

7. Hypothetical #7: The Fibbing Consumer

Frank, a successful but recently divorced middle-aged man, lies about his height and weight on a dating website. To facilitate these "fibs," Frank posts pictures of himself taken during his more athletic college days and photoshops a semi-recent version of his current head on them, adding some "bonus" hair and a hat. The website's terms of service, to which Frank agreed by clicking through them, requires all participants not to lie in their profiles. The website charges a fee to its participants. After Frank goes out on a few first dates with people he meets on the website, several of them contact the website and, among

411. *But see* Matt Simon, *Fantastically Wrong: Europe's Insane History of Putting Animals on Trial and Executing Them*, WIRED (Sept. 4, 2014), https://www.wired.com/2014/09/fantastically-wrong-europes-insane-history-putting-animals-trial-executing [https://perma.cc/9JBT-DHMF]; James Williams, *Beastly Justice*, SLATE (Feb. 21, 2013), https://slate.com/human-interest/2013/02/medieval-animal-trials-why-theyre-not-quite-as-crazy-as-they-sound.html [https://perma.cc/JT7W-K33T].

other things, complain about the "fibs" and "hatphishing" in his profile.

Analysis:

(1) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a protected computer? No. This is a contract breach by Frank. This is not a computer intrusion scenario and Frank is not culpable under the CIAA. The website, however, is entitled to pursue contract remedies against Frank, as set forth in the agreement and as allowed by the applicable contract doctrines of the jurisdiction.[412]

No criminal culpability is possible under the CIAA.

8. Hypothetical #8: The Artful CAPTCHA Dodger

Carol, the CEO of a startup, exploits a vulnerability to circumvent a competitor's CAPTCHA in order to aggregate information more quickly for purposes of commercial gain and repackaging. In the course of her automated collection efforts, the competitor's system goes down.

Analysis:

(1) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a protected computer? Yes, there has been a confidentiality and an availability impairment. The confidentiality of the system was impaired when Carol gained access to the information without completing the CAPTCHA. She did not engage with the system as set *a priori* and gained access to information that was restricted by the CAPTCHA. An impairment in availability occurred when the competitor's website went down.

(2) Was there express or implied consent? No.

(3) Was there knowledge or intent to harm? Both knowledge and intent to harm existed with respect to the circumvention of the CAPTCHA but only knowledge existed with respect to the website crash.

Criminal culpability is possible for Carol under the CIAA.

9. Hypothetical #9: The Grabby User

(a) Trudy, a college student, uses a script to "game" her school's class registration system and gain access to a seat in all of the classes

412. Frank and his hat are likely to continue to experience challenges in finding love.

she wants. Her classmates are mad because she gained preferential access to registration.

(b) Niaj, an avid camper, writes a script to obtain preferential admission to various campsite locations on a national park website. The first time he uses the script, it works and Niaj receives a prime spot to set up his tent. The second time he executes the script, the website crashes because of others engaged in the same conduct at the same time as Niaj.

Analysis:[413]

(1) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a protected computer? Trudy did not cause an availability change because the system continued to function for other users as designed *a priori*. Conversely, Niaj and others impaired the availability of the campsite reservation website. Trudy is not culpable because no impairment to the CIA of a protected computer occurred.

(2) Was there express or implied consent for Niaj's conduct? Implied consent potentially existed because of the lack of a CAPTCHA or other technological barrier to prevent the use of a script. However, if a robot.txt[414] notice is present, it may be a relevant fact in determining whether or not implied consent existed.

(3) Was there knowledge or intent to harm? Niaj had knowledge but no intent to harm.

Criminal culpability may be appropriate in any case where a method of gaining preferential access results in an impairment to the availability of the website. The owner of the protected computer would not consent to a use of the public website that would render it unavailable to other users. This is a gray area where the conduct on an individual basis may not pose a problem but, in the aggregate, the conduct results in an impairment to the availability of a protected computer.

10. Hypothetical #10: The Nosy Aggregator

(a) Heidi applied to a college that notifies applicants of admission decisions by directing them to a unique URL. Eve wants to know who has been admitted to the college and writes a script to generate new

413. A ticket bot statute may impact this kind of aggregation conduct — the BOTS Act of 2016, Pub. L. No. 114-274, 130 Stat. 1401 (2016) — which may impact some types of "ticket" data aggregation. Although this data does not qualify as a "ticket," other similar situations might trigger the statute.

414 . *Robots.txt*, MOZ, https://moz.com/learn/seo/robotstxt [https://perma.cc/Q2QD-QTTW].

publicly-viewable URLs, which simply contain different ending numbers, and because of this enumeration, she is able to see the admission decisions of the 5,000 applicants. She provides the data to her school newspaper for an article about college admissions practices.

(b) Heidi's friend Victor has applied to a college that requires applicants to set up a password-protected account. Applicants login to their accounts on a specified date to learn the admission decision. Heidi guesses Victor's password and logs in to his account to see the admission decision.

(c) Heidi is having coffee with Victor while Victor logs into to his account to find out whether he has been accepted to the college. While Victor is in the restroom, Heidi uses the machine's browser history to reopen the closed tab on his computer that contains his decision letter.

Analysis:

10(a) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a protected computer? No. No criminal culpability is appropriate under the CIAA.

10(b) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a protected computer? No. However, Heidi's conduct is a violation of CIAA's criminal impersonation with a credential provision because she tricked the system into exposing the information protected by Victor's credential without his consent. In this case, the credential is co-owned by Victor, as it was issued for his benefit as a consequence of his application for admission. Without his consent, Heidi pretended to be Victor when she logged into his account.

10(c) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a protected computer? With respect to Victor's protected computer, an impairment in confidentiality may have occurred — the tab was closed by Victor and then reopened by Heidi. However, prosecutorial discretion and restraint should result in a warning or a misdemeanor, at best. Heidi may also have violated the CIAA's criminal impersonation with a credential provision insofar as she tricked the college's server into believing she was Victor without Victor's consent.

11. Hypothetical #11: The (Un)Advanced Persistent User

Helen is unaware that her home network router needed to be rebooted. Her iPad prompts her to choose the wrong SSID — the SSID of her neighbor's network. Helen then ferociously types in all of her

known passwords into her neighbor's network login interface for hours to no avail.

Analysis:

(1) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a protected computer? No.

(2) Even if there was an impairment to the CIA of a protected computer, there would be no knowledge or intent on Helen's part.

No criminal culpability is possible under the CIAA.

12. Hypothetical #12: The Competitor Aggregator

(a) SukdUp is a startup that aggregates publicly-viewable information from another company, HooktIn, by screenscraping the data at the rate a human user would interact with the publicly-viewable website. HooktIn objects to SukdUp's aggregation, and sends them a cease and desist letter. SukdUp continues to scrape data.

(b) SukdUp is a startup that aggregates publicly-viewable information from another company, HooktIn, by screenscraping the data at a rate that slows the performance of the website because of SukdUp's bots. HooktIn objects to SukdUp's aggregation, and sends them a cease and desist letter informing SukdUp that their bots are impairing the availability of the system. SukdUp continues to scrape data using the availability-impairing bots.

(c) SukdUp is a startup that aggregates publicly-viewable information from another company, HooktIn, by screenscraping the data. HooktIn objects to SukdUp's aggregation, and sends them a cease and desist letter and employs aggressive technological measures to block SukdUp's crawlers from aggregating information from HooktIn. SukdUp exploits a vulnerability in HooktIn's technological blocks and continues to scrape data.

Analysis:

12(a) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a protected computer? No. SukdUp may continue to collect the publicly available data at the rate a human would interact with the website. No criminal culpability exists under the CIAA.

12(b) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a protected computer? Yes, there is an availability impairment. Was there consent by the computer's owner? Implied consent initially existed because the website was publicly viewable. However, the cease and desist letter advised SukdUp that its scraping method was

impairing the availability of the system and that HooktIn did not consent to SukdUp's continued use of the availability-impairing bots. Was there knowledge or intent to cause harm? Initially, no. However, after the cease and desist letter was sent, SukdUp has knowledge that the current aggregation methodology used for its screenscraping activity is causing an impairment to the availability of HooktIn's system. Notwithstanding the public nature of the information at issue, HoooktIn does not consent to activity by SukdUp that impairs the availability of its system. Both knowledge and intent to cause harm exists. Criminal culpability is possible under the CIAA.

12(c) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a protected computer? Yes, there are both confidentiality and integrity impairments. A confidentiality impairment occurred when SukdUp exploited a vulnerability to view content that technically blocked its scrapers. Forensic analysis could also reveal an integrity impairment depending on methodology used to exploit the vulnerability and the subsequent results. Was there consent by HooktIn? Implied consent existed initially because the information was publicly available on the website. After the cease and desist letter was sent and technical barriers were put in place, consent no longer existed. Was there knowledge or intent to cause harm? Yes. Criminal culpability is possible under the CIAA.

13. Hypothetical #13: The Rogue Corporate Insider

(a) Walter, a systems administrator, accidentally deletes proprietary data before leaving his current employer for a job with a new company.

(b) Walter, a systems administrator, purposefully deletes proprietary data before leaving his current employer for a job with a new company.

(c) Walter, a systems administrator, plants logic bombs to delete large amounts of data (but not backups) one month after he leaves his job.

(d) Walter, a systems administrator, posts his former corporate login credentials and the note "this company discriminates against African American employees" on 4chan after he leaves the company for another job. For two weeks, no one uses the credentials. Then, on the third week following the posting, a third party uses the credentials to

log in to Walter's account and steals trade secrets and protected information, which he sells to the company's competitors.

(e) Walter, a current employee at the company, logs in to his account and downloads information from the corporate network to use for a business he is building on the side.

(f) Walter, a former employee, asks Eve, a current employee, if he can borrow her credentials to log in to the Company's network and view information.

Analysis:

13(a) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a protected computer? Yes, an availability impairment and potentially an integrity impairment occurred. Was there consent by the computer's owner? Probably so, if performed in accordance with Walter's duties as a systems administrator. Was there knowledge or intent to cause harm? No. No criminal culpability exists.

13(b) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a protected computer? Yes, an availability impairment exists. Was there consent by the computer's owner? No. Purposeful deletion of the proprietary data (without express instructions to do so and outside the normal data destruction practices of the company) evinces a lack of consent on the part of the owner of the protected computer. Was there knowledge or intent to cause harm? Yes, both knowledge and intent to cause harm exist, again assuming that the deletion was outside the normal data destruction practices of the company. Criminal culpability is possible.

13(c) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a protected computer? Yes, an availability impairment exists. An integrity impairment may also exist. Was there consent by the computer's owner? No. Walter's credentials had been terminated and it was unlikely that such destructive activity was ever in the scope of his work and consented to by the owner of the protected computer. Was there knowledge or intent to cause harm? Yes, both knowledge and intent to cause harm exist. Criminal culpability is possible under the CIAA.

13(d) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a protected computer? No, but criminal culpability is possible under the CIAA for Walter for aiding and abetting criminal impersonation with a credential. The third party is potentially criminally culpable for

criminal impersonation with a credential under the CIAA. The third party could also be prosecuted for trade secret theft potentially. Walter could also be prosecuted for aiding and abetting that theft.

13(e) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a protected computer? No. No criminal culpability exists under the CIAA. But, Walter could potentially be prosecuted for trade secret theft (if the information qualifies for trade secret protection) and potentially sued for violations of any nondisclosure agreements he signed with the company.

13(f) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a protected computer? No, but criminal culpability is possible for Walter under the CIAA for criminal impersonation with a credential.

14. Hypothetical #14: The Password Sharer

(a) Olivia, who is unable to get a stable WiFi connection, calls her spouse Ted and asks him to check her personal Gmail account for a message she is waiting for from her mother. Olivia has previously given Ted the password to her Gmail account.

(b) Olivia then gives Ted the password to her work email account and asks Ted to see if she has gotten any emails from her boss.

(c) Olivia shares her Netflix password with her friend Vanna, and Vanna watches several movies.

(d) Olivia, who is a government employee, gives the password to her government email account to Vanna and asks Vanna to check her emails for her.

Analysis:

14(a) No criminal impersonation exists. This is an assignment of contract rights by Olivia. If the assignment violates a EULA, it is a possible contract breach, but no criminal culpability exists under the CIAA.

14(b) This is criminal impersonation with a credential by Ted because Olivia does not have the authority to license her credential. The credential was issued by Olivia's employer for Olivia's use alone to benefit the employer in the course of her work. There is no apparent authority for Olivia to share her password and Ted knows or should have known that Olivia does not possess this authority. Olivia aids and abets a criminal impersonation with a credential, or conspires to

criminally impersonate with a credential. Criminal culpability for both Olivia and Ted is possible under the CIAA, but if it is a first offense, prosecutorial restraint is advised.

14(c) No criminal impersonation occurred. The credential was issued primarily for Olivia's benefit. Under contract law, this activity is merely an assignment of contract rights by Olivia. If the assignment violates a EULA, it is a possible contract breach, but no criminal culpability under the CIAA exists.

14(d) Criminal impersonation with a credential by Vanna occurred, as did conspiracy or aiding and abetting a criminal impersonation by Olivia. The government is the owner of Olivia's credential; it was issued to Olivia primarily to benefit the government in the course of Olivia's employment. Criminal culpability under the CIAA for both Olivia and Vanna is possible.

15. Hypothetical #15: The Rogue Government Insider

(a) Grace, an FBI agent who has signed an agreement imposing a duty of confidentiality as part of her employment, queries a confidential law enforcement database to find information about her sister's new boyfriend because she is concerned the boyfriend may have a violent criminal background.

(b) Pat, a DoD contractor who has signed an agreement imposing a duty of confidentiality as part of his employment, queries a confidential DoD database to determine what, if any, information it may contain about a competitor to Pat's company. He then shares that information with others in his company who do not have access to the DoD database.

(c) Wendy, a CIA employee who has signed an agreement imposing a duty of confidentiality as part of her employment, discloses classified information to a congressional staffer on the Senate Select Committee for Intelligence about questionable payments to a foreign guerrilla group that has committed terrorist acts in foreign countries.

Analysis:

15(a) Grace's actions constitute accessing a government computer for a non-governmental purpose and would violate the duty of confidentiality imposed as a condition of her employment. Criminal culpability is possible under the CIAA's abuse of government position of trust provision.

15(b) Pat's actions constitute accessing a government computer for a non-governmental purpose and obtaining and transmitting

that information for a non-governmental purpose. Pat's actions violate the duty of confidentiality imposed as a condition of his employment. Criminal culpability for abuse of government position of trust under the CIAA is possible.

15(c) Wendy's actions would not violate the CIAA so long as she complied with appropriate channels for reporting per statutory or agency guidelines and, accordingly, was eligible for federal whistleblower protections. But, if she did not comply with the rules and regulations associated with these protections, criminal culpability may exist under the CIAA.

16. Hypothetical #16: Bots for Tots, Silver Spears, and Research Recon

(a) Lucifer is a bot herder and broker who sells time on his botnet of compromised children's internet-connected toys.

(b) Lucifer is a bot herder who engages in a "silverphishing" campaign, sending out emails with malicious links to the AARP mailing list of senior citizens in an effort to compromise their machines and harness them as part of a botnet.

(c) Lucy, a security researcher, buys time on Lucifer's botnet of toys to help further knowledge for defending the Internet of Things and protecting children.

Analysis:

16(a) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a protected computer? Yes, depending on specific details of how the toys were compromised, an integrity or availability impairment in the harnessed machines occurred. Was there consent by the computer's owner? No. Was there knowledge or intent to cause harm? Yes, both knowledge and intent to cause a CIA impairment. Lucifer is potentially culpable and chargeable with many counts of computer intrusion under the CIAA.[415] Lucifer is also potentially culpable and chargeable under the CIAA for trafficking in epidemic malware when he sells access to the botnet to third parties.

16(b) Is there a forensically-demonstrable confidentiality, integrity, or availability impairment to a protected computer? Yes, depending on specific details of the phishing campaign, an integrity or availability impairment in the harnessed machines occurred. Was there consent by the computer's owner? No. Was there knowledge or intent to cause harm?

415. Lucifer may also be guilty of being a reprehensible person.

Yes, both knowledge and intent to cause a CIA violation. Lucifer is potentially culpable and chargeable with many counts of computer intrusion under the CIAA.[416]

16(c) Is Lucy intentionally acquiring access to a protected computer infected with epidemic malware intending to commit a CIA impairment? No, her intent is to conduct research. No criminal culpability is appropriate under the CIAA.

17. Hypothetical #17: The Silverphishing Botnet Harpoon

The AARP and the DOJ wish to collaborate to take down Lucifer's silverphishing botnet, which tricks senior citizens' machines into becoming part of Lucifer's botnet and attacking power grids in DDoS attacks.

Analysis:

The botnet is subject to possible takedown through the epidemic malware provision by the AARP in conjunction with the DOJ and other agencies provided they follow the guidelines of the epidemic malware provision of the CIAA.

IV. CONCLUSION

In the 1300s, the bubonic plague, also known as the Black Death, swept Europe.[417] Ultimately it claimed the lives of approximately 60% of Europe's population before tapering off.[418] Now believed to have been spread by fleas on rats and other animals,[419] this infection agent had not been identified accurately at the time, leading to increased infections. Using the only mitigation strategy available, quarantine, the population addressed the disease with limited success.[420]

Seven hundred years later, the plague is substantially controlled.[421] However, new infections such as Ebola threaten our population.[422] While Ebola has caused loss of life, the scale of loss was limited in comparison to the scale caused by the plague. The successful prevention of mass casualties from Ebola arose partly from advances in epidemiology and the existence of new types of population-level

416. Lucifer may also again be guilty of being a reprehensible person.

417. *History of the Plague*, CTRS. FOR DISEASE CONTROL AND PREVENTION, https://www.cdc.gov/plague/history/index.html [https://perma.cc/CC6T-9MG4].

418. *Id.*

419. *Frequently Asked Questions*, CTRS. FOR DISEASE CONTROL AND PREVENTION, https://www.cdc.gov/plague/faq/index.html [https://perma.cc/TPF5-QSCA].

420. *Id.*

421. CTRS. FOR DISEASE CONTROL AND PREVENTION, *supra* note 417.

422. *Years of Ebola Virus Disease Outbreaks*, CTRS. FOR DISEASE CONTROL AND PREVENTION, https://www.cdc.gov/vhf/ebola/history/chronology.html [https://perma.cc/CE6Y-TA84].

mitigation strategies.[423] We are entering an era of "plagues" in security. Whether it becomes an era of Black Death or a period of mitigated "outbreaks" depends on our response. The extent of social disruption due to security threats will be determined in large part by our legal and technical preparation and tools.

This article offered a new paradigm for computer intrusion law inspired by the lessons of epidemiology and insights from the field of computer security. Rejecting the traditional paradigm of trespass reflected in most legal scholarship on computer intrusion, we instead have proposed a novel reframing — the CIAA. The CIAA replaces the confused, often unworkable concepts of "access without authorization" and "exceeds authorized access" with a new three-part analysis: (1) forensically-demonstrable technical harm; (2) intent of the defendant; and (3) consent of the owner of the system or machine (protected computer).

Through the addition of an affirmative defense to protect security research, the CIAA better balances the interests of innovation policy and national security than the current CFAA approach. With the addition of a new claim for impersonation with a credential, a new claim for abuse of government position of trust, and the elimination of all civil claims under the new act, our paradigm successfully eliminates the current circuit splits visible in CFAA case law. Finally, with the creation of an epidemic malware provision, the CIAA creates a framework for structured public-private takedown operations that address current botnet activity and anticipates threats from other kinds of self-propagating malware that may materialize in the future.

423. *Id.*