Journal of Criminal Law and Criminology

Volume 103 | Issue 3 Article 7

Summer 2013

Criminalizing Hacking, not Dating: Reconstructing the CFAA Intent Requirement

David Thaw

Follow this and additional works at: http://scholarlycommons.law.northwestern.edu/jclc

Part of the Criminal Law Commons

Recommended Citation

David Thaw, *Criminalizing Hacking, not Dating: Reconstructing the CFAA Intent Requirement*, 103 J. Crim. L. & Criminology 907 (2013).
http://scholarlycommons.law.northwestern.edu/jclc/vol103/iss3/7

This Symposium is brought to you for free and open access by Northwestern University School of Law Scholarly Commons. It has been accepted for inclusion in Journal of Criminal Law and Criminology by an authorized administrator of Northwestern University School of Law Scholarly Commons.

0091-4169/13/10303-0907
THE JOURNAL OF CRIMINAL LAW & CRIMINOLOGY Vol. 103, No. 3
Copyright © 2013 by David Thaw
Printed in U.S.A.

CRIMINALIZING HACKING, NOT DATING: RECONSTRUCTING THE CFAA INTENT REQUIREMENT

DAVID THAW*

Cybercrime is a growing problem in the United States and worldwide. Many questions remain unanswered as to the proper role and scope of criminal law in addressing socially undesirable actions affecting and conducted through the use of computers and modern information technologies. This Article tackles perhaps the most exigent question in U.S. cybercrime law—the scope of activities that should be subject to criminal sanction under the Computer Fraud and Abuse Act (CFAA), the federal antihacking statute. At the core of current CFAA debate is the question of whether private contracts, such as website terms of use or organizational acceptable use policies should be able to define the limits of authorization and access for purposes of criminal sanctions under the CFAA. Many scholars and activists argue that such contracts should not, because they may result in ridiculous consequences such as the criminalization of misrepresenting one's desirability on an online dating website. Critics of

* Visiting Assistant Professor of Law, University of Connecticut School of Law and Affiliated Fellow, Yale Law School Information Society Project.

This work benefited from the thoughtful commentary of Jack Balkin, Derek Bambauer, Rebecca Bolin, Bryan Choi, Mathilde Cohen, Anjali Dalal, William Eyre, James Grimmelmann, Kaaryn Gustafson, Dalié Jiménez, Camilla Hrdy, Margot Kaminski, Orin Kerr, James Kwak, Andrea Matwyshyn, George Mocsary, Christina Mulligan, Paul Ohm, Lisa Ouellette, Mark Paulding, Randy Sabett, Julia Simon-Kerr, and the participants in the *Journal of Criminal Law and Criminology*'s February 2013 Symposium on Cybercrime. A draft of this work will be presented at the 2013 Privacy Law Scholars Conference, and the author extends anticipatory thanks to the participants for what is expected to be thoughtful and insightful commentary on this work and for inspiring future related work. The research staff of the University of Connecticut Law Library provided invaluable research assistance with this work, specifically including Craigin Howland. Finally, the author would like to extend his deepest gratitude to the editors and staff of the *Journal of Criminal Law and Criminology*, including Jonathan Jacobson, Lily Katz, Megan Lawson, Jessica Notebaert, Robert (Max) Tanner, Daniel Truesdell, and Hannah Wendling, for their tremendous assistance and patience with the expansion of a planned short Essay into a full Article responsive to current events shortly before the Symposium.

such arguments rebut that failing to allow contract-based restrictions opens the door for hackers to engage in many types of disfavored activity not otherwise subject to criminal sanction. This Article examines the tension between these two positions, both from the standpoint of current U.S. jurisprudence and scholarship, and from the standpoint of the respective purposes of criminal and tort law in deterring and punishing socially undesirable behavior. The Article concludes by proposing a legislative revision to the CFAA's mens rea element that substantially mitigates the risk of overbroad criminalization while leaving intact the ability of the law to deter and punish the most serious acts affecting and utilizing computers.

TABLE OF CONTENTS

INTRODUCTION 909
I. HACKING: A (BRIEF) CONTEXTUAL HISTORY OF THE CFAA 912
A. Legislative History 913
B. What Is Hacking and Who Are Hackers? 915
1. Security Vulnerabilities and the "Cybercrime Ecosystem" 917
C. Criminal and Civil Prosecutorial History 920
1. *United States v. Drew* (C.D. Cal. 2009) 921
2. *United States v. Nosal* (9th Cir. 2012) (en banc) 923
3. *United States v. John* (5th Cir. 2010) 925
II. CRIMINALIZATION BY CONTRACT 926
A. The Concept of "Authorized Access" 927
B. The "Harms" of Computer Crime—Against What *Should* We Protect? 928
1. Circumvention of Code-Based Restrictions 929
2. Existing Criminal Activities Made Easier or Having Increased Impact on Victims 930
3. Existing Offensive (but Not Criminal) Activities Rising to the Criminal Level in the Electronic or Virtual Context 932
4. Computer-Specific Activities that Are Otherwise Not Criminalized 932
C. Effective Prevention: Criminalization vs. Private Options 934
1. Private Law (Tort and Contract) Deterrence of Cybercrime 936
2. Criminal Law Deterrence 939
III. CRIMINALIZING (ONLY) HACKING: MENS REA AS A SOLUTION 942
A. Kerr's Code-Based Restriction Test 943
B. Representative Zoe Lofgren's Proposed Reform 944
C. Mens Rea Reform: A Responsive Return to Congressional Intent 945
IV. CONCLUSION 947

INTRODUCTION

This Article addresses a growing problem with existing United States federal law addressing cybercrime. The Computer Fraud and Abuse Act of 1986 (CFAA), which in part revised earlier (limited) legislation on the subject, is the primary federal antihacking statute providing both criminal penalties and (limited) rights of private action for certain unauthorized activities using computers and similar information systems. Congress originally intended to address only a narrow range of crimes[1] but, as others have observed,[2] the statute's scope expanded dramatically over the past two decades.

The result of this expansion threatens to criminalize wide varieties of activities, common to the ordinary computer and Internet user, that are apparently innocuous in the context of "hacking," but technically constitute unauthorized activities or activities exceeding a user's authorized access. It is now common, if not near-universal, practice for popular Internet websites to have terms-of-service agreements[3] and for employers and other operators of computer systems to have acceptable-use policies.[4] Such policies frequently contain provisions governing what activities are and are not acceptable on the website or computer system. Over the course of the past several years, prosecutors and private parties increasingly have asserted these terms to define the boundaries of authorized access on computer systems; thus, violations of those terms constitute unauthorized access in violation of the CFAA.

While existing scholarship on the subject is still limited, the balance seems to favor an approach under which private agreements cannot define the boundaries of criminal activity.[5] The federal courts of appeal have split

---

[1] *See infra* Part I.A for further discussion of congressional intent.

[2] *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1561 (2010).

[3] Terms-of-service agreements generally are contracts of adhesion that lay out the ways in which a website operator allows users to access, interact with, and otherwise make use of the website and its associated systems. Such agreements almost always include restrictions on behaviors, if any, that the website operator considers inappropriate.

[4] Employers and other network operators (e.g., colleges and universities, Internet service providers, public libraries) nearly universally require users to agree, whether at the time of access (for transactional users like patrons of a public library) or at the time of setup (for relationship users like resident students at universities), to various conditions for use of the network. These conditions are specified in what is most commonly known as an acceptable-use policy. It functions similarly to the terms-of-service agreements referenced *supra* in note 3, but generally focuses more on the ways in which individuals use the network (i.e., what data is sent to/from computers and other devices they connect to the network) rather than on the ways in which users interact with a specific program or application (e.g., a website).

[5] *See* Kerr, *supra* note 2; *see also* Andrea Matwyshyn, *The Law of the Zebra*, 28 BERKELEY TECH. L.J. (forthcoming 2013) (manuscript at 5–8) (on file with the Journal of

on the issue, with the Fifth[6] and Seventh[7] Circuits permitting such agreements to define authorized access for criminal purposes and the Fourth[8] and Ninth Circuits[9] rejecting such an approach. To date, the U.S. Supreme Court has not addressed the issue or granted certiorari in any case decided by the courts of appeal.

This Article responds to the debate in existing scholarship and the problems presented by the circuit split in an interconnected world.[10] It specifically takes up Professor Orin Kerr's invitation[11] seeking debate on the subject of access- or authorization-based tests in electronic crimes and challenges the solution proposed by Professor Kerr and the courts. The Article also responds to recent events[12] and resultant attention in Congress to possible reform of the CFAA. It identifies the shortcomings and risks in these current proposals, and suggests an alternate method of addressing overbreadth and vagueness problems in the existing statute through legislative reform of the mens rea element of the statute.

I propose legislative reconstruction of the existing mens rea element for at least § 1030(a)(2) of the CFAA[13] and perhaps all portions of 18 U.S.C. § 1030, where private agreements (e.g., terms of service) may define the boundaries of authorized access to computing and information systems. Specifically, I suggest a two-part intent requirement: (1) that the actor intentionally engage in an action not only constituting unauthorized access,[14] but also that the *intent be that the action result in unauthorized*

Criminal Law and Criminology).

[6] United States v. John, 597 F.3d 263, 272 (5th Cir. 2010).

[7] Int'l Airport Ctrs. v. Citrin, 440 F.3d 418, 421 (7th Cir. 2006).

[8] WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 207 (4th Cir. 2012).

[9] United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012) (en banc).

[10] The electronically interconnected nature of the Information Age allows prosecutors and parties the ability to forum shop for a favorable circuit in a way perhaps not previously conceived of. Not only are potential actors held accountable in those areas where they know they establish minimum contacts (e.g., where they mail an item in a mail fraud scheme), but also where they may not know (or the average person may not even be able to know) they established contacts (e.g., the location of various Internet services to which they directly and secondarily connect).

[11] Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1643–44 (2003).

[12] *See, e.g.*, Matt Pearce, *Swartz's Dad Lashes Out at Prosecutors*, L.A. TIMES, Jan. 18, 2013, at AA2.

[13] 18 U.S.C. § 1030(a)(2) (2006). The other sections may require intent reform as well. However, the additional damages elements of those provisions often serve as sufficient protection against overbroad prosecution. Nonetheless, there are advantages to a uniform mens rea element for all portions of the statute where private agreements may govern the scope of authorized access.

[14] This is the effect of the current language, which some courts have described as nearly

access, an express element requiring proof that the actor reasonably should have known that the action in question was unauthorized under a terms-of-service or similar agreement;[15] and (2) that this action be in furtherance either of one of a list of specifically prohibited computer-specific crimes[16] or alternatively in furtherance of an act otherwise unlawful under existing state or federal law.

The goal of this proposed reform is to better align the effect and reach of the statute with congressional intent regarding acts deserving of criminal punishment, while at the same time maintaining its ability to serve as an effective deterrent to (and mechanism of punishment for) acts uniquely involving computers and modern information technologies that I argue should be criminalized. In Part II.B of this Article, I present a typology describing the types of acts with which the federal criminal law should be concerned. Based on that typology, I evaluate the degree to which legal alternatives may serve as substitutes in deterring and/or punishing perpetrators of such actions. I conclude that the most obvious alternative, private tort law, is vastly insufficient either as a deterrent or a mechanism of punishment, suggesting the importance of engaging the criminal law.

Reform of the mens rea element also suggests a larger question in the context of electronic crimes—how to conceive of "intent" in virtual worlds

---

tautological and providing trivial differentiation. *See, e.g.*, *Nosal*, 676 F.3d at 856–58.

[15] In other words, the provision prohibiting the action at issue must not have been buried in difficult-to-understand language in the middle of a 10,000-word agreement. There exists substantial literature and ongoing work on effective user-notice mechanisms upon which Congress may draw in crafting such a notice requirement. *See, e.g.*, Aleecia M. McDonald et al., *A Comparative Study of Online Privacy Policies and Formats*, *in* PRIVACY ENHANCING TECHNOLOGIES 37, 37–55 (Ian Goldberg & Mikhail J. Atallah eds., 2009); CTR. FOR INFO. POLICY LEADERSHIP, TEN STEPS TO DEVELOP A MULTILAYERED PRIVACY NOTICE (2007), *available at* http://www.informationpolicycentre.com/files/Uploads/Documents/Centre/Ten_Steps_whitepaper.pdf; Corey A. Ciocchetti, *The Future of Privacy Policies: A Privacy Nutrition Label Filled with Fair Information Practices*, 26 J. MARSHALL J. COMPUTER & INFO. L. 1 (2009).

[16] For example, a distributed denial-of-service (DDoS) attack in itself is unlikely to be criminal as pertains to the victim website but for its effect on the target machine, an effect that is difficult to describe as criminal within the ambit of physical-world-oriented criminal statutes or other electronic crimes statutes. *See* United States v. Raisley, 466 F. App'x 125, 126–27 (3d Cir. 2012) ("Raisley . . . used [an] infected network of computers to launch 'Distributed Denial of Service' [] attacks against websites . . . . A DDOS attack uses multiple computers simultaneously to request information from a website. If done on a large enough scale, the requests overwhelm the website, take the victim server off line, and render the site inaccessible."). The district court convicted Raisley for these activities under the Computer Fraud and Abuse Act. Note, however, that it is possible that the use of individual machines taking part in the attack on the target website *may* constitute individual acts violating the CFAA or other statutes, but such use (assuming it was, in fact, unauthorized) is far more difficult to track than is the effect on the target website itself.

where the physical-world actions taken to bring about virtual-world results may have different (and sometimes disjunctive) intent associated with them. The Article opens this discussion, in part, by analogizing my proposed CFAA mens rea reform to distinctions in the intent requirements of physical-world crimes. It is a first step in this regard, and one I hope opens an ongoing discussion regarding the question of intent with respect to actions that have both physical-world and virtual-world consequences.

This Article proceeds in three Parts. Part I provides a contextual history of the CFAA relevant to the question of prosecution for agreement-based authorization violations of the CFAA and the role of the mens rea element in protecting against overbroad prosecutions. It provides background on congressional intent, examines the types of bad actors and the types of harms against which Congress sought to protect, and proposes a stratification of the cybercrime ecosystem as a way to categorize the types of criminal activity at issue. It then proceeds to provide a background on select cases highlighting the challenges inherent in the CFAA's existing authorized-access approach and intent requirement. Part II explores the concept of defining the boundaries of criminal action as a function of private agreements, including examining physical-world analogues such as criminal trespass. Building on the discussion of what harms may arise in a computer-centric world, it proposes a typology of computer-based or computer-enhanced crimes against which computer-crime legislation *should* protect. It then proceeds to examine why such protection is necessary for adequate deterrence, providing a foundation for the argument that existing CFAA reform proposals are inadequate. Part III examines other existing proposals, presents examples of how they cannot address the concerns raised by various types of harms that arise in the computer-crime context, and alternatively proposes legislative reform of the mens rea requirement of the CFAA as a solution that both protects against overbroad prosecution and maintains the ability of private (electronic) property owners to post virtual "no trespassing" signs and have those signs enjoy the necessary protection of the criminal law.

I. HACKING: A (BRIEF) CONTEXTUAL HISTORY OF THE CFAA

In the (admittedly limited) scholarly discussion of the CFAA to date, much attention is given to the expansion (both by congressional act and judicial interpretation), potentially overbroad use, and ill-defined aspects of the criminal acts defined by the statute and its civil analogues. Scholarship and judicial notice have also spent substantial time discussing the logical, implied, and literal meanings of the statute, but comparatively less discussing the legislature's original intent as expressed in the congressional debates surrounding the CFAA's adoption.

While there remains healthy debate as to the extent to which congressional intent should be balanced against literal interpretation—and this Article does not seek to address such debate—legislative intent, when evidence of it exists, is at least worthy of consideration. This is particularly true in cases where rapidly changing technological conditions make difficult the construction of statutes to address undesired, but not yet technically identifiable, behavior. This Part examines the congressional record surrounding the adoption of the 1986 amendments to 18 U.S.C. § 1030, which introduced the name "Computer Fraud and Abuse Act," with an eye toward how the bill's authors attempted to use the mens rea element of the statute to protect against overbroad use of the statute. It then proceeds to examine the types of criminals and criminal activity the statute's authors *did* seek to criminalize, the reasons behind it. It also discusses how subsequent criminal and civil prosecution under the CFAA has diverged from that intent in a manner inconsistent with legislative purpose.

A. LEGISLATIVE HISTORY

The CFAA originally was enacted as a response to the growing use of computers, particularly by the federal government, and the growing threat of computer crimes.[17] In the nearly thirty years since its original enactment, the CFAA has been amended multiple times and interpreted in an increasingly expansive way by the courts. Professor Kerr has written an excellent overview and discussion of this history,[18] and rather than recount this work, the following discussion focuses specifically on those elements of Congress's original intent that suggest how current jurisprudence departs from this congressional intent and how the solutions proposed in this Article may restore that original intent.[19]

According to one of its leading sponsors, Representative William J. Hughes, the CFAA's primary focus was "technologically sophisticated criminal[s] who break[] into computerized data files."[20] Rep. Hughes analogized this type of activity, committed by colloquially described

---

[17] 132 CONG. REC. 9159–61 (1986) (statement of Rep. William J. Hughes).

[18] Kerr, *supra* note 2, at 1564–65.

[19] As discussed in the congressional debates referenced *supra* note 17, the Computer Fraud and Abuse Act of 1986 actually was an update to 18 U.S.C. § 1030, originally enacted as part of the Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, § 2102, 98 Stat. 1976, 2190 (codified as amended in scattered sections of 18 and 28 U.S.C.), which already addressed some existing criminal restrictions on the unauthorized use of computers. *See also* Kerr, *supra* note 2, at 1563–64.

[20] 132 CONG. REC. 9160.

"hackers," to physical-world trespass.[21] In his statement, and indeed throughout the congressional debates of the CFAA at the time, no focus was given to criminalization of breaches of agreements between private parties beyond those possibly implicit in the concept of trespass. Quite to the contrary, in fact, the only notable mention of criminalization of other activities was Rep. Hughes's statement describing the then-proposed legislation as "expand[ing] in an appropriate *but limited* manner the types of criminal misconduct involving computers that [would] be subject to Federal jurisdiction."[22]

This discussion goes on further to illuminate why Congress felt that these new elements of computer-based crime should be limited in scope. Rep. Hughes's statement discusses the fact that the CFAA amended previous law to *raise* the mens rea requirement from "knowingly" to "intentionally"[23] out of specific concern for overbroad prosecution, including the need to "preclude liability on the part of those who inadvertently 'stumble into' someone else's computer file."[24] As described in Hughes's statement to the House, "It is not difficult to envision a situation in which an authorized computer user will mistakenly enter [in violation of the statute] someone else's computer file . . . [b]ecause the user had 'knowingly' signed onto the computer in the first place . . . ."[25]

This discussion highlights well the concerns raised by Professor Kerr[26] and other scholars[27] about the potential abuse of a federal law criminalizing "unauthorized access" to electronic information resources where the threshold constituting lack of authorization is poorly defined. Providing a comprehensive and enduring test in the face of rapidly changing technology is an impossible task. Whether or not Congress realized this challenge at the time, it nonetheless attempted to employ a proper solution—reliance on a heightened mens rea element to protect against overbroad prosecution. Regrettably, as discussed below, through both civil and criminal prosecution and resulting judicial interpretations, this heightened requirement has been whittled away.

---

[21] *Id.*

[22] *Id.* (emphasis added).

[23] H.R. REP. NO. 99-612, at 1 (1986).

[24] 132 CONG. REC. 9160.

[25] *Id.*

[26] *See* Kerr, *supra* note 2, at 1562.

[27] *See* Matwyshyn, *supra* note 5; *see also* Letter from Laura W. Murphy et al., to Chairmen and Ranking Members of the House Comm. on the Judiciary and the House Subcomm. on Crime, Terrorism, and Homeland Sec. (Apr. 2, 2013), *available at* http://cyberlaw.stanford.edu/files/blogs/LetterOpposingCFAADraft_final.pdf.

B. WHAT IS HACKING AND WHO ARE HACKERS?

The thesis of this Article—and its resultant policy conclusion—rests heavily on an understanding of exactly what are the harms against which computer-crime legislation seeks to protect.[28] The legislative history of the congressional record discussed above focuses on "a new breed of criminal: the technologically sophisticated criminal who breaks into computerized data files."[29] It demonstrated a particular concern with this growing class of hackers transforming their work into profitable white collar crime,[30] a premonition that certainly has come to pass.[31] This section describes a crime "ecosystem" that has emerged comprising modern variations on Rep. Hughes's hacker and some views on the motivations of various elements of that ecosystem. It also lays the groundwork for the core harms against which I claim the CFAA drafters sought to protect.

In the early 2000s, Finnish scholar Pekka Himanen authored a qualitative work describing three motivations for so-called "hackers."[32] In this work, Professor Himanen describes three motivations for hackers: a "work ethic," a "money ethic," and a "nethic."[33] The first motivation contrasts what Himanen calls the traditional Protestant work ethic of work as a means of sustenance with the "hacker work ethic" in which technologically inclined individuals are motivated by the "intrinsic interest" and "playful explorations" in which the accomplishment of the work is itself the reward sought.[34] The second motivation attempts to build on the first, casting hackers' view toward financial gain as disjunctive from traditional capitalism, focusing on a desire to achieve only that level of financial gain necessary to achieve individual independence after which one derives fulfillment from accomplishment, rather than a strictly increasing measure of fulfillment as a function of wealth accrual.[35] Finally, the third motivation asserts that hackers adopt certain social norms in their online interactions, norms that may override other motivations or serve as primary

---

[28] For the purposes of discussion at this point, I focus exclusively on the reasoning for criminalization separate from the fact that the CFAA also provides analogous civil actions for parts of its criminal prohibitions.

[29] 132 CONG. REC. 9160.

[30] *Id.*

[31] *See generally* Ross Anderson et al., Measuring the Cost of Cybercrime (June 26, 2012) (paper presented at the Eleventh Workshop on the Economics of Information Security), *available at* http://cseweb.ucsd.edu/~savage/papers/WEIS2012.pdf.

[32] PEKKA HIMANEN, THE HACKER ETHIC AND THE SPIRIT OF THE INFORMATION AGE (2001).

[33] *Id.* at ix–x.

[34] *Id.* at 3–4, 8.

[35] *Id.* at 53–57.

motivations.[36] Himanen gives freedom of expression and personal privacy as two leading examples of such norms.[37]

Himanen's work may be (perhaps rightly) criticized as relying too heavily on philosophical and political economic analysis and too weakly on empirical evidence, particularly in addressing a question ripe for qualitative analysis. Nonetheless, its analysis provides a useful link in drawing the connection between the hackers driving the motivations of the 98th and 99th Congresses and the modern cybercrime ecosystem proposed in this section. The Congresses that crafted and ultimately passed the CFAA were concerned with technologically sophisticated youth driven primarily by Himanen's first motivation who might later develop into financially motivated criminals who damage, modify, or copy information from computer systems as a means of achieving the financial independence depicted by Himanen's second motivation. Himanen's 2001 work generally does not contemplate this possibility. However, its focus on the hacker's desire for financial independence to engage in activities driven by the first motivation suggests individuals who highly value that independence. While resorting to computer-based fraud, theft, and other crimes might seem less likely in the Internet boom days during which Himanen's work was written, I suggest such activities follow quite logically as the demand for programming and other skills possessed by hackers diminished following the "dot-com bust" of 2001 and concurrent flooding of the market with (at least modestly) skilled programmers. And indeed, what limited data is available on the subject reveals that many with such skills have resorted to participation in computer-based criminal activity over the past several years.[38] Nor have the capacities of these would-be criminals and the potential market for such activities gone unnoticed by organized crime.[39]

---

[36] *Id.* at 85–89.

[37] *Id.* at 89.

[38] While well-known and accepted in the cybersecurity industry, there is limited empirical data to validate these conclusions. There is some limited data available on this from the trade press and some additional limited data from computer science researchers. Federal and international law enforcement agencies have released (very) limited aggregate data, and the only publicly available unclassified data set of cybersecurity "breach" incidents provides only incident data and generally not data on the perpetrators themselves.

[39] *See generally* Jason Franklin et al., An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants (Oct. 31, 2007) (paper presented at the 14th ACM Conference on Computer and Communications Security), *available at* http://www.cs.cmu.edu/~jfrankli/acmccs07/ccs07_franklin_eCrime.pdf (examining the underground market for advertisement, sale, and exchange of stolen sensitive financial information); Brian Krebs, *Shadowy Russian Firm Seen as Conduit for Cybercrime*, WASH. POST, Oct. 13, 2007, at A15 (providing a qualitative account of businesses engaged in the trafficking of stolen consumer data).

The modern result is what I describe as a "cybercrime ecosystem," in which participants are stratified along levels of technical sophistication, access to the most recent data on and methods for compromising computer systems, and degree of sensitivity of target computer systems.[40] The teenage youths hacking the Pentagon of Rep. Hughes's day are not so much gone as supplanted or captured by organized activity in an interconnected world where computer exploits are commoditized and access to large-scale attack networks (Botnets) are controlled by a smaller set of more sophisticated gatekeepers.

1. *Security Vulnerabilities and the "Cybercrime Ecosystem"*

The activities of financially motivated hackers or organizations, and to some extent politically motivated hackers or organizations, rely heavily on the availability of cybersecurity vulnerabilities. Colloquially known within the industry as "exploits," these vulnerabilities are aspects of computer systems that provide a potential attacker the ability to engage the target computer system in activities for which it was not intended or which the administrators of that system have attempted to prohibit by technical means. These are the types of "attacks" or "hacking" that Professor Kerr asserts should form the core test of whether "unauthorized access" to a system has occurred.[41] As I describe in detail in Parts II and III, I believe Professor Kerr's proposal in this regard is incomplete both in that it fails to cover certain types of activities contemplated by electronic-crimes statutes and in that it incorrectly assumes code-based restrictions can (let alone will) fully (or even mostly) implement the restrictive and permissive desires of system operators. Nonetheless, the background of the code-circumvention or exploit ecosystem is an important element of the justification for computer-misuse statutes not yet discussed in the literature. This section provides an overview of that ecosystem as a background for understanding the need for such statutes, backed by the force of the criminal law, in the modern era.[42]

Cybersecurity vulnerabilities can be modeled in a lifecycle from initial discovery to final commoditization. The emergence of vulnerabilities can

---

[40] The concept of the "cybercrime ecosystem" was developed collaboratively by the author and Mark Paulding, Esq., an attorney with Hogan Lovells US LLP and president and CEO of YellowHat Laboratories, Inc. (a cybersecurity technology company).

[41] Kerr, *supra* note 11, at 1643 ("I propose that courts . . . limit the phrase 'without authorization' to the circumvention of code-based restrictions.").

[42] The cybercrime ecosystem proposed in this section, and the discussion of cybersecurity vulnerabilities that follows, stem from the collaborative work discussed *supra* in note 40 and from my ongoing research into cybersecurity regulation. *See* David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. (forthcoming 2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2241838.

best be described primarily as a process of discovery by scientists rather than one of creation by hackers. Technologists study information systems to determine unanticipated ways in which those systems can be manipulated to deviate from their normal operation. The methods for causing such deviations are vulnerabilities that can be activated or "exploited" to exercise (unauthorized) control over the system. This process of discovery, which often focuses on technical vulnerabilities but may also include administrative or physical vulnerabilities, is the first stage in the vulnerability lifecycle.

While some vulnerabilities may be widely distributed soon after discovery, most follow a lifecycle of distribution commensurate with their ability to be exploited for strategic, financial, or social gain. Potential for strategic gain focuses on incentives for organizations or state actors to target specific assets. Generally these assets are targeted to enable political, military, or economic goals, and the targets are not fungible. Potential for financial gain creates incentives for individuals and organizations to exploit vulnerabilities that may allow them to engage in fraud, identity theft, and other financial crimes that can be executed through or substantially facilitated by unauthorized access to information systems. Unlike with strategic incentives, financially motivated attackers generally view targets as commodities—any target capable of resulting in a "fraud conversion" is as valuable as any other such target. Social gain follows a separate pattern, under which actors—primarily individuals—seek to elevate their standing within social groups by gaining unauthorized access to information systems.

These three categories collectively suggest the incentive structures that result in the vulnerability lifecycle. The lifecycle models the emergence of cybersecurity threats from advanced, recently discovered attacks to highly commoditized, well-known vulnerabilities for which readily accessible solutions exist. Strategic incentives drive the first stage in the vulnerability lifecycle. This "innovation" occurs when strategically oriented entities identify or fund the identification of "new" vulnerabilities. Such entities consistently need to identify new vulnerabilities because their incentives are based around the idea of finding the crack in the wall of a specific target, rather than any wall with a known (but unrepaired) breach. Consider, for example, the case of the car thief. Most car thieves are unconcerned with getting any one person's specific car, but rather focus on ensuring they get any (acceptable) car. Hence the advice about easily circumventable security devices—if you can slow down the thief enough to make it not worth their while compared to the next car, the thief will move on to that next car. In contrast, the high-end or specialty-order car thief—the one from the movie *Gone in 60 Seconds* who takes orders for specific cars—

will need to be able to circumvent all the security devices for that one, specially modified, 1966 Ford Mustang. And so it goes with information-security incentives: if the attacker is strategically motivated, he will need to identify every possible vulnerability to ensure he can deface the Arizona State Police website, not just the website of any random police department. Thus these goals drive the identification of new vulnerabilities, whether by members of the organizations or governments engaged in strategic actions themselves or by those entities contracting the services of skilled technologists.

Once developed, these vulnerabilities create a "secondary market" through which strategically oriented entities can "fund" their future operations (or, perhaps, derive secondary "social" benefits in the case of politically motivated organizations like LulzSec).[43] This "commercialization" of threats forms the second stage in the vulnerability lifecycle, when financially motivated organizations "purchase" newly developed vulnerabilities after initial use but before those vulnerabilities become widely known. The key difference for financially motivated entities lies in the lifecycle stage at which they operate. While most financial fraud efforts do not require targeting a specific entity, such as a given bank, they do require overcoming leading-edge security—financial institutions, historically aware of their attractiveness as targets, are likely to repair vulnerabilities before those compromises become well-known. For organized criminal enterprises to profit from attacks on more fortified financial institutions, therefore, those enterprises must be able to exploit vulnerabilities sufficiently early in the lifecycle that enough targets have not yet patched the vulnerability.

The final stage in the vulnerability lifecycle (historically at least) is driven by the desire for social gain. Colloquially termed "script-kiddies," attackers in this category are concerned with elevating their social standing by compromising any information system. This elevation of social standing can take many forms, ranging from simple praise and admiration of peers to literal gain from identity theft and (disorganized) fraud. Unlike in the case of commercialized vulnerabilities, socially motivated attackers generally are completely nonspecific as to what class of system they attack, and are unconcerned with compromising only systems that are likely to employ more current and/or advanced defensive procedures. Thus, compromising

---

[43] LulzSec was an offshoot of the well-known hacker collective "Anonymous," key members of which recently pleaded guilty in a U.K. court to charges relating to the 2011 high-profile attacks against Sony Corporation and the U.S. Central Intelligence Agency. *See* Mathew J. Schwartz, *LulzSec Hackers Plead Guilty to CIA, Sony Attacks*, INFORMATIONWEEK SECURITY (Apr. 10, 2013, 9:07 AM), http://www.informationweek.com/security/attacks/lulzsec-hackers-plead-guilty-to-cia-sony/240152582.

these systems becomes a matter of identifying any system that does not maintain up-to-date security, an easy task in the contemporary security environment. The transfer mechanism from commercialized vulnerabilities to fully commoditized vulnerabilities is not specifically clear, but the transfer incentives can partially be defined by the limited term of usefulness for commercialized vulnerabilities discussed above. Once a commercialized vulnerability becomes sufficiently well-known that it no longer is likely to yield a financial return, maintaining the relative "secrecy" of that vulnerability no longer confers an advantage on financially motivated attackers and their incentives to keep it secret—and force their constituent members to do the same—drop accordingly.

Finally, it is worth noting that certain activities, variously titled "hacktivism,"[44] may be somewhat orthogonal to the ecosystem described in this section. As described in the sources cited in note 44, hacktivists have many incentives for their activities, some of which may be fully independent of (and perhaps opposite to) financial gain, which would complicate their placement within the ecosystem considered as a linear progression. Future work examining the cybercrime ecosystem may wish to consider using multidimensional/multifaceted approaches.[45] However for the purposes of this Article the linear ecosystem described herein adequately describes the majority of activities deserving of criminal punishment described in Part II.B of this Article.

C. CRIMINAL AND CIVIL PROSECUTORIAL HISTORY

This section presents an overview of select criminal and civil prosecutions under the CFAA. As noted above, more comprehensive

---

[44] *See generally* Sean Gallagher, *'Funded Hacktivism' or Cyber-Terrorists, AmEx Attackers Have Big Bankroll*, ARS TECHNICA (Mar. 30, 2013, 7:45 AM), http://arstechnica.com/security/2013/03/funded-hacktivism-or-cyber-terrorists-amex-attackers-have-big-bankroll/; Peter Ludlow, *What Is a 'Hacktivist'?*, N.Y. TIMES OPINIONATOR (Jan. 13, 2013, 8:30 PM), http://opinionator.blogs.nytimes.com/2013/01/13/what-is-a-hacktivist/; *see also* Mathew J. Schwartz, *9 Ways Hacktivists Shocked the World in 2012*, INFORMATIONWEEK SECURITY (Dec. 21, 2012, 9:06 AM), http://www.informationweek.com/security/attacks/9-ways-hacktivists-shocked-the-world-in/240145117.

[45] *See, e.g.*, David Bernard Thaw, Characterizing, Classifying, and Understanding Information Security Laws and Regulations: Considerations for Policymakers and Organizations Protecting Sensitive Information Assets 29–30 (May 12, 2011) (Ph.D. dissertation, University of California, Berkeley), *available at* http://www.davidthaw.com/papers/DavidThawDissertationFinal.pdf (citing ARLENE G. TAYLOR, THE ORGANIZATION OF INFORMATION 300 (2d ed. 2004)).

overviews of this history already exist in the cybercrime literature,[46] and this Article does not challenge that work. Rather, this section examines notable cases that will be used to illustrate how the revised mens rea requirement proposed in Part III would have achieved an outcome more consistent with the types of harms against which Congress sought—and ought—to protect.

1. *United States v. Drew (C.D. Cal. 2009)*

In *United States v. Drew*, defendant Lori Drew was prosecuted under the CFAA for actions stemming from violations of the website myspace.com's (MySpace)[47] terms of service.[48] Drew, the mother of a teenage daughter, created a falsified profile on MySpace for the purpose of harassing another teenage girl (Megan Meier) who was a classmate of Drew's daughter.[49] The harassment via the falsified profile had such a substantial emotional impact on Megan Meier that she ultimately committed suicide.[50]

After trial, the jury convicted Drew on the sole count of "accessing a computer involved in interstate or foreign communication without authorization or in excess of authorization to obtain information . . . ."[51] Drew subsequently moved to have the conviction vacated pursuant to Federal Rule of Criminal Procedure 29[52] on the grounds that conviction under the CFAA, where exceeding authorized access was a function solely of violation of a website's terms of service, was insufficient to constitute a misdemeanor violation of the CFAA and unconstitutional under the void-

---

[46] *See* Kerr, *supra* note 2; Matwyshyn, *supra* note 5.

[47] At the time of Drew's actions, MySpace was one of the leading social networking websites by volume of users and user activity, "receiving an estimated 230,000 new accounts per day . . . . [E]ventually the number of profiles exceeded 400 million with over 100 million unique visitors worldwide." United States v. Drew, 259 F.R.D. 449, 454–55 (C.D. Cal. 2009). As the average user of social networking websites in the United States is now aware, MySpace's presence has substantially diminished and been supplanted by rival Facebook. Readers desiring to contextualize the impact of Drew's actions in a "modern" setting may wish to consider what effect could result were such actions to be taken today via Facebook.

[48] *Id.* at 452.

[49] *Id.*

[50] *Id.*

[51] *Id.* at 453; *see also* 18 U.S.C. § 1030(a)(2)(C) (2006).

[52] Federal Rule of Criminal Procedure 29 provides that "[a]fter the government closes its evidence or after the close of all the evidence, the court on the defendant's motion must enter a judgment of acquittal of any offense for which the evidence is insufficient to sustain a conviction." FED. R. CRIM. P. 29. This may include a defendant challenging a conviction on grounds involving matters of law for the court (as trier of law) to decide. *See Drew*, 259 F.R.D. at 456 (citing United States v. Pardue, 983 F.2d 843, 847 (8th Cir. 1993)).

for-vagueness[53] doctrine.[54]

The court's analysis suggests that the mens rea element of § 1030(a)(2)(C) of the CFAA does not present a direct impediment to Drew's conviction.[55] The court did, however, grant Drew's Rule 29(c) motion on the grounds that allowing violations of terms of service agreements to sustain criminal liability under the CFAA was unconstitutional under the void-for-vagueness doctrine, in substantial part because it failed to provide sufficient definition of the criminal offense such that "'ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement.'"[56]

Drew is an excellent case with which to examine the conundrum presented by the CFAA's current mens rea element and concept of authorized access. Lori Drew's actions certainly were reprehensible and deserving of criminal punishment. This would be the case even had Megan Meier not ultimately harmed herself; that the states may use their police power to outlaw harassment is not a widely challenged policy decision. Drew's conviction under the current language of the CFAA, however, would have presented a substantial problem—it would have required permitting the criminalization of perhaps otherwise-lawful conduct solely on the basis of an agreement, *subject to change at any time and without active notice*, between private parties. Furthermore, this agreement (the website terms of use) was not subject to negotiation; it was effectively, if not in fact, a contract of adhesion. This result is often troubling for those who read *Drew*—and rightly so. The criminal law is unable to hold accountable a person for such a reprehensible act because of other acts it may *potentially* criminalize. Yet, as discussed in greater detail in Part III, *Drew* is also a compelling example of why the federal law *should* criminalize certain actions taken using a computer. Previewed here briefly, I argue that Drew's actions are properly the subject of federal computer-crimes legislation because her ability to engage in otherwise-unlawful harassment and intimidation (of a minor child, no less!) was substantially

---

[53] For a comprehensive discussion of applications of the void-for-vagueness doctrine to the CFAA, see Kerr, *supra* note 2, at 1571–78.

[54] *Drew*, 259 F.R.D. at 451.

[55] *Id.* at 461–62 ("It cannot be considered a stretch of the law to hold that the owner of an Internet website has the right to establish the extent to (and the conditions under) which members of the public will be allowed access to information, services and/or applications which are available on the website. . . . [W]hile public policy considerations might in turn limit enforcement of particular restrictions, the vast majority of the courts (that have considered the issue) have held that a website's terms of service/use can define what is (and/or is not) authorized access vis-a-vis that website.") (internal citations omitted).

[56] *Id.* at 463 (quoting Kolender v. Lawson, 461 U.S. 352, 357–58 (1983)).

increased and made easier as a function of her unauthorized access to an Internet-connected computer.

2. *United States v. Nosal (9th Cir. 2012) (en banc)*

In *United States v. Nosal*, defendant David Nosal was charged with violations of the CFAA for conspiring with colleagues still employed at a former employer to use their (then-current) access to exfiltrate competitive business information for the purpose of starting a competing business enterprise.[57] Nosal filed a motion to dismiss the indictment arguing that the CFAA does not contemplate misuse of information obtained through (otherwise) authorized access as a criminal violation.[58] The district court initially denied the motion, but after the Ninth Circuit decided *LVRC Holdings v. Brekka*,[59] reheard argument and, consistent with *Brekka*'s ruling, granted the motion.[60] The Government appealed, and a panel of the Ninth Circuit initially reversed the dismissal.[61] Nosal applied for rehearing by the circuit en banc, which was granted. The en banc court reversed the original panel's decision, affirming the district court.[62]

The en banc Ninth Circuit found the mens rea element of § 1030(a)(2)(C) to be nearly tautological.[63] According to the Ninth Circuit's reading of the CFAA, if a person's actions exceed authorized access, they necessarily intended[64] that their actions do so. The en banc court upheld its reasoning from *Brekka*, holding that "the phrase 'exceeds

---

[57] United States v. Nosal, 676 F.3d 854, 856 (9th Cir. 2012) (en banc).

[58] *Id.* at 856.

[59] LVRC Holdings v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2009) (opting, in a civil action brought pursuant to paragraph (g) of the CFAA, for a narrow interpretation of the CFAA and holding that "a person uses a computer 'without authorization' under §§ 1030(a)(2) and (4) when the person has not received permission to use the computer for *any* purpose (such as when a hacker accesses someone's computer without *any* permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway") (emphasis added).

[60] *Nosal*, 676 F.3d at 856.

[61] *See* United States v. Nosal, 642 F.3d 781, 782 (9th Cir. 2011), *rev'd*, 676 F.3d 854 (9th Cir. 2012) (en banc).

[62] *Nosal*, 676 F.3d at 856.

[63] *Id.* at 859 ("In the case of the CFAA, the broadest provision is subsection 1030(a)(2)(C), which makes it a crime to exceed authorized access of a computer connected to the Internet *without* any culpable intent.").

[64] More specifically, the person's state of mind met the relevant threshold for the federal mens rea degree of "intentionally," the degree adopted in the statute. *See* 18 U.S.C. § 1030(a)(2) (2006). *See also supra* Part I, where a discussion of the legislative history sharply contrasts this outcome (where only intent to commit the act, *not* intent that the act constitute or result in unauthorized access, is required) with apparent congressional intent as to the selection of "intentionally" as the mens rea requirement for the CFAA.

authorized access' in the CFAA does not extend to violations of use restrictions."[65] Notably, for the purposes of this Article, the court expressly declined to determine "whether Congress *could* base criminal liability on violations of a company or website's computer use restrictions."[66]

The *Nosal* en banc decision well highlights the risks of an expansive interpretation of "exceeds authorized access" in the context of the CFAA. The majority presents several compelling examples, ranging from minors using *any* of Google's services (prior to March 1, 2012),[67] to letting close friends and relatives access one's e-mail or Facebook accounts, to describing oneself as "tall, dark and handsome" on an online dating website when one is in fact "short and homely" as actions that would "earn you a handsome orange jumpsuit."[68] The court held that these compelling examples, Supreme Court precedent stating that courts shall not rely on the discretion of prosecutors to save an otherwise unconstitutional statutory provision,[69] and the rule of lenity require a narrow construction of this provision of the CFAA "so as to avoid 'making criminal law in Congress's stead.'"[70]

The *Nosal* en banc dissent, while perhaps overly optimistic about the probabilities of prosecutorial discretion as an answer to overbreadth concerns,[71] does present compelling arguments as to the reasons why the federal law *should* criminalize certain computer-misuse actions. The dissent argues that misuse of employer computer systems should be subject to criminal penalty in certain cases, analogizing the need for criminalization

---

[65] *Nosal*, 676 F.3d at 863.

[66] *Id.*

[67] On March 1, 2012, Google implemented a single service-wide privacy policy merging its privacy commitments across all its web services into a single document. *See* Kate Freeman, *Google Changes Again, Launches One Privacy Policy to Rule Them All*, MASHABLE (Jan. 24, 2012), http://mashable.com/2012/01/24/google-changes-again-launches-one-privacy-policy-to-rule-them-all/. The *Nosal* en banc majority notes that prior to this change, although "not widely known . . . Google forbade minors from using its services." *Nosal*, 676 F.3d at 861.

[68] *Nosal*, 676 F.3d at 861–62.

[69] *Id.* at 862 (citing United States v. Stevens, 130 S. Ct. 1577, 1591 (2010)).

[70] *Id.* at 862–63 (quoting United States v. Santos, 553 U.S. 507, 514 (2008)).

[71] *See, e.g.*, *id.* at 864 (Silverman, J., dissenting) ("In ridiculing scenarios not remotely presented by *this* case, the majority does a good job of knocking down straw men—far-fetched hypotheticals involving neither theft nor intentional fraudulent conduct, but innocuous violations of office policy."); *cf.* Lee v. PMSI, Inc., No. 8:10-cv-2904-T-23TBM, 2011 WL 1742028, at *1–2 (M.D. Fla. May 6, 2011) (dismissing a former employer's counterclaim asserting CFAA violations for "excessive [personal] internet usage" in an employment discrimination lawsuit brought by a former employee alleging she was unlawfully discriminated against for becoming pregnant); *Nosal*, 676 F.3d at 860 n.6 (majority opinion) (citing *Lee*).

to that found in consumer banking and auto sales:

> A bank teller is entitled to access a bank's money for legitimate banking purposes, but not to take the bank's money for himself. A new car buyer may be entitled to take a vehicle around the block on a test drive. But the buyer would not be entitled . . . to take the vehicle to Mexico on a drug run.[72]

And indeed, federal law *does* criminalize these activities.[73] Such activities pose a sufficiently compelling danger to society and individuals that Congress has made the policy decision to throw behind their prevention the weight of the criminal law. As I discuss in detail in Part I, these compelling examples may not translate well to the *Nosal* facts, which are, perhaps, activities better suited to resolution (and prevention) through civil litigation under theories of tort and contract.

3. *United States v. John (5th Cir. 2010)*

The bank-teller example presented by the dissent in *Nosal* mirrors that of the case of *United States v. John*.[74] In *John*, defendant Dimetriace Eva-Lavon John was charged with, *inter alia*, violation of the CFAA when, as a Citigroup employee, she used Citigroup computers to access information about customer accounts for the purposes of providing that information to others to incur fraudulent charges on Citigroup customer financial accounts.[75] John appealed her jury conviction on these (and other) counts on the grounds that the CFAA only prohibited unlawful acquisition of information from a computer, not unlawful *use* following authorized acquisition.[76] The Fifth Circuit rejected this formulation of the statute, holding that access can be limited by purpose and that "[s]he was not authorized to access [customer] information for any and all purposes but [rather] for limited purposes."[77] The court noted the Ninth Circuit's concerns in *Brekka* regarding potential defendants lacking constitutionally required notice of changes in policy, reasoning alternatively that "[a]n authorized computer user 'has reason to know' that he or she is not authorized to access data or information in furtherance of a criminally fraudulent scheme."[78]

The reasoning presented here by the Fifth Circuit's holding illustrates

---

[72] *Nosal*, 676 F.3d at 865 (Silverman, J., dissenting).

[73] *See, e.g.*, 18 U.S.C. § 656 (2006) (criminalizing "[t]heft, embezzlement, or misapplication by bank officer or employee"); § 2312 (criminalizing "[t]ransportation of stolen vehicles").

[74] United States v. John, 597 F.3d 263 (5th Cir. 2010).

[75] *Id.* at 269.

[76] *Id.* at 271.

[77] *Id.* at 272.

[78] *Id.* at 273.

well why the federal law *should* criminalize certain computer crimes. As I discuss in detail in Part I, computers—like telegraph and telephone communications systems—facilitate the perpetration of crimes in new ways that criminals continue to discover as technology develops. As a brief preview of my argument in that Part, I suggest that the federal law must enable deterrence of computers and other modern information systems as vehicles for enhancing the ability to commit existing crimes and affording criminals the opportunity to innovate in developing new crimes.

II. CRIMINALIZATION BY CONTRACT: COMPUTER-CRIME HARMS AND PREVENTION AND PUNISHMENT

This Part explores the concept of defining criminal activities as a function of agreements among private parties. This concept is neither new nor unique to computer-related crimes; physical-world examples of private agreements defining the boundaries of criminal activity have existed at common law for centuries. The classic, and perhaps most well-known example, is that of criminal trespass. What perhaps *is* novel, or at least uncommon, in the context of cybercrime is that the private agreements establishing criminal boundaries are generally complex, lengthy, difficult to understand, and subject to change at any time and without notice.

I begin with a discussion of the concept of "authorized access" that so permeates the scholarship and judicial opinions interpreting the CFAA. I then proceed to contrast that concept with the view of Congress's original intent developed in Part I. I then examine how, together, these approaches do and do not accord with recent CFAA jurisprudence. This discussion lays out the problem now facing society—how to address the very real threat of modern computer crimes while both avoiding overbreadth and protecting the historic right of private property owners to set limits on the use of their property by others. Equally important, this discussion also highlights the challenge of balancing overbreadth with the need for deterring and/or punishing socially undesirable activities. Since much of the CFAA debate focuses on the question of private agreements as a basis for criminal sanctions, this discussion may be most informative respecting the role of the criminal law in maintaining predictable property relations. However, as discussed below in Part II.B, many of the potential actions with which I argue the federal criminal law should be concerned have serious consequences beyond property interests. Thus, as readers consider the implications of my analysis, I suggest that the importance of punishing social harms (e.g., the public shaming of a victimized teenager[79]) may be equally important.

---

[79] *See infra* note 95.

I first propose a typology of the types of socially undesirable activities federal computer-crimes law should be concerned with and proceed to discuss and compare the efficacy of civil and criminal deterrence options for discouraging those activities.

A. THE CONCEPT OF "AUTHORIZED ACCESS"

As discussed in Part I, the key question in CFAA prosecutions often is whether a person has engaged in activities constituting "unauthorized access" to or "exceed[ing] [their level of] authorized access" to a computer system.[80] The mens rea element of the statute has become nearly meaningless as a distinguishing condition, and the concept of a "protected computer" has been extended to nearly any Internet-capable device.[81] Thus in many (if not most) CFAA cases, the question becomes whether the defendant's actions (regardless of that person's intent) constitute "unauthorized access" to a computer system or whether those actions "exceeded authorized access" on the system.[82]

As discussed in the Introduction, this Article in part responds to Professor Kerr's invitation for dialogue regarding criminalization of conduct involving computers and the Internet.[83] Specifically, I suggest that Professor Kerr's contention that code-based restrictions can provide a complete solution to "access" and "authorization" concepts in the computer-misuse context is flawed and overlooks practical, theoretical, and normative problems. In the section that follows, I propose a typology for categorizing computer misuse and in Part III below I examine how Professor Kerr's proposal fails to address some of these concepts.

---

[80] *See* 18 U.S.C. § 1030(a)(2), (e)(6) (2006).

[81] *See* United States v. Drew, 259 F.R.D. 449, 457–58 (C.D. Cal. 2009) (holding that one element of a computer being protected "is satisfied whenever a person using a computer contacts an Internet website" and that user's computer or information device receives or "reads any response from that site") (citing Reno v. American Civil Liberties Union, 521 U.S. 844, 849 (1997) (observing the international reach of computers connected to the Internet)); *see also* 18 U.S.C. § 1030(e)(2)(B) (defining a "protected computer" as one "used in 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"). Perhaps curiously, this may extend as far as prosecuting a U.S. citizen in a domestic court under U.S. law for using a foreign computer system in a way that otherwise is fully lawful under U.S. law but that (maybe unintentionally) constitutes a technical violation of the terms of service of that foreign computer system, and thus constitutes an act "exceed[ing] authorized access" on the foreign system. Even more curious might be the case where the governing provision of the terms of service is in a foreign language but the primary user interfaces of the website are available in English.

[82] For a more detailed discussion, see generally Kerr, *supra* note 11.

[83] *Id.* at 1601.

B. THE "HARMS" OF COMPUTER CRIME—AGAINST WHAT *SHOULD* WE PROTECT?

This section proposes a four-part typology to describe the types of computer-based activities with which federal computer-crime law should be concerned. The typology derives from practical, theoretical, and normative concerns with Professor Kerr's "code-based restriction" test.[84] In a 2003 article, Professor Kerr proposes that "courts limit access 'without authorization' to access that circumvents restrictions by code."[85] I lay out here the framework of concerns with such a test. Later, in Part III, I revisit these concerns in the context of a fully developed background exploring what types of computer misuse should be criminalized and why.

A code-based restriction test has practical, theoretical, and normative problems. From a practical standpoint, it is unclear that operators of computer systems *will* implement such restrictions for all types of activities they consider inappropriate to their systems. Furthermore, it is unclear that even the intent to implement such restrictions will yield an effective result, both for reasons of technical competence[86] and cost restriction.[87] From a theoretical standpoint, it is unclear that all the types of use restrictions a computer system operator may wish to impose *can* be implemented via code-based restrictions.[88]

Finally, from a normative standpoint, consider how a code-based restriction proponent might answer the first two questions. One possible such answer claims the concerns raised by the first two problems are *de*

---

[84] *Id.* at 1649.

[85] *Id.* (emphasis omitted).

[86] This is a substantially challenging technical problem, not one easily accomplished even *with* qualified personnel, and qualified personnel are not easy to find.

[87] Cost restrictions are not limited to direct costs; implementing such restrictions often substantially impacts business processes and it is well-known in the information security industry that such impact carries high indirect cost.

[88] A simple example is a social networking website's prohibition on using the service to threaten, harass, or intimidate another person. Threats, harassment, and intimidation are contextual and nondeterministic in nature—thus, they cannot easily, and likely cannot with any useful reliability, be represented in a code-based restriction. Nonetheless, they are perfectly legitimate activities for a computer system operator to wish to restrict, and the consequences of such activities can be so severe that ordinary tort and contract remedies are a poor deterrent (if one at all) to potential offenders. It is also worth noting that existing cybersecurity regulation recognizes that not all threats can be managed by technical measures, but rather are grouped in "administrative, technical, and physical" categories. *See, e.g.*, 15 U.S.C. § 6801(b) (2006) ("[E]ach agency . . . shall establish appropriate standards . . . relating to *administrative, technical, and physical safeguards* . . . .") (emphasis added); *see also, e.g.*, BJ's Wholesale Club, Inc., 140 F.T.C. 465, 472 (2005) (requiring that "respondent obtain an assessment and report . . . set[ting] forth the specific *administrative, technical, and physical* safeguards that respondent has implemented") (emphasis added).

minimis and that only whatever restrictions *can* be implemented in a code-based restriction are proper bases for criminal liability. I suggest that such a response is undesirable. It ignores the potential harms that are made worse by and perhaps even entirely dependent upon modern computer and information systems as a vehicle for undesirable activity. As I argue in the following sections, the criminal law *should* be concerned about such harms. Normatively stating that they can be ignored under a computer-misuse law is, I suggest, a dangerous proposition opening the door to the Internet as a vehicle to commit otherwise unlawful activity in a manner difficult (if not impossible) to prosecute.

These considerations suggest four categories into which the types of activities against which I claim federal computer-crime law should protect can be grouped: (1) activities where the specific intent is the circumvention of a code-based restriction (colloquially known as "hacking"); (2) activities already criminalized under existing "physical-world" crimes but whereby those activities are made easier to accomplish or their effect on victims amplified as a function of computer and information technologies; (3) activities that do not give rise to the need for criminal deterrence in the physical world, but when considered in the context of computers and the Internet or virtual environments may take on a character requiring criminal deterrence; and (4) activities specifically unique to computers and the Internet, which both are otherwise lawful and lack physical-world analogues that may already provide a degree of criminal deterrence.

1. *Circumvention of Code-Based Restrictions*

This category describes the most "straightforward" form of computer misuse—the classic "hacking" described by the congressional debates discussed in Part I above. As described by Professor Kerr,[89] this can include a range of activities from simple password misuse[90] employed by technically unsophisticated rogue employees to more sophisticated cyberattacks employed by attackers at the innovation and (to some extent) commodification stages of the cybersecurity vulnerability lifecycle proposed in Part I.

Many of these activities, particularly those falling closer to the innovation stage of the cybersecurity vulnerability lifecycle, pose clear examples of precisely the types of harmful activities with which Congress was concerned when it passed the CFAA.[91] Other activities, however, such

---

[89] Kerr, *supra* note 11.

[90] For example, the unauthorized use of another user's password.

[91] *See* 18 U.S.C. § 1030 (2006); *supra* Part I (discussing the congressional debates and the Act's introduction by Representative Hughes).

as password sharing, technically and precisely fall under the ambit of circumventing code-based restrictions but likely fall far afield of Congress's intent to criminalize unauthorized access. Consider, for example, the teenage girl who shares her Facebook password with her mother to seek advice on a social circumstance while away at college, or the bedridden widower who shares his financial account password with his sister so she can assist in managing his financial matters while he is incapacitated. Surely these are not the types of activities Congress sought to criminalize. I develop this idea further in my criticism of Professor Kerr's code-based restriction test in Part III.

2. *Existing Criminal Activities Made Easier or Having Increased Impact on Victims*

This category of activities is often controversial within the context of cyberlaw.[92] It addresses those things for which the physical world already has existing law *potentially* on point, but where it could be argued that such law is inadequate to deal with computer-based or virtual-world crimes. This inadequacy manifests as a result of: (1) the transaction cost of engaging in the crime being substantially lowered as a function of computer use or execution of the act in a virtual world; or (2) the damage, harm, or other resultant injury to the victim(s) being amplified as a function of computer use or execution of the act in a virtual world.

A common example of the first category is wire fraud. The physical-world[93] version of wire-fraud cases bears a nontrivial marginal cost of

---

[92] Consider the classic debate regarding cyberspace and the law of the horse framed by Judge Frank Easterbrook and Professor Lawrence Lessig. Judge Easterbrook argued that "the best way to learn the law applicable to specialized endeavors is to study general rules . . . . Teaching 100 percent of the cases on people kicked by horses will not convey the law of torts very well." Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 207–08. Professor Lessig responsively argued, "[T]here is an important general point that comes from thinking in particular about how law and cyberspace connect." Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 502 (1999). This is because cyberspace substantially changes a fundamental characteristic of regulability—i.e., that whereas the architecture of the physical world (e.g., roads, rivers, buildings, etc.) has strong permanence, the architecture of cyberspace (e.g., the computer code that implements various systems, services, apps, etc.) has comparatively far weaker permanence and thus is more easily subject to change. *Id.*; *see also* LAWRENCE LESSIG, CODE VERSION 2.0, at 31–82 (2006).

[93] In the context of wire (as opposed to strictly postal mail) fraud, a "physical-world" characterization may seem idiosyncratic—wire transmissions are by nature electronic communications. In their original form (telegraph communications), however, up to and including the use of telephone systems, such acts still carried a substantial marginal cost of execution just as did such fraud via postal mail. This marginal cost is what distinguishes them from the category of "virtual-world" or "(fully) electronic" crimes discussed in this

execution—each new "target" for the fraudulent scheme costs the perpetrator a nontrivial amount of time or currency. By contrast, when such a crime is executed via computer, such as by e-mail, this marginal cost is dramatically reduced (if not de facto eliminated). Stated differently, the use of the computer both reduces a deterrent against the crime and increases the number of probable targets of the crime. Such schemes are so widespread and executed at such low cost that the average reader of this (or any other scholarly or scientific) journal need only look to the "spam" folder of his e-mail account to find evidence of them.[94]

Recent years contain several notable examples[95] of the second category in the form of cyberbullying[96] and harassment. In these instances, the impact of harassment on a target victim was multiplied quite literally thousands (if not millions) of times over as the scope of the audience was amplified through the use of computers and the Internet. Without such outlets, perpetrators of those crimes would be limited either to publication via traditional press and media outlets—where at least some degree of journalistic professional discretion should serve as a buffer—or to the perpetrator's self-funding of such publication, where cost provides a similar buffer limiting harm. In the age of social networking and web self-publishing media such as Facebook, YouTube, Instagram, and the like, such harm to the victim may be achieved at effectively no cost to the perpetrator.

---

section, because in that latter case a marginal cost of execution no longer acts as a deterrent to the prospective criminal.

[94] Barracuda Networks, a commercial provider of spam-filtering software, provides a public report of their spam-filtering activities. As of March 4, 2013, 84% of total e-mail processed by Barracuda's filtering equipment was spam, based on a forty-eight-hour running average. *Spam Data*, BARRACUDACENTRAL (Mar. 4, 2013, 11:31 PM), http://www.barracudacentral.org/data/spam; *see also* Charles Arthur, *Interview with a Link Spammer*, REGISTER (Jan. 31, 2005, 1:41 PM), http://www.theregister.co.uk/2005/01/31/link_spamer_interview/; Paul Boutin, *Interview with a Spammer*, INFOWORLD (Apr. 16, 2004), http://www.infoworld.com/d/security-central/interview-spammer-717. For a contemporary account of spamming incentives in social media, see Graham Cluley, *Interview with a Pinterest Spammer, Earning $1000 a Day*, NAKED SECURITY (Mar. 28, 2012), http://nakedsecurity.sophos.com/2012/03/28/pinterest-spammer-interview/.

[95] *See, e.g.*, Brandon Baur & Reena Ninan, *Bullied Teen Amanda Todd's Video Passes 17M Views*, ABCNEWS (Oct. 24, 2012), http://abcnews.go.com/US/bullied-teen-amanda-todds-video-passes-13m-views/story?id=17548856; Michael Pearson, *Social Media Casts Spotlight on Ohio Rape Case*, CNN (Jan. 4, 2013, 2:17 AM), http://www.cnn.com/2013/01/03/justice/ohio-rape-online-video; Andrew Welsh-Huggins, *Social Media Threats Against Steubenville Rape Victim Must Stop, Says Ohio Attorney General*, VANCOUVER SUN (Mar. 19, 2013), http://www.vancouversun.com/news/Twitter+Facebook+threats+against+Steubenville+rape+victim+must+stop/8122281/story.html.

[96] *See generally* Lyrissa Lidsky & Andrea Pinzon Garcia, *How Not to Criminalize Cyberbullying*, 77 MO. L. REV. (forthcoming 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2097684.

A notable physical world analogue to the second category is the concept of sentencing enhancements for crimes committed through the use of weapons, specifically firearms. The underlying crime is the same, but society has made a decision to further punish that underlying crime as a result of it being committed involving the use of a firearm—even if the firearm never is discharged. This is similar to the case of using computers and modern information systems in the commission of crimes.

It is upon the analysis of these two sets of examples that I suggest such crimes *should* be criminalized under federal law.

3. *Existing Offensive (but Not Criminal) Activities Rising to the Criminal Level in the Electronic or Virtual Context*

This category of activities addresses those actions that are not criminalized under existing law (although they may give rise to civil liability) but may take on a different nature when conducted electronically or in virtual worlds, where they may rise to a level posing sufficient risk of harm to justify a need for deterrence by criminal sanction. I suggest it likely that as we transition through the Information Age and computers and information systems increasingly become interwoven into our lives, we will become more familiar with the types of activities that fall into this category.

For now, I suggest the following example: commercial advertising on a computer system at a scale that so overwhelms the system as to render its primary function ineffective or completely inoperable, but where the individual acts do not themselves circumvent any code-based restriction or otherwise constitute a criminal act. One possible example of this is the sending of excessive e-mail advertisements (colloquially known as spam) or the posting of commercial advertisements in blog comments to such a degree that the blog itself becomes unmanageably long and unreadable because the pages cannot render properly.[97]

4. *Computer-Specific Activities that Are Otherwise Not Criminalized*

The final category of activities is unique to the computer context, and does not represent a "fixed list" of possibilities. As technology advances, those at the innovator end of the cybersecurity vulnerabilities lifecycle will develop new means of executing attacks on computing systems. Assuredly, most of these discoveries will fall into the first category by involving circumvention of at least some code-based restriction. At least a few, however, will not, and will constitute unauthorized access only as a function of what is (not) permissible under a computer system's terms of

---

[97] *See* Arthur, *supra* note 94.

service. The technical nature of the attack will be such that code-based restrictions will be unable to provide a "lock" that must be broken before the attack achieves its goal, and the activities involved in the attack will otherwise not be criminalized.

The most salient example of this is a distributed denial-of-service (DDoS) attack.[98] In this type of attack, many thousands or perhaps millions of computers all attempt to access an Internet resource concurrently in an attempt to overload that resource, rendering it unable to respond to requests. The most common variant is a DDoS attack against a specific website, in which these computers repeatedly request a page or pages from a website, such that the spike in traffic is greater than the website's servers can handle and the website effectively becomes inaccessible. Notable DDoS attacks have been launched by politically motivated attackers against prominent government[99] and private-sector[100] websites.[101] The mechanism of attack can vary but each "attacking" computer circumvents no code-based restriction on *the website itself*[102] by simply attempting to access a website. Nor do any of those computers individually (or, to the best of my knowledge, collectively) violate any other[103] state or federal statute.

---

[98] For an overview of this concept appropriate for nontechnical audiences, see *Denial-of-Service Attack*, WIKIPEDIA, http://en.wikipedia.org/wiki/Denial-of-service_attack (last modified May 20, 2013, 1:56 AM); *see also* SHON HARRIS, CISSP ALL-IN-ONE EXAM GUIDE 1034–35 (5th ed. 2010) (providing additional technical detail).

[99] *See, e.g.*, Mathew J. Schwartz, *LulzSec Claims Credit for CIA Site Takedown*, INFORMATIONWEEK SECURITY (June 16, 2011, 10:35 AM), http://www.informationweek.com/security/cybercrime/lulzsec-claims-credit-for-cia-site-taked/230800019.

[100] *See, e.g.*, Robert Lemos, *DDoS Attacks on Major Banks Causing Problems for Customers*, EWEEK (Dec. 28, 2012), http://www.eweek.com/security/ddos-attacks-on-major-banks-causing-problems-for-customers/.

[101] I mention attacks on government-owned computers because of their notoriety and importance to understanding the overall cybersecurity/cybercrime ecosystem. It is worth noting, however, that attacks against (at least) federal government computer systems are handled under separate provisions of the CFAA, *see* 18 U.S.C. § 1030(a)(1) & (a)(3) (2006), which have received substantially less scrutiny by federal appellate courts. While the structure of the language in the statute is similar, different interests are protected when government computers are at risk than when private computers are at risk. For the purposes of this Article, I limit the scope of my examination and its resultant proposed reform to those provisions of the CFAA pertaining to private computer and information systems.

[102] Some DDoS attacks are orchestrated using "innocent" third-party computers onto which attackers have (possibly by circumventing a code-based restriction) installed software that enables those computers to be remotely instructed to participate in the attack by accessing the target website at a given time. While such circumvention may constitute unauthorized access by circumvention of a code-based restriction *as pertains to the innocent third party*, it does not as pertains to the target of the attack.

[103] An argument could be constructed that this constitutes criminal harassment or assault. However, I think this argument is tenuous both because of the lack of requisite mens rea to cause harm or intimidation to a specific person and because of the lack of requisite effect in

These types of computer-specific actions that clearly result in harm (i.e., the unavailability of a website) but are not otherwise criminalized but for the terms of service of a website (which can prohibit the execution of a DDoS attack or any otherwise-authorized access part of a scheme to disable or disrupt access to the website) are exactly the types of activities against which computer-specific federal criminal law *should* protect. The challenge in protecting against them, however, is that they are ever-changing as technology evolves and difficult to define as a class a priori—particularly without running the risk of opening up avenues for overbroad prosecution. Although beyond the scope of this Article, I suggest to the reader here and later in Part III.C that this type of problem in law may present an interesting crossover with questions of administrative law and delegation of legislative authority.

C. EFFECTIVE PREVENTION: CRIMINALIZATION VS. PRIVATE OPTIONS

The U.S. legal system provides two primary categories of law for the deterrence of socially undesirable actions by private individuals: private law, under which cost may be associated with action through liability under contract or at tort; and criminalization, under which actions are prohibited by the state under penalty of fine, imprisonment, or other use of the police power.[104] These two categories serve different—although sometimes overlapping[105]—purposes. Private liability established under tort or contract law generally concerns circumstances under which one individual's actions cause redressable harm to another. Tort law, for example, may also serve a deterrent purpose,[106] but tort law's primary purpose concerns

---

that regard. Certain exceptional cases—e.g., an attack on a celebrity or political candidate's website—*might* qualify under this standard, but I think criminal prosecution on that basis seems a weak argument at law, and even weaker if tried to a lay jury where a truly "harmed" victim cannot be presented.

[104] Kenneth W. Simons, *The Crime/Tort Distinction: Legal Doctrine and Normative Perspectives*, 17 WIDENER L.J. 719, 720 (2008).

[105] Notably, the CFAA has a civil analogue, 18 U.S.C. § 1030(g). However, it applies only to actions that result in *direct* damages and thus excludes the bulk of the matters discussed in this Article and elsewhere giving rise to overbreadth concerns in the criminal context. Additionally, criminal prosecutions under the CFAA paragraphs for which subsection (g) provides civil liability less commonly involve violations of use agreements, and when those prosecutions do involve such violations, it is usually in the context of a larger otherwise-criminal scheme, such as employees engaged in fraud or larceny conspiracies. *See, e.g.*, United States v. John, 597 F.3d 263, 271–73 (5th Cir. 2010).

[106] *See, e.g.*, Taylor v. Superior Court, 598 P.2d 854, 857 (Cal. 1979) ("The allowance of punitive damages in [motor vehicle collision] cases may well be appropriate because of another reason, namely, to deter similar future conduct, the 'incalculable cost' of which is well documented. [California law] expressly provid[ed] that punitive damages may be recovered 'for the sake of example.'") (internal citations omitted).

maintenance of a reasonable standard of care among actors in society.[107] Contract law primarily is concerned with the establishment of individualized agreements between and among private parties, incurring rights and obligations not part of generalized "standards of care" espoused in tort law. Like tort, however, contract law primarily concerns itself with redress for breach of specific actions. Neither of these private law alternatives[108] focuses on the general prevention of socially undesirable activities or activities for which compensation cannot be provided.

The criminal law, by contrast, concerns the activities society most strongly seeks to prevent. While ranging in degrees of severity, criminal law generally seeks to deter activities that unjustifiably or inexcusably cause substantial harm to individual or public interests.[109] These types of harms may[110] or may not[111] generally have direct civil liability analogues, but in all cases focus on actions the state wishes to prevent. As described by Professor Kenneth Simons, criminal law can be distinguished from tort law in that "criminal law prohibits 'public' wrongs and tort law 'private' wrongs."[112]

This section responds, in part, to criticisms that the concept of website terms of service and other usage agreements constitute private agreements between private parties concerning private matters—and thus are not the proper province of the criminal law. It articulates the deterrence character of each alternative in the context of the cybersecurity ecosystem and the

---

[107] *See, e.g.*, Adams v. Bullock, 125 N.E. 93, 93 (N.Y. 1919) (describing a "duty to adopt all reasonable precautions to minimize the resulting perils [from an action]").

[108] For the purposes of this Article, I do not consider the private law alternative of non-criminal civil penalties (e.g., parking tickets) because an appropriate infrastructure (e.g., an Internet driver's license) does not exist for the administration of such penalties. Furthermore, for at least some of the categories of actors described herein (e.g., sophisticated innovator/code-based restriction circumvention attackers), a civil penalty system even *with* the proper infrastructure would likely be a highly ineffective deterrent as those would be precisely the people most capable of circumventing the system.

[109] *See* N.Y. PENAL LAW § 1.05 (McKinney 2009) ("The general purposes of the provisions of this chapter are: 1. To proscribe conduct which unjustifiably and inexcusably causes or threatens substantial harm to individual or public interests . . . ."); *see also, e.g.*, Criminal Justice Codification, Revision and Reform Act of 1973, S. 1, 93d Cong. § 1-1A.2 ("General Purposes: The purpose of this code is to establish order with justice so that the nation and its people may be secure in their persons, property, relationships, and other interests."). These selected excerpts were suggested in SANFORD H. KADISH & STEPHEN J. SCHULHOFER, CRIMINAL LAW AND ITS PROCESSES 156–57 (7th ed. 2001).

[110] For example, homicide and its tort analogue of wrongful death liability.

[111] For example, adultery, bigamy, perjury, and certain inchoate offenses. However, under the doctrine of negligence per se, if actual damages occur, civil liability may nonetheless result unless the jurisdiction's legislature has expressly repudiated this doctrine. *See* RESTATEMENT (THIRD) OF TORTS § 14 (2010).

[112] Simons, *supra* note 104, at 720.

cybercrime typology described in Parts I and II.B above, and identifies both why private law does not present an effective deterrence mechanism and why the actions described therein are "deserving of punishment" to the degree provided for by the criminal law.

1. *Private Law (Tort and Contract) Deterrence of Cybercrime*

As described above, private law primarily concerns the maintenance of appropriate standards of care (conduct) among actors in society and the preservation of duties assumed in valid agreements. Deterrence in this context thus depends on a combination of several elements. First, there must be a cognizable harm (most often one that is financially measurable)[113] actually and proximately resulting from the tortious act or directly resulting from the breach. Second, the party aggrieved by this act or breach must be both willing and able to initiate and follow through with civil prosecution. Third, the aggrieved party must have the capacity through civil procedure to identify the party responsible for the tortious and/or breaching conduct. Fourth, and most importantly, the allegedly responsible party must have the means to compensate the aggrieved party financially, lest it become "judgment proof" and the aggrieved party's costs in civil prosecution exceed its expected recovery.

In the cybercrime context, the concept of a cognizable harm that is *financially measurable* may be difficult to ascertain. Unlike in the physical-crimes context, when an attacker "accesses (and acquires) information," he does not necessarily deprive the aggrieved party of that information. The marginal cost of copying electronic data is generally trivial; it is in fact a more complex operation to both copy and completely remove information from a computer system than it is only to copy such information.[114] In the cases where an attacker does modify or delete data, ascertaining the value of that data may be complex or even impossible.[115]

---

[113] The need for a harm to be financially measurable stems from the award of damages as the primary "cost" to the bad actor (i.e., tortfeasor or breaching party). If damages cannot properly be measured, except in contract cases where liquidated damages provisions *may* govern, the deterrent effect is substantially reduced because the potential tortfeasor or potential breaching party need not fear judgment against him.

[114] Copying and subsequent deletion of data—the electronic equivalent of absconding with a physical-world file from a filing cabinet—requires two operations, the latter of which is more likely to trigger automated warnings and/or leave traceable evidence. *See infra* note 115. Copying such data—the electronic equivalent of taking the file, bringing it to a photocopier, and then replacing it—involves only one operation and is less likely to trigger automated warnings and/or leave traceable evidence. *See infra* note 115. As evidenced by the physical-world analogues presented here, the electronic equivalents have exactly inverse levels of difficulty and risk from their physical-world counterparts.

[115] Most modern computer operating systems have the capability to monitor file access,

While certain types of data, such as trade secrets or prepatent inventions, may have measurable economic value, the value of other data—such as custodial data,[116] personal files, or software applications[117] and system configuration files[118]—may be limited to the measurement of indirect costs.[119] When the industry standard expects organizations to maintain resiliency protocols for their information systems, determining the *marginal* cost in activating those protocols may be difficult. If an external firm is engaged, the costs may be more calculable, but when internal staff and resources—already maintained by the organization for other reasons—are used, cost determination may be more complicated. While on balance these factors would seem to militate against the costs of civil litigation in many cases, it bears note that in recent months litigants increasingly have attempted to advance such claims.[120]

These reasons also suggest a lack of willingness on the part of potential civil litigants to engage in civil prosecution. The potential

---

execution, modification, and deletion operations. This capacity, part of the broader category of "auditing" functions in cybersecurity, is resource intensive because it requires both real-time constant monitoring and the maintenance of records of actions. Many software applications on a computer will access (read but not modify data from) a file, and will do so with greater frequency than they will delete data from that file. Far fewer applications will delete files, and they will do so with much less frequency than they access files. For this reason, to the extent a computer system operator enables auditing functions, system performance constraints strongly mitigate in favor of enabling auditing functions only for file deletion and not for both file deletion and file access.

[116] "Custodial data" is a term adopted by the information security industry to refer to data, such as consumers' personal information, that is provided to another party for specific purposes (e.g., financial account information for an Internet-based purchase). The term "data custodian" refers to the party responsible for the maintenance of that data consistent with applicable law. *See* Harris, *supra* note 98, at 125–26. Industry-standard practice dictates that custodial data should be redundantly available through backup measures in the event of a system compromise or other failure. *See id.* at 809–12.

[117] Software applications should be reinstallable from their original installation source; it is industry-standard practice to maintain appropriate reinstallation media and/or other backup methods. *See id.* at 805–06.

[118] Practices similar to those described *supra* in note 117 likewise apply to system configuration files.

[119] For example, business disruption, labor, and other costs associated with system restoration from backups; regulatory compliance costs; etc.

[120] *See, e.g.*, Harris v. comScore, Inc., No. 11 C 5807, 2013 WL 1339262, at *10 (N.D. Ill. Apr. 2, 2013) (granting partial class certification in suit against manufacturer of alleged "tracking software" for, *inter alia*, claims of damages to plaintiff class members' computers resulting from installation and/or use of the tracking software); Sharma v. Howard Cnty., No. 12-cv-2269-JKB, 2013 WL 530948, at *7 (D. Md. Feb. 12, 2013) (dismissing for failure to state a claim, but recognizing in dicta that a claim for consequential damages under the CFAA's civil tort provision may include the costs of a responsive investigation); Oracle Am., Inc. v. Serv. Key, LLC, No. C 12-00790 SBA, 2012 WL 6019580, at *4 (N.D. Cal. Dec. 3, 2012).

reputational risks of engaging in public litigation further compound this probable reticence. A prospective corporate litigant, for example, in initiating civil prosecution against a cybertortfeasor, effectively reveals to the public that its defensive cybersecurity measures were inadequate to stop the alleged attacker. Furthermore, the litigation itself bears costs—costs the prospective litigant must weigh against the likelihood of recovery. As discussed above in Part I.B cybercriminals do not represent a group likely to pay a civil judgment, either because they are individuals who lack the resources to do so or because they comprise organized crime in foreign jurisdictions beyond the (effective) reach of U.S. civil courts. Finally, as others have discussed, cybercriminals are often effective at disguising their identities, confounding the capacities of prospective *civil litigants* to identify prospective tortfeasors.[121]

This discussion primarily addresses cybercrime activity in the first category of the typology described above. With respect to the remaining categories, I suggest that individuals will generally engage in activities of these types, and that such individuals will not likely have the capacity to pay civil judgments in amounts sufficient to allow equally financially limited parties the capacity to prosecute a civil claim.[122] One possible exception is the category of commercial entities engaging in advertising activities as described in the third category above. However, these activities represent a sufficiently small percentage of potential socially undesirable acts and are sufficiently distinguishable from other types of acts that even if successfully prosecuted, they seem unlikely to have a deterrent effect outside the limited scope of commercial advertising. At this early stage in development of industries such as online behavior advertising, it is likely premature to predict the deterrence effect on such commercial entities.

Collectively, these factors—particularly the judgment-proof nature of most cybercriminals—strongly suggest that civil litigation is unlikely to be an effective deterrent in the context of the cybersecurity ecosystem and the typology of cybercrime and cybercriminals presented here. Reticence to prosecute, inability to recover even compensatory (let alone punitive) damages, and the high costs of and possible technical barriers to prosecution all suggest that an alternative method of deterrence is required to disincentivize the types of cybercrime activities I suggest society does

---

[121] Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 470 (2012).

[122] Prospective litigants would likely need to engage counsel on a contingent-fee basis, but traditionally judgment-proof defendants such as the average citizen are unlikely to have either sufficient resources or reason to carry the types of insurance that would enable payment of judgments in sufficient amounts to cover the costs of this type of litigation.

have an interest in preventing.

2. *Criminal Law Deterrence*

I consider the possible effect of deterrence through criminal law in the context of three prospective categories of cybercriminals: (1) hackers, who engage in activities in categories 1 or 4 above (regardless of motivation);[123] (2) individuals, who engage in activities in category 2 above; and (3) individuals and entities who engage in activities in category 3 above. For each of these categories, I consider the effect of employing the police power and threat of criminal penalties as a deterrent.

As discussed in the previous subsection, hackers present perhaps the most challenging deterrence problem in that they both may be difficult to identify and may be located in foreign jurisdictions. Both these factors certainly are challenges to the criminal law. Criminal law enforcement, however, has substantially better resources at its disposal than private parties both for the investigative activities required to identify hackers and the interjurisdictional activities[124] required to extend the law's reach and deterrent effect to parties situated outside the territorial United States.[125] The deterrent effect of the criminal law is not hampered by the financial insolvency of hackers; the effect of its primary method of punishment (e.g., imprisonment or other deprivation of liberty) does not vary with the financial capacities of the alleged criminal. Admittedly, I am unaware of any empirical evidence as to the efficacy of threat of criminal punishment in the cybercrime context.[126] However, the analytical prospects are more

---

[123] For the purposes of this analysis, I suggest that whether the motivation is for personal enrichment, financial gain, or political statement (*see supra* Part I.B) is irrelevant as pertains to the possible deterrent effect of criminal sanctions *relative to* that of private law deterrents. In all three cases, the relative reach of the criminal law and the enhanced costs criminalization brings relative to civil liability do not vary based on the hacker's motivation. While that motivation may change the prospective cybercriminal's calculus as to whether the risks of prosecution outweigh the advantages of the act, the difference within each category relative to its private law counterpart will proportionally be the same.

[124] For example, engagement of extradition and other international law enforcement procedures.

[125] Brian Krebs, *Alleged Romanian Subway Hackers Were Lured to U.S.*, KREBS ON SECURITY (June 6, 2012), http://krebsonsecurity.com/2012/06/alleged-romanian-subway-hackers-were-lured-to-u-s/.

[126] Much contemporary criminal deterrence literature focuses on the efficacy of deterrence measures at preventing physical-world (as opposed to electronic) crimes, particularly crimes against persons and/or property crimes. *See generally* Daniel S. Nagin, *Criminal Deterrence Research at the Outset of the Twenty-First Century*, 23 CRIME & JUST. 1 (1998); *see also generally* Steven N. Durlauf & Daniel S. Nagin, *The Deterrent Effect of Imprisonment*, *in* CONTROLLING CRIME: STRATEGIES AND TRADEOFFS 43, 43–94 (Philip J. Cook et al. eds., 2011).

favorable than private law alternatives and at least some such law enforcement efforts have proven effective.[127]

Individuals engaging in acts from category 2, actions already criminalized but made easier, or those where the effect on the victim(s) is amplified through the use of computers, present perhaps the easiest cases to differentiate the efficacy of criminal law versus private law deterrence. As noted above, these actors comprise individuals who are generally judgment-proof in a civil litigation from a financial perspective. The cases and hypotheticals considered in this Article[128] predominantly involve individuals physically present in the territorial jurisdiction of the United States. While the limitations of existing empirical evidence discussed above with respect to hackers still apply to this category, the difficulties in identifying alleged perpetrators and securing them in police custody are substantially reduced (if not trivial). Notwithstanding the absence of empirical evidence on the deterrent effect of criminal sanction in the cybercrime context, this suggests a substantially more effective mode of deterrence than the unlikely probability of civil prosecution.

Individuals and organizations engaging in acts from category 3, actions that are not criminal in the physical-world context but that may justify criminal deterrence in the context of cybercrime, present a challenging question. In the example presented above (overzealous advertising that renders ineffective a computer system's intended operation), the commercial nature of the actor likely (as discussed above) increases the probable efficacy of private law deterrence. Additionally, such action seems well suited to tort remedies—there is a redressable harm resulting from the socially undesirable actions. While compelling, I suggest this approach focuses too much on the commercial nature of the alleged offender and too little on the trespassory nature of the offender's action. Consider, for example, the physical-world analogue. If a neighborhood storeowner entered onto a homeowner's property and placed a single advertising billboard (without permission) on the homeowner's lawn, this action—while technically constituting trespass—would likely be better suited to resolution through civil action. Alternatively, however, if that same storeowner placed 500 such billboards, completely blockading the homeowner's egress from her residence, it seems more probable that law

---

[127] *See supra* note 125; *see also Authorities Bust $72 Million Dollar Conficker Fraud Ring*, INFOSEC ISLAND (June 27, 2011), http://www.infosecisland.com/blogview/14789-Authorities-Bust-72-Million-Dollar-Conficker-Fraud-Ring.html.

[128] Generally speaking, the most prominent examples are those of the malicious insider in an organization using his access to engage in fraud or similar activities (the insider threat), and the malicious individual attempting to harass, threaten, or intimidate another person through the use of social media and related Internet-based communications (the cyberbully).

enforcement would become involved and criminal trespass charges found appropriate. Placing 500 billboards on a homeowner's lawn is, of course, a completely implausible scenario. In the context of Internet advertising, however, through practices such as e-mail spam[129] or advertising overtaking commenting threads on blogs,[130] the electronic equivalent of this scenario is not only plausible, but a well-known phenomenon. While it remains an open question whether such activity is *deserving* of criminal punishment,[131] certainly the threat of imprisonment will give pause to at least some actors who otherwise may consider themselves judgment proof.

Finally, consider the case of use restrictions on a website. In the physical world, homeowners may allow certain persons limited access to their property for limited purposes at limited times (e.g., a cleaning service may be permitted to enter their homes on Friday afternoons to clean, but may neither enter on Thursdays nor enter with the purpose of observing and taking pictures of private areas of the homes while cleaning). If the cleaning service violates these permissions, for example by entering on a Thursday, it may in fact be violating the applicable criminal trespass statute.[132] As computer and information systems grow increasingly complex through the advent of social media and portable Internet-enabled devices, the degree to which system operators *will* have the organizational capacity to (assuming it is even computationally possible to) implement all the code-based restrictions necessary to effect the virtual-world equivalents of these types of restrictions diminishes. Similar physical-world analogies apply for the degree to which a patient, prior to surgery, consents to the surgeon "assaulting" her person, or to which a homeowner permits a landscape decorator to make modifications of a certain sort to the property.

In summary, this Part asserts that in the current ecosystem of cybersecurity vulnerabilities, and considering the typology of potential cybercriminals proposed from the background presented in Part II, private law simply is an insufficient deterrent. It fails sufficiently to deter the types of harmful activities Congress sought to prevent when originally considering the CFAA, and it will fail to deter the types of harmful activities Congress may not specifically have considered in 1986, but that I suggest are properly the province of the federal criminal law. Together

---

[129] *See* Arthur, *supra* note 94.

[130] *See id.*

[131] The question of whether such activity deserves criminal punishment need not be answered for the purposes of this discussion. Furthermore, as discussed in Part III, my proposed reform leaves the decision whether to criminalize such activities properly where it belongs—in the hands of the legislature(s)—separate from the question of whether terms of service or other private agreements may trigger criminal enforcement as a general rule.

[132] This varies by jurisdiction.

with Part I, this Part argues that activities of this latter type—activities falling into categories 2, 3, and possibly 4 above—are both deserving of criminal punishment and require criminalization to achieve the appropriate level of deterrence.

Additionally, this Part identifies how the scope of activities deserving of punishment includes activities that cannot be fully captured by code-based restrictions. Further, it illuminates how, as discussed in Part I and by other scholars, terms-of-service-based restrictions under current broader CFAA interpretations capture activities surely not intended by Congress to fall under the scope of criminal sanction. In the final Part of this Article, I directly consider existing proposals to address this disjunction between activities deserving of punishment and what broader interpretations of the CFAA contemplate criminalizing, detail how those proposals manifest the problems described above, and propose an alternative revision to the CFAA.

III. CRIMINALIZING (ONLY) HACKING: MENS REA AS A SOLUTION

Parts I and II of this Article present a backdrop of socially undesirable activity in the context of computers and the modern Internet. They discuss the shortcomings of the current state of the CFAA, concurring with existing scholarship arguing that it is overbroad in the activity it potentially criminalizes. This background suggests, however, that notwithstanding the risks of overbreadth, there still exist harms against which Congress ought (and to at least some extent, clearly did intend)[133] to protect. Further, the activities leading to many of these harms cannot be proscribed and adequately deterred without the ability of computing system operators to define the boundaries of authorized access—the boundaries of their "private property"—in terms-of-service and similar agreements limiting the purposes for which they allow entrants onto their property.

This Part proceeds first by examining two existing proposals, Professor Kerr's code-based restriction test and Representative Lofgren's proposed express ban on private agreements defining authorized access, in the context of the activities and resulting harms outlined in Parts I and II. It identifies how each of these proposals falls short of the desired protection according to the reasoning described above. It then concludes by proposing an alternative solution—refinement of the mens rea element of the CFAA. This is a proposal both consistent with the 1986 congressional hearings and

[133] Specifically, this includes at least those types of activities in category 4 of the typology presented in Part II that clearly involve interference with or disruption of computing and information systems, but do so without violating any level of authorized access except for the terms of service or other private agreements of those systems.

with the protections against overbroad prosecution and socially undesirable activity outlined in this Article.

A. KERR'S CODE-BASED RESTRICTION TEST

As discussed above,[134] Professor Kerr proposed in a 2003 article a test for interpretation of the scope of access and authorization based on the concept of circumventing code-based restrictions, or aspects of how "the [computer] owner or her agent codes the computer's software so that the particular user has a limited set of privileges on the computer."[135] Specifically, Professor Kerr proposes that courts interpret the term "access" to be subject to the terms of private agreements governing use, but that the term "(without) authorization" be limited to circumvention of these code-based restrictions.[136] Professor Kerr's proposed test has merit in that it would substantially address the problem of potentially overbroad prosecution under computer-misuse statutes. The test fails, however, in that it cannot even address all the types of computer misuse Congress originally contemplated in the legislative hearings surrounding adoption of the CFAA, let alone new forms of computer misuse against which I argue the criminal law should (continue to) protect.

As discussed above in Part II.B, I suggest practical, theoretical, and normative concerns with a code-based restriction test. I identify practical concerns primarily relating to cost and availability of requisite skill required to implement the desired code-based restrictions. One might respond to this concern by arguing that it is not the government's role to design criminal law to solve business problems at the expense of potentially overbroad prosecution. For the sake of argument, assume this response is satisfactory. The code-based restriction test still fails to address the theoretical concerns I present above. Simply restated, not every access restriction that a computer system operator may validly wish to implement *can* be implemented in code.[137] Some restrictions involve nondeterministic problems, such as the identification of criminally harassing and/or threatening speech, which cannot reliably be implemented in a computer program. This concept is well recognized in cybersecurity and data-protection regulation where, for example, protective measures required of regulated entities are divided into "administrative, technical, and physical" measures.[138]

---

[134] *See supra* Part II.B.1.

[135] Kerr, *supra* note 11, at 1644.

[136] *Id.* at 1643.

[137] *See supra* note 88 and accompanying text.

[138] *See supra* note 88 and accompanying text.

Additionally, as noted in Part II.B above, I assert that normative concerns mitigate against limiting the types of restrictions a computer system operator may put in place to those that can be implemented in code. Such a proposition would be analogous to limiting the protections of criminal (physical) trespass only to those security measures that can physically prevent a person from entering onto property. The law of criminal trespass does not require landowners to erect impenetrable walls around their property; nor should the law of computer misuse and electronic trespass. To do otherwise would strip the protections of computer-misuse statutes such as the CFAA and create an "open season" for enterprising hackers,[139] spammers, cyberbullies, and others with malicious intent.

B. REPRESENTATIVE ZOE LOFGREN'S PROPOSED REFORM

On January 15, 2013, in partial response to the events surrounding the suicide of noted Internet entrepreneur Aaron Swartz,[140] Representative Zoe Lofgren prepared draft legislation (colloquially known as Aaron's Law)[141] proposing expressly to preclude determination of unauthorized access under the CFAA based on "violation of an agreement . . . or contractual

---

[139] Consider again the example of the DDoS attack, discussed above in Part II.B.4. No code-based circumvention *of the target system* occurs when a DDoS attack is executed—the attacking computers only access publicly available webpages without violating any code-based restrictions. The net result, however, is to disable and render unusable the target system, a condition clearly contemplated by Congress as impermissible in § 1030(a)(5)(A) of the CFAA. A DDoS attack precisely is the "knowing[] . . . transmission of a program, information, code, or command" that "intentionally causes damage." 18 U.S.C. § 1030(a)(5)(A) (2006). The only missing element here, under a code-based restriction test, is that the website operator has no effective means to implement code, making the DDoS attack "without authorization" because there presently do not exist any viable technical defenses against a properly executed DDoS attack. A code-based restriction test thus effectively grants authorization to attackers to disable at will any website they choose. Surely this cannot be Congress's intent; Representative William J. Hughes described "subsection 1030(a)(5) [as] a malicious mischief provision, . . . designed to provide penalties for those who intentionally damage or destroy computerized data belonging to another." 132 CONG. REC. 9160 (1986). Rendering data inaccessible and/or disrupting a business's ability to transact electronically with its customers is an effective means of damaging the data. Indeed, Representative Hughes specifically stated that the sponsors of the CFAA agreed that "the concept of 'loss' embodied in this [provision] will not be limited solely to the cost of actual repairs," but would also include "the cost of lost computer time." 132 CONG. REC. 7817 (1986). Representative Hughes's statement suggests at least that such disruption may constitute the basis for the offense.

[140] *See supra* note 12.

[141] Hayley Tsukayama, *Demand Progress Calls for Change to Computer Hacking Law #thecircuit*, POST TECH (Jan. 17, 2013, 2:38 PM), http://www.washingtonpost.com/blogs/post-tech/post/demand-progress-calls-for-change-to-computer-hacking-law-thecircuit/2013/01/17/4cde44d8-60d2-11e2-9940-6fc488f3fecd_blog.html.

provision."[142] Representative Lofgren's proposal, while laudable for its attempt to address the problems of overbroad prosecution under the CFAA, fails to provide a workable solution for precisely the same reasons discussed above with respect to Professor Kerr's code-based restriction test. Aaron's Law as revised adopts the code-based restriction test. Leading cybersecurity technical professionals and attorneys echoed concerns similar to those presented here shortly after Representative Lofgren announced her proposed reform, which, even in its original form, effectively adopted the code-based restriction test.[143]

C. MENS REA REFORM: A RESPONSIVE RETURN TO CONGRESSIONAL INTENT

With what, then, are we left to balance the risks of overbroad prosecution and the damage caused by aggressive, modern cybercriminals? As discussed above in Part I.A, the CFAA's congressional sponsors discussed in 1986 changes heightening the mens rea requirement in the statute to avoid criminalizing accidental or unintentional unauthorized access. Unfortunately, as discussed later in Part I, the courts have interpreted the CFAA's mens rea element to be nearly tautological. In summary, it fails to separate the intent to commit the act that constitutes or results in unauthorized access from the intent actually to disregard authorization or access restrictions.[144] I propose resolving the challenges posed here through legislative reform of the mens rea element, revising it to ensure this separation and appending an additional requirement designed to protect against future unpredictable and overbroad prosecution as computing and information systems increasingly integrate into our lives and persons.

The result is a two-part mens rea test with respect to whether the acts in question constitute unauthorized access. The first part requires not only that the access in question be in violation of a technical or other provisional access restriction, but also that the actor's intent be specifically that her actions would violate the given restriction. A key element of this test is that

---

[142] H.R. 18, 113th Cong. (2013), *available at* http://www.lofgren.house.gov/images/stories/pdf/aarons%20law%20revised%20draft%20013013.pdf.

[143] Taylor Armerding, *'Aaron's Law' Could Have Unintended Consequences*, CSO SECURITY AND RISK (Jan. 18, 2013), http://www.csoonline.com/article/727023/-aaron-s-law-could-have-unintended-consequences.

[144] By way of analogy to physical-world crimes, the CFAA fails to separate the intent (generally) to swing one's arm from the intent that by swinging one's arm, one will connect with the face of another person in a manner designed to cause injury to that person. The first generally will fail to satisfy mens rea requirements for intentional assault consummated by battery, whereas the latter will satisfy those requirements.

the actor must be on actual notice of the restriction. While there is no clear bright line as to what constitutes proper notice and what does not, certainly a term buried in the middle of a paragraph in a 25,000-word document should not reasonably constitute actual notice.[145] Congress may look to the work of scientists and scholars in the privacy community, which has made substantial progress over the past several years in developing proposals for providing notice of key terms in privacy policies.[146] My proposal does not speak to whether other provisions not noticed so prominently may still have binding effect in civil matters; it addresses under what circumstances criminal prosecution may advance under the CFAA where unauthorized access is conditioned on an agreement term as opposed to circumvention of a code-based restriction.

The second part of my proposed reform requires that the act in question be in furtherance of one of a specifically prohibited list of actions, which Congress may update from time to time[147] or in furtherance of an act otherwise criminalized under state or federal law. The concept of a specifically prohibited list allows Congress the flexibility to make policy decisions and criminalize acts it deems appropriate from categories 3 and 4 of the typology presented in Part II.B. Thus for matters unique to the computer-crimes space, Congress may create criminal liability as necessary. I note that this is to some extent compatible with Professor Kerr's suggestion of "replac[ing] one-size-fits-all unauthorized access statutes with new statutes that explicitly prohibit particular types of computer misuse."[148] The alternative attachment to existing criminal law allows the CFAA still to afford protection for acts the law already finds impermissible, but which may be more easily accomplished or their effects aggravated by the use of computers and the Internet (category 2 of the typology presented above). It

---

[145] Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 540, 543 (2008); *see also An Interview with David Vladeck of the F.T.C.*, N.Y. TIMES MEDIA DECODER (Aug. 5, 2009, 2:24 PM), http://mediadecoder.blogs.nytimes.com/2009/08/05/an-interview-with-david-vladeck-of-the-ftc/.

[146] *See supra* note 15.

[147] In practice, the state of cybercrime likely would advance more quickly than a legislature could respond, and such a task may ultimately fall to an administrative agency. It is a separate, if interesting, question outside the scope of this Article as to whether delegation of determinations as to *what* constitutes a crime can survive scrutiny under the *Mistretta v. United States* nondelegation doctrine test. *See Mistretta*, 488 U.S. 361, 372 (1989) (permitting Congress to allow the U.S. Sentencing Commission to determine the recommended ranges of sentences established in the Sentencing Guidelines and holding that Congress need only "'lay down by legislative act an intelligible principle to which the person or body authorized to [exercise the delegated authority] is directed to conform'") (quoting J.W. Hampton, Jr., & Co. v. United States, 276 U.S. 394, 409 (1928)).

[148] Kerr, *supra* note 11, at 1643.

also allows Congress the flexibility to criminalize only those code-based circumventions that are in furtherance of some otherwise-unlawful act (which would be captured under this attachment to existing criminal law), or all (intentional) circumventions of code-based restrictions regardless of purpose (by adding that provision to the specifically prohibited actions list).

The result is a CFAA under which each of the following scenarios would result in criminal liability: the attacker trying to damage computer systems, whether by code-based circumvention or other method; the malicious insider attempting to defraud the customers of their employer bank; the cyberbully attempting to harass and intimidate his victim by publicly disseminating a video of her physical abuse in the hopes it "goes viral"; and the ex-employee using his or her not-yet-revoked access credentials to steal valuable trade secrets for sale to a competitor. Each of these acts is either on the specifically prohibited list or in furtherance of some activity otherwise criminalized by state or federal law. In each case, the perpetrator's actions are reprehensible, deserving of criminal punishment, and worthy of deterrence by the threat of criminal sanction.

Contrast these results with those of the elderly gentleman who misrepresents himself as tall, dark, and handsome (when he, in fact, does not quite meet these characteristics) and the teenager at college who shares her Facebook password with her mother, whose acts are neither on the specifically prohibited list nor in furtherance of some otherwise criminal act. Neither of these acts, nor the many others discussed by the courts,[149] constitutes such reprehensible conduct. And accordingly, under this revised mens rea test, such acts would not trigger liability for unauthorized access.

IV. CONCLUSION

Criminal deterrence of computer misuse presents a challenging problem because it introduces two new concepts, both of which must be addressed in a rapidly developing environment, the basic assumptions of which may change far more quickly than legislatures can act. The first are new, computer-specific crimes that did not exist before the introduction of this technology or that are directed toward interference with the technology itself. The second are existing actions, which may or may not already be criminalized, but which are made so much easier by the (mis)use of computers and the impact on victims potentially so amplified by that misuse that this misuse is itself worthy of punishment under and requires the deterrent force of the criminal law.

---

[149] United States v. Nosal, 676 F.3d 854, 861–62 (9th Cir. 2012) (en banc); *see also* Lee v. PMSI, Inc., No. 8:10-cv-2904-T-23TBM, 2011 WL 1742028, at *1–3 (M.D. Fla. May 6, 2011).

In such circumstances, it is difficult—if at all possible—to predict a priori the ways in which criminals will attempt to misuse computers and the Internet. Rather than relying on definitional distinctions for concepts like authorization and the scope of proper use, this Article suggests returning the focus to the intent behind the actions. Intent requirements can be crafted before legislatures know of the instances or even potential types of misuse that the law seeks to deter and punish through criminal sanctions. This Article proposes one such reform to the CFAA as a means of resolving the tension between risk of overbroad prosecution and the need to afford private property owners some protection against virtual trespassers.