

# CYBERCRIMES & MISDEMEANORS: A REEVALUATION OF THE COMPUTER FRAUD AND ABUSE ACT

By Reid Skibell<sup>†</sup>

## ABSTRACT

This Article contends that the Computer Fraud and Abuse Act is an overly punitive and largely ineffective approach to combating computer crime based on two fundamental critiques. The 1986 version of the CFAA contemplated a core distinction between harmless trespass and more substantial intrusions. Over time, this distinction has become obscured and is resulting in over-criminalization of offenders. Furthermore, the increased penalties for computer crime created by the USA PATRIOT Act, and the Cyber Security Enhancement Act, are unjust in application and ineffectual in deterring prospective computer criminals.

## I. INTRODUCTION

When considering the nature and evolution of federal computer crime legislation, it is telling that the passage of the principal law for combating computer crime, the Computer Fraud and Abuse Act (“CFAA”),<sup>1</sup> was based in part on a fear derived from the movie *WarGames*,<sup>2</sup> which had been released the prior year.<sup>3</sup> That such a mundane movie could be the genesis of the U.S. computer crime laws is indicative of how, historically, there has been little connection between public policy and reality in this

---

© 2003 Reid Skibell

<sup>†</sup> Reid Skibell is a J.D. Candidate at Columbia Law School, and has an M.Sc. in Information Systems from the London School of Economics. He has worked extensively in the technology industry, in both the United States and Europe. The author would like to specially thank Tugba Colpan and Andrea Skibell for their help in editing early drafts of the article, and John Dunagan for his assistance with technical computer security issues.

1. Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2000).
2. *WARGAMES* (MGM/UA Studios 1983).
3. See Richard C. Hollinger & Lonn Lanza-Kaduce, *The Process of Criminalization: The Case of Computer Crime Laws*, 26 *CRIMINOLOGY* 101, 106-07 (1988) (explaining that surveys showed computer crime barely registered as a public concern prior to the movie but was found to be a serious one in its wake); Joseph M. Olivenbaum, *Rethinking Federal Computer Crime Legislation*, 27 *SETON HALL L. REV.* 574, 596 (1997) (noting the importance the movie played in the original debates on the CFAA).

area of the law.<sup>4</sup> What makes this tendency so problematic is that policy-makers evince little concern for the practical effects that have resulted from strengthening the CFAA due to the high degree of consensus in the political community. The legislative history of the 1986 amendments to the CFAA, its first major reworking, contains detailed discussions on the proper limits to criminal liability and the appropriate role of government. The record reflects the careful planning, extensive debate, and compromises that went into crafting these revisions.<sup>5</sup> In this sense, the 1986 amendments are emblematic of a cautious approach to computer crime which seeks to flesh out the complexities of the issue. In contrast, the 2002 hearings on the Cyber Security Enhancement Act,<sup>6</sup> the most recent addition to the CFAA, read like an exercise in unanimity, demonstrating near universal agreement that computer crime is a significant and growing problem whose solution lies in aggressive criminal sanctions.<sup>7</sup> The degree of consensus was so pronounced that there was little, if any, debate on the proposed changes; and even traditional defenders of civil liberties like the Center for Democracy and Technology found few concerns over which to voice protest.<sup>8</sup> Congress has sought to strengthen the CFAA with every revision since 1986 by creating new crimes, lowering the required level of intent, and increasing the penalties. The consistency of this strengthening process prompted one court to conclude that in interpreting the Act where there is ambiguity, Congress's intent should be presumed to enlarge the scope of the CFAA's reach.<sup>9</sup>

The CFAA is the cornerstone of the federal government's strategy for combating computer crime, and the punitive mindset upon which it is

---

4. For a full description of the progression of the social conception of the computer criminal, and how far removed it has become from what the available evidence suggests is the true nature of the computer criminal, see Reid Skibell, *The Myth of the Computer Hacker*, 5.3 INFO., COMM. & SOC'Y 336 (2002).

5. See S. REP. NO. 99-432, at 5-14 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2482-92.

6. Homeland Security Act of 2002, H.R. 5710, 107th Cong. § 225 (2002) (Section 225 is known as the Cyber Security Enhancement Act of 2002).

7. See *Cyber-Security Enhancement Act of 2001: Hearing on H.R. 3482 Before the Subcomm. on Crime, House Comm. on the Judiciary*, 107th Cong. 17-19 (2002) [hereinafter *Hearing on H.R. 3482*] (statement of Alan Davidson, Staff Counsel, Ctr. for Democracy & Tech.), available at <http://www.house.gov/judiciary/davidson021202.htm>. The Center for Democracy and Technology ("CDT") was the lone opposition voice at the hearing and their only criticism had to do with the Internet Service Provider provisions of the law, not ones concerning cybercrime.

8. *Id.*

9. See *United States v. Middleton*, 231 F.3d 1207, 1212 (9th Cir. 2002) ("Congress has consciously broadened the statute consistently since its original enactment.").

based is embedded within it and likely indicative of its future direction. The speed of technological change and the complexity of the new information economy demand a sophisticated treatment, but the appreciation of this complexity that was present in the 1986 amendments has been lost. This Article challenges this dominant computer crime paradigm, arguing that the current version of the CFAA is deeply flawed in how it categorizes and penalizes computer crime. Essentially, the original distinction between harmless computer trespass and felonious computer crime has been obscured, resulting in a misguided and ineffective computer crime policy. Part II traces the development of the CFAA, showing how the Act has evolved and explaining the rationale behind the many changes. Part III examines the world of the computer criminal, detailing the poor fit between the CFAA and the proper object of the legislation. Parts IV and V raise two primary objections to the Act's current structure and argue that this structure results in over-criminalization. Part VI analyzes the changes made to the penalty structure by the USA Patriot Act ("USAPA")<sup>10</sup> and the Cyber-Security Enhancement Act and argues that the proper ends of the criminal justice system are not furthered by excessively harsh sanctions for computer crime. Finally, Part VII concludes that a return to a more balanced approach, as embodied by the 1986 version of the CFAA, is necessary to create a more just and effective national computer crime policy.

## II. THE EVOLUTION OF THE COMPUTER FRAUD AND ABUSE ACT

In 1984, Congress hastily drafted and passed the CFAA. At the time, the Act was widely criticized as being overly vague and too narrow in scope.<sup>11</sup> In light of these deficiencies, Congress undertook a more careful study of computer crime and completely revised the Act in 1986.<sup>12</sup> Since then, the CFAA has been amended eight more times during its relatively short lifespan. An appreciation of the Act's history is necessary to understand the problems with the current version. Rather than attempt to detail the extensive number of small changes that have been made, this Article focuses on those that have proven most important in practice.

---

10. United and Strengthening America by Providing Appropriate Tools by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 [hereinafter USAPA].

11. See Dodd S. Griffith, Note, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453, 466-67 (1990) (noting the widespread dissatisfaction with the original 1984 Act).

12. *Id.* at 474-82.

In devising the structure of the 1986 Act, a key Congressional concern was differentiating between computer trespass and more damaging types of computer crime.<sup>13</sup> Part of the rationale for this distinction was a belief that the law's focus should be on combating computer abuses that would either result in significant economic harm or threaten the integrity of sensitive data. There was also a generalized concern about over-prosecution and Congress felt that the division between computer trespass and felonious computer crime would be an effective means to curb excessive use of the Act.<sup>14</sup> One example of how Congress attempted to build this understanding into the CFAA is the addition of the trespass provision found in subsection (a)(3). By creating subsection (a)(3), Congress criminalized all unauthorized access to federal computers but decided it would be improper to classify such access as more than a misdemeanor.<sup>15</sup> It also limited the definition of trespass to attacks by outsiders, even though such a limitation would create a gap in the reach of the Act.<sup>16</sup> Congress viewed the creation of the trespass offense as a compromise that provided "the best means of balancing the legitimate need to protect the Government's computers against the need to prevent unwarranted prosecutions of Federal employees and others authorized to use Federal computers."<sup>17</sup> In this manner, Congress sought to send the message that illegally accessing a federal computer is a crime, but limited the penalty to a level that properly reflected the insubstantial nature of the offense.

---

13. S. REP. NO. 99-432, at 9 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2487.

14. This distinction is emphasized in a number of places within the legislative history. For example, in discussing the intent requirement of subsection (a)(4) it was noted that, "The Committee remains convinced that there must be a clear distinction between computer theft, punishable as a felony, and computer trespass, punishable in the first instance as a misdemeanor." *Id.* at 10, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2488. It also makes the distinction when explaining that consuming time on a system does not qualify as having defrauded the system's owner of anything: "[I]t is important to distinguish clearly between acts of fraud under (a)(4), punishable as felonies, and acts of simple trespass, punishable in the first instance as misdemeanors." *Id.* Similar wording is also used to describe why merely obtaining knowledge of how to break into a system is also not a fraud. *Id.*

15. *Id.* at 10-11, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2488.

16. An outsider is anyone who intrudes on a computer from outside the organization, as opposed to an insider who exceeds their authorized access by viewing sensitive data or entering into a restricted computer. The CFAA in 1986 only covered "federal interest computers," and the insider-outsider distinction was based on whether or not the attacker worked for the government. Consequently, the Act would not apply in the rare case of an intradepartmental trespass. *See id.* at 8, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2486.

17. *Id.*

The 1986 amendments also enlarged the scope of the CFAA by creating three new felony offenses: computer fraud, trafficking in network passwords, and hacking.<sup>18</sup> Subsection (a)(4) created a federal computer fraud offense, but Congress distinguished computer fraud from mail and wire fraud by mandating that using a computer was a requirement for criminal liability.<sup>19</sup> The fraud subsection also contained a computer use exemption, which stipulated that the value of computer time used by the hacker while inside the foreign system was not to be treated as a fraud. Congress was concerned that a simple trespass might be turned into felony fraud based on the economic value of the computer time.<sup>20</sup> Congress also created a second new offense, subsection (a)(6),<sup>21</sup> making it a crime to traffic in network passwords.<sup>22</sup> The most important addition was the creation of a hacking offense, subsection (a)(5), intended to penalize those who damaged or altered the data of another. All three of the new offenses required damages exceeding \$1,000 to become a felony, unless a violation of subsection (a)(5) involved the alteration of medical records.<sup>23</sup> These three new offenses included a mens rea of “intentionally,” a higher requirement than the level of “knowingly” which was used throughout the 1984 version of the CFAA.<sup>24</sup> The intent threshold was also raised in other parts of the Act; the rationale was that those who might mistakenly access a protected computer or stumble upon another’s data protection should be exempted from liability.<sup>25</sup>

The Act was modified in minor ways in 1988, 1989, and 1990 to clarify certain terms. The next significant change came in 1994. Subsection (a)(5) was rewritten to create two new offenses. The first offense covered intentional acts, which remained a felony, and the second created a misdemeanor crime for merely reckless acts. This misdemeanor crime was a departure from the 1986 Act, which did not criminalize unintentional damage caused while accessing a system.

---

18. *Id.* at 9, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2487.

19. *See id.* (“The Committee does not believe that a scheme or artifice to defraud should fall under the ambit of subsection (a)(4) merely because the offender signed onto a computer at some point near to the commission or execution of the fraud.”).

20. *See id.* at 10, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2487 (“[The trespass/felony distinction] would be wiped out were the Committee to treat every trespass as an attempt to defraud a service provider of computer time.”).

21. 18 U.S.C. § 1030(a)(6).

22. S. REP. NO. 99-432, at 13, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2490-91.

23. *Id.* at 12, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2490.

24. *See id.* at 10, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2488.

25. *See id.* at 5-6, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2483-84

There were some practical problems prosecuting cases under the CFAA during the first ten years of the Act's existence. During this time, a generalized concern about the growing seriousness of computer crime was also forming.<sup>26</sup> Consequently, the CFAA was fully revised in 1996, establishing the law's current structure. The compromises that had been written into earlier versions of the CFAA were largely abandoned in favor of a broad expansion of the Act. For example, the subsection (a)(3) federal computer trespass provision was expanded to apply to government insiders as well as outsiders and the computer use exception was deleted from the (a)(4) fraud subsection.<sup>27</sup> These earlier compromises had not proven to be a significant handicap to prosecutors,<sup>28</sup> thus the compromises' elimination without a specified need is illustrative of just how thoroughly the Act was altered in 1996.

Another type of change involved "loopholes" that prosecutors had identified as potentially problematic.<sup>29</sup> Congress's approach to fixing these possible holes marked a sharp departure from its handling of the 1986 amendments. Instead of balancing the state's interest against the threat of over-criminalization as was done in 1986, Congress used wording that expanded the scope of the Act as far as possible. For example, Congress found that a definition of "damage" was necessary because the 1994 amendments were written to require both "damage" and "loss," and there was a concern that in some cases there might be evidence of financial losses but not sufficient permanent damages to fall under the Act.<sup>30</sup> Con-

---

26. See Haeji Hong, Note, *Hacking Through the Computer Fraud and Abuse Act*, 31 U.C. DAVIS L. REV. 283, 290 (1997) (explaining that expanding the scope of the Act was the major impetus for the manifold changes made).

27. Computer Crime & Intell. Prop. Section, U.S. Dep't Justice, *Legislative Analysis of the 1996 National Information Infrastructure Protection Act*, at [http://www.usdoj.gov/criminal/cybercrime/1030\\_anal.html](http://www.usdoj.gov/criminal/cybercrime/1030_anal.html) (last modified June 10, 1998) [hereinafter CCIPS, *Legislative Analysis*].

28. Evidence for this comes from the fact that none of the cases listed as being pursued by the DOJ include "computer use" as the basis for the crime. See Computer Crime & Intell. Prop. Section, *Computer Intrusion Cases*, at <http://www.cybercrime.gov/cccases.html> (last modified July 8, 2003) [hereinafter CCIPS, *Computer Intrusion Cases*]. Also, the DOJ admits that the change to section (a)(3) was not really necessary. See CCIPS, *Legislative Analysis*, *supra* note 27 ("While this defense would almost have negated the law and thus defied a common-sense interpretation of the former law, Congress added the word 'non-public' to make it perfectly clear that a person who has no authority to access any non-public computer of a department or agency may be convicted under (a)(3) even though permitted to access publicly available computers.").

29. See CCIPS, *Legislative Analysis*, *supra* note 27 (arguing for the need to amend the CFAA).

30. See *id.*

gress defined “damage” in two ways. First, damage included any impairment to a system. Second, damage could be any harm which the Act prohibited.<sup>31</sup> Congress intentionally refrained from making a list of prohibited actions to avoid being under-inclusive.<sup>32</sup> Congress intended any ambiguities in drafting to be interpreted in favor of prosecutors.

The 1996 amendments also completely restructured subsection (a)(5), creating three offenses: two felonies and one misdemeanor. Congress changed the Act to cover a wide range of crimes and thus applied a different mens rea to each offense.<sup>33</sup> The first felony, codified in subsection (a)(5)(A), covered anyone who intentionally damages a computer by knowingly transmitting a harmful program. This subsection contained the highest mens rea of the three newly created offenses and is the only one that applies equally to insiders or outsiders.<sup>34</sup> The second felony subsection applies to those who intentionally access a computer without authorization and recklessly cause damage.<sup>35</sup> Determining that the culpability of criminal trespass was sufficient to make reckless damage a felony, Congress purposely lowered the mens rea for external attacks.<sup>36</sup> Finally, the third subsection imposes a misdemeanor penalty on intentionally accessing a computer without authorization and negligently causing damage.<sup>37</sup>

---

31. *Id.* (“In addition, Congress has listed two new threshold harms in its definition of ‘damage’: causing physical injury to any person [18 U.S.C. § 1030(e)(8)(c)] and threatening the public health or safety [18 U.S.C. § 1030(e)(8)(c)].”). It should be noted that the definition of “damage” as “threatening the public health or safety” was codified at 18 U.S.C. § 1030(e)(8)(d).

32. *See id.* (“The statutory language avoids listing specific acts that can cause such impairment to insure that its coverage is suitably broad.”).

33. *See* ORRIN HATCH, THE NATIONAL INFORMATION INFRASTRUCTURE PROTECTION ACT OF 1995, S. REP. NO. 104-357, at 11 (1996) (outlining the restructuring of § 1030(a)(5)), available at <ftp://ftp.loc.gov/pub/thomas/cp104/sr357.txt>.

34. *See id.* at 2; *see also id.* at 11 (explaining that § 1030(a)(5)(A) applies to insiders and outsiders).

35. *See id.* at 10 (“Subsection 1030(a)(5)(B) would penalize, with a fine and up to 5 years’ [sic] imprisonment, anyone who intentionally accesses a protected computer without authorization and, as a result of that trespass, recklessly causes damage.”).

36. *See id.* at 11 (“[I]t is equally clear that anyone who knowingly invades a system without authority and causes significant loss to the victim should be punished as well, even when the damage caused is not intentional.”).

37. *See id.* at 11-12 (“Finally, subsection 1030(a)(5)(C) would impose a misdemeanor penalty, of a fine and up to 1 year imprisonment, for intentionally accessing a protected computer without authorization and, as a result of that trespass, causing damage. This would cover outside hackers into a computer who negligently or accidentally cause damage.”).

The only limitation provided to counterbalance the expansion of the Act was raising the jurisdictional damage level from \$1,000 to \$5,000.<sup>38</sup> This monetary threshold is the only difference between a felony offense and a misdemeanor for an external attacker who recklessly or intentionally causes damage. The \$5,000 floor can also be waived upon proof of physical injury to any person or if public safety is threatened.<sup>39</sup> This change has not proven to be significant to prosecutions under the CFAA.<sup>40</sup>

In the wake of the 9/11 tragedy, Congress passed the USAPA<sup>41</sup> which contains provisions directed at combating the threat of cyberterrorism. These provisions changed the CFAA by making it easier to charge computer criminals with a felony. First, Congress mandated that \$5,000 in damage did not have to be shown if the computers attacked were used for national security or criminal justice.<sup>42</sup> Congress also changed two sections to make it easier to reach the felony monetary threshold. As the only criminal court to define “loss” under the CFAA, the Ninth Circuit in *United States v. Middleton*<sup>43</sup> adopted a definition that arguably went beyond the 1996 amendments by including the cost of damage assessments and any lost revenue or costs associated with an interruption in service.<sup>44</sup> Congress subsequently endorsed this interpretation of “loss” by codifying it into the new law.<sup>45</sup> The second change involved allowing the damage from a single attack to be aggregated across many computers.<sup>46</sup> Thus, a virus causing only minimal damage to any given infected computer but

---

38. See CCIPS, *Legislative Analysis*, *supra* note 27 (arguing that the increased importance of computers in the economy meant that it was proper to raise the threshold of what constituted significant financial losses).

39. See HATCH, *supra* note 33, at 13-19.

40. This is clear from the DOJ’s list of cases prosecuted under the CFAA. See CCIPS, *Computer Intrusion Cases*, *supra* note 28.

41. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), H.R. 3162, 107th Cong. (2001), available at [http://www.eff.org/Privacy/Surveillance/Terrorism\\_militias/hr3162.pdf](http://www.eff.org/Privacy/Surveillance/Terrorism_militias/hr3162.pdf).

42. See Computer Crime & Intell. Prop. Section, *Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001*, at <http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm> (last updated Nov. 5, 2001) [hereinafter CCIPS, *Field Guidance*].

43. 231 F.3d 1207 (9th Cir. 2000).

44. *Id.* at 1210-11.

45. See CCIPS, *Field Guidance*, *supra* note 42 (arguing that the changes “codify the appropriately broad definition of loss adopted in [*Middleton*]”).

46. *Id.*

contaminating a large number of computers could reach the felony monetary threshold.<sup>47</sup>

The USAPA also raised the penalties for violating the CFAA's felony provisions. The maximum punishment for first-time offenders was raised from five to ten years. In the case of repeat offenders, the maximum punishment was raised from ten to twenty years, and a new provision was inserted that allowed related state convictions to be counted as prior offenses.<sup>48</sup> The newly passed Cyber Security Enhancement Act complements the USAPA in directing the Sentencing Commission to upgrade the seriousness of penalties assessed under the CFAA.<sup>49</sup> The Commission responded to this directive by changing the guidelines in April 2003, guaranteeing that those convicted of computer crimes would face substantially increased penalties.<sup>50</sup>

### III. WHAT EXACTLY IS A "HACKER"?

Part of Congress's rationale in taking a more punitive approach to cybercrime has been that the quality of the threat has changed and the penalties should rise accordingly to meet this new danger. Representative Lamar Smith, Chairman of the House Subcommittee on Crime, effectively conveys this perspective:

America must protect our national security, critical infrastructure, and economy from cyber attacks. Penalties and law enforcement capabilities must be enhanced to prevent and deter such criminal behavior. Until we secure our cyber infrastructure, a few keystrokes and an Internet connection is all one needs to disable the economy or endanger lives. A mouse can be just as dangerous as a bullet or a bomb.<sup>51</sup>

Smith's comments are representative of the change in focus of computer crime laws, particularly after 9/11. Essentially, the CFAA has be-

---

47. *Id.*

48. *Id.*

49. See Computer Crime & Intell. Prop. Section, *Amendments & Redline Showing Changes Resulting from Sections 225 and 896 of the 2002 Homeland Security Act*, at [http://www.usdoj.gov/criminal/cybercrime/homeland\\_225.htm](http://www.usdoj.gov/criminal/cybercrime/homeland_225.htm) (last updated May 19, 2003).

50. See Patricia Manson, *Panel OKs Tougher Federal Sentencing Rules*, CHI. DAILY L. BULL., Apr. 21, 2003, at 1 (giving some examples where the penalties would double under the new guidelines).

51. *Hearing on H.R. 3482, supra* note 7, at 2 (statement of Rep. Lamar Smith, Chairman, Subcomm. on Crime of the House Comm. on the Judiciary).

come narrowly focused on combating a certain type of computer criminal. However, the individuals that fall under the current scope of the CFAA are not limited to malevolent intruders and cyberterrorists. This profound over-simplification of the cybercriminal archetype goes to the heart of this Article's critique.

The computer underground lexicon generally divides computer criminals into three separate types: script-kiddies, hackers, and crackers.<sup>52</sup> The first group carries out the majority of computer intrusions. Script-kiddies employ tools downloaded from the Internet to exploit common security weaknesses. They have limited programming knowledge and commit very basic errors, like trying to execute UNIX commands on machines not running UNIX-compatible operating systems. Consequently, a significant portion of the damage that they cause is unintentional as script-kiddies are prone to making mistakes especially when starting out.<sup>53</sup> Because the programs they use are generally geared toward nuisance crimes like defacing a website rather than to more serious crimes like stealing sensitive data, the amount of damage this first group can do is usually limited. Furthermore, Martin Caminada, whose study of security incidents within Dutch corporations, is noteworthy for the depth of information they were able to solicit from attacked companies, found that properly deployed firewalls helped minimize the damage that these types of attackers could do.<sup>54</sup> However, some of the tools script-kiddies utilize are quite powerful, and it

---

52. To this third group can be added cyberterrorists who have traditionally not been included in discussions of the computer underground. Crackers and cyberterrorists are similar in that they are both motivated by something more than the thrill of breaking into foreign systems. The reason that cyberterrorists are not a part of the traditional lexicon is that their very existence is doubtful. *See infra* note 62 and accompanying text.

The other category of person prosecuted under the computer crime laws are corporate insiders, but their motivations and method of attack make them distinct from the computer criminals analyzed in this paper. A computer may be the means for the commission of their crime, but they should not be understood as computer criminals. *See* Skibell, *supra* note 4, at 353.

53. *See* Richard Barber, *Hackers Profiled—Who Are They and What Are Their Motivations?*, *COMPUTER FRAUD & SEC.*, Feb. 2001, at 14; Editorial, *Hackers, Crackers and Phreakers Oh My!*, *COMPUTER FRAUD & SEC.*, Apr. 1999, at 18 (script-kiddies make very common programming mistakes with regularity); Duncan Graham-Rowe, *Access Granted*, *NEW SCIENTIST*, Aug. 12, 2000, at 42 (“[Script-kiddies have] no idea what they’re doing. They download programs or scripts and hack by pointing and clicking.”).

54. Martin Caminada et al., *Internet Security Incidents: A Survey Within Dutch Organizations*, 17 *COMPUTERS & SEC.* 417, 425-26 (1998); Telephone Interview with Dr. John Dunagan, Microsoft Researcher, Microsoft Corp. (Dec. 28, 2002) (explaining that technology is making it increasingly difficult to illegally access sensitive data); *see also* Wade Roush, *Hackers: Taking a Byte Out of Computer Crime*, *TECH. REV.*, Apr. 1995, at 32 (firewalls and related technology protects sensitive data from external attacks).

would be a mistake to assume they are only capable of minor vandalism. This group is also important because hackers and crackers usually begin as script-kiddies before advancing to the other groups.<sup>55</sup>

The second type of computer intruder is the hacker, distinguished as being more experienced and possessing more programming skills than a script-kiddie. Hackers are able to use the standard tools with a much higher degree of sophistication and some are adept enough to design intrusion programs.<sup>56</sup> The cracker shares the hacker's sophistication, but the difference lies in motivation. For hackers, the desired reward is the hack itself because of the rush involved in breaking into what was thought to be a secure system.<sup>57</sup> There is also a voyeuristic component, as hackers often describe themselves as being drawn to the power of being able to see what is hidden from the general populace.<sup>58</sup> While this motivational distinction between hackers and crackers may appear subtle, it is crucial to understanding that hackers pose a relatively insubstantial criminal threat to companies and institutions.

Though hackers may be skilled, available evidence suggests that they pose a rather limited criminal threat. Paul Taylor's research on the computer underground community found that hackers have little interest in pursuing financial or ideological goals. What motivates them to attack a given target is the opportunity to boast that they have conquered it.<sup>59</sup> Douglas Thomas makes an even stronger argument. He found that the talented hackers who could pose the greatest threat are the ones who also tend to be the most concerned with ethical issues. Thomas argues that, "[skilled hackers] tend instead to be the most strongly motivated by an ethic which values security, which values information, and which puts innovation and learning at the top of their list of priorities."<sup>60</sup> Taylor and

---

55. See Barber, *supra* note 52, at 15.

56. DOUGLAS THOMAS, HACKER CULTURE 43-44 (2002); *id.*

57. PAUL A. TAYLOR, HACKERS: CRIME IN THE DIGITAL SUBLIME 56-58 (1999). Taylor's research is noteworthy for its extensive interviews with computer intruders and the insider perspective he was able to uncover.

58. *Id.*

59. *Id.* at 59-61; see also Tom Mulhall, *Where Have All the Hackers Gone? Part 3—Motivation and Deterrence*, 16 COMPUTERS & SEC. 291, 293-97 (1997); Emmanuel Goldstein, *Q&A with Emmanuel Goldstein of 2600: The Hacker's Quarterly*, CNN INTERACTIVE, Mar. 22, 2002, available at <http://www.cnn.com/TECH/specials/hackers/qandas/goldstein.html> (defining hacking as an "inquisitive" activity); Mark Ward, *Sabotage in Cyberspace*, NEW SCIENTIST, Sept. 14, 1996, at 12 (describing hackers as motivated primarily by curiosity).

60. *Cyber Terrorism and Critical Infrastructure Protection: Hearing Before the Subcom. on Gov't Efficiency, Fin'l Mgmt. and Intergovernmental Relations of the Comm. on Gov't Reform*, 107th Cong. (2002) [hereinafter *Critical Infrastructure Protection*

Thomas have performed the most extensive academic work to date on the computer underground, thus their assessment of the criminal potential of hackers should be given substantial weight. Furthermore, Caminada's empirical research lends support to this view of hackers as benign. They conclude that the majority of computer intruders have no interest in damaging the systems they penetrate. Specifically, they found that, "[n]ot a single responding organization mentions incidents in which the perpetrator has read or modified any truly sensitive data, such as customer files or financial data."<sup>61</sup>

The real danger from computer crime comes from the third category of intruders that includes crackers and cyberterrorists. Crackers include those who attack computer systems for personal profit, such as people carrying out economic espionage, or for malicious purposes, like virus writers. Cyberterrorists are grouped with crackers because they share similarly malevolent purposes, but they still remain a theoretical threat. To date, there is no evidence of any cyberterrorists currently operating. Although much has been written about the threat from this third group, there are good reasons to believe that the threat is overstated, particularly the specter of cyberterrorism.<sup>62</sup> While a full examination of the subject is beyond the scope

---

*Hearing*] (statement of Douglas Thomas), available at <http://www-rcf.usc.edu/~douglast/testimony.pdf>.

61. Caminada, *supra* note 54, at 423; see also TAYLOR, *supra* note 57, at 21-22 (arguing that crackers are a very tiny group existing only on the fringes of the digital underground).

62. I have dealt with this subject at length, arguing that the societal vision of the dangerous computer intruder is not borne out by reality. While the statistics on the surface show an economic threat from crackers, a careful analysis shows the danger is substantially inflated. See Skibell, *supra* note 4, at 347-53. Joshua Green effectively makes a similar case against cyberterrorism. Green concludes that:

There is no such thing as cyberterrorism—no instance of anyone ever having been killed by a terrorist (or anyone else) using a computer. Nor is there compelling evidence that al Qaeda or any other terrorist organization has resorted to computers for any sort of serious destructive activity. What's more, outside of a Tom Clancy novel, computer security specialists believe it is virtually impossible to use the Internet to inflict death on a large scale, and many scoff at the notion that terrorists would bother trying.

Joshua Green, *The Myth of Cyberterrorism*, WASH. MONTHLY, Nov. 2002, at 8, available at <http://www.washingtonmonthly.com/features/2001/0211.green.html>; see also *Critical Infrastructure Protection Hearing* (statement of Douglas Thomas), *supra* note 60, at 5 ("The reality is that there is very little that a well-funded terrorist group could do that a 16-year-old hacker couldn't. And neither of them threatens us in a way that can rightly be called 'terrorism.'"); Scott Berinator, *The Truth About Cyberterrorism*, CIO MAG., Mar. 15, 2002, available at <http://www.cio.com/archive/031502/truth.html> (stating that data

of this Article, an observation made by the respected political scientist Murray Edelman is enlightening. Edelman noted that the public image of small outsider groups is particularly vulnerable to being exploited politically because these groups have no political constituency and the public has little contact with them.<sup>63</sup> The characteristics of the digital criminal community closely correspond to Edelman's criteria. The media portrayal and societal image of the computer criminal have also shifted markedly over the last twenty years.<sup>64</sup> In a short period of time, the public's perception of the computer criminal has gone from harmless, socially awkward nerd to dangerous cyberterrorist, leaving the question as to how much, if any, of this change reflects reality, and how much is a creation of symbolic politics.

The combination of the composition of the computer underground and the Edelman hypothesis suggests that there is a severe mismatch between the mythical computer criminal targeted by the increasingly-strict CFAA changes and actual perpetrators who are at risk of prosecution under the Act. This disparity between the imagined and the real criminal threat has substantial consequences in light of the broad reach of the law's felony provisions. This Article now turns to explaining how the legal distinction between benign trespass and harmful cracking has been virtually written out of the Act, thereby allowing all categories of computer criminals to fall under the harsh penalties of the CFAA.

#### IV. COPYING OF FILES AND THE TROPHY PROBLEM

The first major problem with the CFAA concerns the copying of files by computer hackers. As previously explained, the locus of hacker activity is the thrill of breaking a system's security. This experience regularly includes copying files as a token or trophy of the conquest. Often, there will be no intent on the part of the intruder to sell or otherwise benefit from the copied material and the intrusion will cause no actual damage to the system. This behavior can be analogized to someone breaking into the Louvre and making a perfect digital copy of the Mona Lisa to hang in her bedroom, leaving the physical picture unblemished. Certainly, there is a dif-

---

might be threatened but infrastructure attacks are too difficult); Ward, *supra* note 59 at 12.

63. MURRAY EDELMAN, *THE SYMBOLIC USES OF POLITICS* 1-13 (1964).

64. Skibell, *supra* note 4, at 343-347; *see also* TAYLOR, *supra* note 57, at 7-11; THOMAS, *supra* note 56, at 219; Amanda Chandler, *The Changing Definition and Image of Hackers in Popular Discourse*, 24 INT'L J. SOC. OF LAW 229, 249-50 (1996) (concluding that hacking, which used to attract "sneaky admiration" is now viewed as treacherous).

ference between how society would want to treat such a criminal and how it treats someone that steals the Mona Lisa itself. In terms of utility, stealing the painting deprives another party of valuable property and inflicts a corresponding injury on the community by decreasing the overall incentive to produce works of art. This behavior should be prohibited not only for reasons of individual fairness, but because societal utility is threatened. In contrast, copying the Mona Lisa represents an infringement upon an individual's right to exclude, but the harm to society is far less clear. The harm from copying is of a significantly lesser degree. Copying a painting is closer to the crime of trespass than it is to the crime of fraud or theft. Both types of behavior are worthy of punishment, but it is a mistake to treat them identically.

The trophy issue has proven to be problematic in computer crime prosecutions because the government has had mixed success proving that the victim has been deprived of something valuable. In an early 1990 computer crime prosecution, Craig Neirdorf was accused of causing \$80,000 worth of harm to AT&T by posting an illegally obtained sensitive internal document on his electronic bulletin board. During the trial it was revealed that the same information was publicly available for a mere \$13 to anyone who wrote to AT&T.<sup>65</sup> Neirdorf was acquitted of all charges but, in a more recent case, "notorious" computer hacker Kevin Mitnick was not as fortunate. Mitnick broke into the computers of Sun Microsystems and downloaded the Solaris operating system source code for which Sun ("Sun") had paid \$80 million. He plead guilty so the CFAA's reach was not directly implicated, but he received a harsh punishment under the sentencing guidelines because he was charged with causing damage equal to the value of the software. Mitnick had no intention of altering or selling the code. Indeed, there was no genuine damage done to Sun besides public embarrassment.<sup>66</sup> In fact, Sun never reported any loss to its insurance company, the IRS, or its shareholders, casting further doubt on the validity of the damages figure used to calculate Mitnick's penalty.<sup>67</sup> In an interesting parallel to the Neirdorf case, Sun made the code publicly available for a mere \$100 soon after the break-in.<sup>68</sup> The only place that the \$80 million

---

65. BRUCE STERLING, *THE HACKER CRACKDOWN: LAW AND DISORDER ON THE ELECTRONIC FRONTIER* 276-77 (1993).

66. David Banisair, *Computer Hacker's Sentence Spotlights High-Tech Crime Prosecutions*, CRIM. JUST. WKLY., Aug. 3, 1999, available at <http://packetstorm.icx.fr/mag/hwahaxornews/HWA-hn31.txt> (last visited Aug. 24, 2003).

67. Douglas Thomas, *How Much Damage Did Mitnick Do?*, WIRED, May 5, 1999, <http://www.wired.com/news/politics/0,1283,19488,00.html>.

68. See Lindsey Arent, *Did Sun Inflate Mitnick Damages?*, WIRED, May 22, 1999, <http://www.wired.com/news/politics/0,1283,19820,00.html>.

damages figure ever existed was in the trial record, yet that was sufficient to have severe consequences for Mitnick.

The copying of proprietary data is covered by 18 U.S.C. § 1030(a)(4), the computer fraud provision. This subsection criminalizes accessing a computer without authorization and with the intent to defraud, obtain, or attempt to obtain, anything worth more than \$5,000.<sup>69</sup> This provision was designed to “penalize thefts of property via computer that occur as part of a scheme to defraud.”<sup>70</sup> An example of the type of crime the drafters had in mind is setting up a webpage that mirrors a large e-commerce site for the purpose of acquiring credit card numbers. Fraud is a zero-sum game, with gains to one party coming at the expense of another. Mitnick’s crime does not fit comfortably into this conventional conception of fraud, since he obtained something of substantial value but has not deprived his victim of anything. Consequently, he arguably does not possess the requisite mens rea, or criminal purpose, for the crime of fraud. However, the Supreme Court in *Carpenter v. United States*<sup>71</sup> determined that a fraud can be perpetrated without any monetary damage. The Court ruled that a newspaper, *The Wall Street Journal*, had the exclusive right to determine how its confidential information is disseminated, thus a scheme that would infringe on that property right can be classified as fraud.<sup>72</sup> To the extent that a computer intrusion invariably involves a violation of the victim’s right to exclude, *Carpenter* most likely means that any copying of a trophy will be regarded as fraud.

The originator of the scheme in *Carpenter*, Foster Winans, intended to profit from his employer’s property, even though it was not his purpose to directly harm the newspaper.<sup>73</sup> Winans was able to do this because the information had a value outside of the context of the newspaper; it allowed someone to trade in front of information that would most likely drive up the price of a stock. This reveals a crucial difference between *Carpenter* and the Mitnick case: Mitnick had no intent to personally profit and, indeed, it would have been extremely difficult to realize a gain even if he had tried. The data that Mitnick stole had no value outside of the context

---

69. 18 U.S.C. § 1030 (a)(4).

70. S. REP. NO. 99-432, at 9 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2486-87.

71. 484 U.S. 19 (1987).

72. *Id.* The principal defendant, Foster Winans, an employee of *The Wall Street Journal*, was the author of a widely read column that tended to increase the stock price of companies which he highlighted as good buys. The scheme involved his releasing the names of companies in the column early to stockbrokers who would buy the stocks ahead of the market. They would then sell the stocks and Winans would realize a portion of the profits. *Id.*

73. *Id.* at 23 (noting that the net profits of the scheme amounted to over \$690,000).

of Sun. This is true of most, but not all, types of information that hackers might copy. There is also a distinction with regard to the victims' relationship to the information. In *Carpenter*, the value of *The Wall Street Journal's* property interest was directly related to its exclusivity.<sup>74</sup> If the knowledge contained in the column were widely distributed, then investors who might have otherwise purchased the paper would have no interest in reading about these "hidden gems." In contrast, the fact that Sun started giving away the code for a negligible amount to developers and educational institutions demonstrates that exclusivity did not have the same primary relationship to the information's value.

Some support for these differences comes from the First Circuit's decision in *United States v. Czubinski*,<sup>75</sup> which distinguished *Carpenter* in important ways. The defendant, Richard Czubinski, used his job at the IRS to view confidential taxpayer data, though he never disclosed the data to third parties or made practical use of it.<sup>76</sup> Dismissing the wire fraud and computer fraud violations against Czubinski, the court classified his behavior as "idle curiosity" that broke departmental rules but did not rise to the level of fraud.<sup>77</sup> The court held that fraud requires that "either some articulable harm must befall the holder of the information as a result of the defendant's activities, or some gainful use must be intended by the person accessing the information, whether or not this use is profitable in the economic sense."<sup>78</sup> The logic of the court's reasoning fits the circumstances of the trophy problem, where there is no intention to make use of the copied data. Admittedly, in assessing the computer crime charge, the court attached some weight to the fact that Czubinski never downloaded or printed out any of the data he viewed, but the court made its observation in the context of establishing that Czubinski's purpose was benign. Similar to Czubinski, hackers like Mitnick are primarily guilty of curiosity which, even if it should be punishable, does not deserve to be classified as felonious criminal fraud.

One reason that *Czubinski* has not been helpful to cybercriminals is that the First Circuit's focus on intent has been largely disregarded, as

---

74. *Id.* at 28.

75. 106 F.3d 1069 (1st Cir. 1997).

76. *Id.* at 1072. Czubinski was a member of a white supremacist organization and the government was probably expecting to locate evidence that he used his access to the IRS data to further that cause. *Id.* However, it turned out that Czubinski only abused his position to do things like run credit checks on his girlfriend. *Id.*

77. *Id.* at 1078.

78. *Id.* at 1074.

demonstrated in *United States v. Ivanov*.<sup>79</sup> The court stated that the crucial difference with *Czubinski* was that the defendant, Aleksey Ivanov, was not merely viewing the data but had control over it because he had obtained root access to the system.<sup>80</sup> Root access is a descriptive term meaning that the user is recognized as a system administrator and consequently obtains the authority to change passwords or destroy data—authority that normal users do not have. Root access is used to commit computer crime in many instances, but prior to *Ivanov* it was not regarded as sufficient evidence to ensure a fraud conviction under the CFAA.<sup>81</sup> The defendant in *Czubinski* had similar authorization to copy or destroy the IRS data, thus the court’s decision in *Ivanov* clearly increases the relevance of the intruder’s level of access. However, the case has not been criticized and it is a telling example of how courts are reading *Czubinski* as narrowly predicated on the defendant’s physical relationship to the data.

Another reason that *Czubinski* will not be followed comes from a 1996 change that allows a different part of the CFAA to reach the copying of data. Based on the Tenth Circuit decision in *United States v. Brown*<sup>82</sup> that the interstate theft provision in § 2314 does not include intangible information,<sup>83</sup> Congress expanded § 1030(a)(2) by making it a felony to obtain information involved in interstate communication worth more than \$5,000 or to use such information for financial gain.<sup>84</sup> It is particularly noteworthy

---

79. 175 F. Supp. 2d 367 (D. Conn. 2001).

80. *Id.* at 371-72. Ivanov was a Russian national, and the case was litigated before the CFAA was explicitly expanded extra-territorially. The “under control” theory used by the court is largely for the purposes of getting around this jurisdictional problem, but its interpretation of *Czubinski* is still problematic.

81. Congress seemingly addressed the issue of root access in the 1986 amendments, and the relevant sections of the CFAA have not been changed. The legislative history explains that simply accessing a system is not sufficient to qualify as having “obtained” anything:

In intentionally trespassing into someone else’s computer files, the offender obtains at the very least information as to how to break into that computer system. If that is all he obtains, the offense should properly be treated as a simple trespass. But because the offender has obtained the small bit of information needed to get into the computer system, the danger exists that his and every other computer trespass could be treated as a theft, punishable as a felony under this subsection.

S. REP. NO. 99-432, at 9 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2486-87.

82. 925 F.2d 1301 (10th Cir. 1991).

83. *See* CCIPS, *Legislative Analysis*, *supra* note 27 (the change was based upon the *Brown* decision).

84. *See id.* (“Moreover, consistent with Congress’s prior construction of § 1030(a)(2), ‘obtaining information’ includes merely reading it; i.e., there is no requirement that the information be copied or transported. This is critically important because, in

that Congress chose § 1030(a)(2) as the means to deal with this hole in the law because when this subsection was created in 1986 it was intended only to cover the extraordinary situation where the illegally obtained information was either financial records or confidential government documents.<sup>85</sup> Because of the sensitive nature of financial and governmental information, merely viewing the documents is sufficient to damage the party that owns the data. Consequently, Congress made clear that asportation, or removing the data from its original location, was not required for a conviction.<sup>86</sup> Furthermore, the information that subsection (a)(2) originally covered was of such a private nature that there was no reason to add a monetary threshold to that subdivision, whereas subsection (a)(4) already had one. By expanding (a)(2) instead of changing (a)(4), Congress equated obtaining data with viewing it in many contexts where it made little sense to classify the underlying behavior as a crime of conversion.

## V. MENS REA AND THE \$5,000 THRESHOLD

One of the key changes in the 1996 reformation of the CFAA was the division of the subsection (a)(5) anti-hacking provision into three separate offenses based on intent.<sup>87</sup> This portion of the Act is the one most widely used in criminal prosecutions, but neither Congress nor the courts have grappled with the important question of what distinguishes computer hacking that is merely negligent from that which is reckless. The crime of hacking, which by its very nature involves intentionally breaking security to traipse around a foreign system, would seem to involve an inherent and foreseeable risk of causing accidental damage. The logical distinction between the two may be difficult to establish in practice and the mens rea requirement might not provide sufficient protection against over-criminalization. Some commentators also argue that judges commonly lack detailed technical knowledge and consequently have a tendency to overestimate the abilities of computer hackers.<sup>88</sup> While this finding is far from conclusive and it is unclear how such misconceptions would affect

---

an electronic environment, information can be ‘stolen’ without asportation, and the original usually remains intact.”).

85. S. REP. NO. 99-432, at 6, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2489.

86. *Id.*

87. *See* HATCH, *supra* note 33, at 11.

88. *See* TAYLOR, *supra* note 57, at 2-5 (on the example of Kevin Poulsen and Chris Lamprecht’s skills being overestimated); R.U. Sirius, *Superhacker Kevin Mitnick: Menace to Fear or Rogue to Love?*, VILLAGE VOICE, Feb. 22, 1999, *available at* <http://www.villagevoice.com/issues/0007/sirius.php> (on the example of Kevin Mitnick’s skills being overestimated).

the conduct of a trial or the creation of jury instructions, judges may view even unsophisticated script-kiddies under a stringent “reasonable person” standard thus making recklessness far easier to prove. If the negligence/recklessness distinction does not prevent relatively harmless computer intrusions from becoming felonies then the only safeguard against broad application of the two (a)(5) felony provisions is the monetary requirement. Consequently, proper calculation of damages accrued in the course of a computer intrusion is of central importance in ensuring appropriate punishment under the CFAA.

Since the 2001 USAPA changes, calculation of damages under the Act has been based on the reasoning in *Middleton*, which held that loss under the statute includes anything that was the natural and foreseeable result of the intrusion, as well as the costs to repair and “resecure” the system against future intrusions.<sup>89</sup> This figure includes lost profits. Courts have determined lost profits to include damages for loss of goodwill and reputation.<sup>90</sup> Losses can also be aggregated, meaning that instances of minimal damage to multiple computers can be added together to surpass \$5,000.<sup>91</sup> This expansive definition of damage essentially makes the \$5,000 threshold meaningless. The result is that computer hackers are at the mercy of prosecutors because almost any computer intrusion can be charged as a felony under the CFAA’s anti-hacking provisions.

#### A. The Problem of “Resecuring” Costs

In cases involving destruction of property, cost of repair is a common way for courts to determine whether a jurisdictional threshold has been exceeded. As an example, take *Nichols v. United States*,<sup>92</sup> which involved a common liquor store robbery. In *Nichols* the magnitude of the loss was determined by calculating the cost of fixing the roof and interior door that were physically damaged in the course of entering the establishment.<sup>93</sup> It

---

89. *United States v. Middleton*, 231 F.3d 1207, 1213 (9th Cir. 2000).

90. *See, e.g., Ingenix, Inc. v. LaGalante*, 2002 U.S. Dist LEXIS 5795, at \*26, \*29 (E.D. La. Mar. 28, 2002); *In re America Online, Inc.*, 168 F. Supp. 2d 1359, 1380 (S.D. Fla. 2001); *Compuserve Inc. v. Cyber Promotions*, 962 F. Supp. 1015, 1023 (S.D. Ohio 1997). *But cf. United States v. Pierre-Louis*, 2002 WL 1268396, at \*2 (S.D. Fla. Mar. 22, 2002) (admitting the 2001 Patriot Act changes the law on this point). The *Ingenix* opinion was removed from the Lexis Service at the request of the court on August 25, 2003.

91. 18 U.S.C. § 1030(a)(5)(B)(i).

92. 343 A.2d 336 (D.C. App. 1975).

93. *Id.* at 341-42. *Nichols* was chosen as a representative destruction of property case because of its clear and reasoned approach to how to perform a damage calculation. It has also been somewhat influential, having been cited in other jurisdictions, including Alabama, Idaho, Illinois, and Maryland. *See Cartee v. State*, 390 So. 2d 1121, 1124 (Ala. Crim. App. 1980); *State v. Hughes*, 946 P.2d 1338, 1343 (Idaho Ct. App. 1997); *People*

is fair to assign the blame for this damage to the perpetrators of the crime, since their direct actions caused the damage to the store.

The 1986 amendments used a conception of loss similar to *Nichols*. Loss was based on the costs of actual repairs and on the costs incurred during reprogramming or restoring data to its original condition.<sup>94</sup> Costs of repairing the security hole that the attacker used to penetrate the system would not be covered but expenses related to returning the company to its position prior to the incident would be.<sup>95</sup> The 1986 version of the Act also included reliance damages, such as those incurred by an investor who mistakenly invests in a stock based on information contained in an altered database, in the damage calculation.<sup>96</sup> Since the loss is easy to demonstrate and the harm results directly from the actions of the intruder, this inclusion is not a significant departure from the formula used in the destruction of property example. On the other hand, damages for reputational and customer goodwill losses, recovery for which was added in 1996, are particularly difficult to quantify and partial responsibility may lie with the victim company.<sup>97</sup> However, certain types of computer crime, like website defacement, target a company's reputation. Computers are of central importance to businesses and reputation is an important and fragile asset. Thus, inclusion of these costs might thus be justified as an attempt to specifically deter a particularly damaging and malicious type of computer crime.

What is far more difficult to defend is the inclusion of "resecuring" costs, which are the expenses derived from fixing the security hole that the hacker used to access the system. While Congress has never addressed the

---

v. Carraro, 394 N.E.2d 1194, 1196 (Ill. 1979); *Robinson v. State*, 468 A.2d 328, 323 (Md. 1983).

94. See S. REP. NO. 99-432, at 11 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2488-89.

95. This is based on my reading of the 1986 legislative history. No court has made a determination about whether the 1986 version of the CFAA covers the costs of "resecuring," namely those involved in fixing the security weakness used by the attacker. The closest a court came to a ruling on this issue was in *United States v. Sablan*, where restitution only included costs strictly related to repairing the damaged files. *United States v. Sablan*, 92 F.3d 865, 870 (9th Cir. 1996) ("The consequential expenses incurred due to the meetings with the FBI, the staff meeting, and the handling of the crank calls were not expenses necessary to repair the files damaged by Sablan's criminal conduct. These expenses were thus not properly included in the restitution order.").

96. S. REP. NO. 99-432, at 11, reprinted in 1986 U.S.C.C.A.N. 2479, 2489.

97. This will be explained in greater detail in Part VI.C, but the victim company may have consciously elected to not address known weaknesses and thus might not be justified in claiming that the computer criminal tarnished their reputation for taking security seriously.

rationale behind making the intruder liable for these expenses, the *Middleton* court did. The court reasoned that patching the hole is necessary to make the hacked corporation whole, much like fixing the door and roof for the liquor store owner. This figure should not include improvements to the system, but should only make the system as secure as it was before the attack.<sup>98</sup> The problem with this line of reasoning is that it assumes that a computer intruder does damage when they break into a system when, in reality, all they are doing is exploiting a pre-existing weakness or hole in the security of the system. The company was not more secure before the attack—just because no one had chosen to enter did not mean that the door was not wide open. Consequently, “resecuring” by definition includes an improvement to the system, fixing a weakness that was there long before the intruder exploited it.

The court in *Middleton* also pointed out that the eminent foreseeability of resecuring made it fair to include resecuring costs in the damage assessment.<sup>99</sup> However, it is also predictable that the owner of the liquor store in the *Nichols* case would respond to the physical break-in by reinforcing the interior door, improving the locks, and adding a security system; yet none of this is attributed to the thief. Because the choice of the proper level of security lies with the owner of the store, society does not see fit to blame the thief for these costs. The owner of a store is certainly aware of the possibility of a robbery and his decision on the appropriate level of security is independent of the thief’s actions. Yet in the context of computer crime, the CFAA makes the intruder liable for the corporation’s negligence in haphazardly guarding their own data. Surveys indicate that the majority of companies are aware of the weakness in their own security but choose to ignore the danger.<sup>100</sup> Companies often under-invest in security for financial reasons but there is also widespread carelessness such as when people fail to update software or ignore internal security guidelines.<sup>101</sup> Perhaps there is an argument to be made that the sophisticated hacker should be held liable for resecuring a system, as they may have

---

98. *United States v. Middleton*, 231 F.3d 1207, 1213 (9th Cir. 2000); *see also In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 521 (S.D.N.Y. 2001) (“S. Rep. No. 104-357 seems to make clear that Congress intended the term ‘loss’ to target remedial expenses borne by victims that could not properly be considered direct damage caused by a computer hacker.”); *Shurgard Storage Ctr. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000) (justifying the inclusion of investigation costs).

99. 231 F.3d at 1213.

100. *See, e.g.*, Stephen Hinde, *Security Surveys Spring Crop*, 21 COMPUTERS & SEC. 310, 314 (2002); Richard Power, *2002 CSI/FBI Computer Crime and Security Survey*, 8 COMPUTER SEC. ISSUES & TRENDS, Spring 2002, at 1.

101. Hinde, *supra* note 100, at 314.

used their skills to penetrate a system that was reasonably secure. However, the unfairness of the CFAA is evident in the case of script-kiddies, whose sole ability to break into a system is predicated on using a standardized program to exploit a commonly known security weakness. The CFAA would make them guilty of a felony, or enhance their punishment under the sentencing guidelines, simply because a corporation failed to address serious holes in its own security.

Another reason that resecuring should not be included in damage assessments from hackings is the disjuncture between the locus of the underlying crime and the origin of the costs of resecuring. When network security is found to be compromised, a system administrator will generally respond by trying to trace back how the intruder was able to gain access.<sup>102</sup> When the security weakness is found and neutralized, the administrator's job is not yet complete. A good administrator must check the security of all devices or parts of the network that had a relationship with the part compromised to ensure that those related devices do not possess a similar vulnerability. The theory is that all possible sources of entry must be examined before the system can again be declared secure.<sup>103</sup> Companies are also increasingly collecting evidence to use against the intruder as part of their overall response to an attack.<sup>104</sup> The formation of companies special-

---

102. See Dunagan, *supra* note 54; Jim Yuill et al., *Intrusion-Detection for Incident-Response: Using a Military Battlefield-Intelligence Process*, 34 COMPUTER NETWORKS 671, 671-672 (2000) (explaining the standard response to an intrusion).

103. See Dunagan, *supra* note 54 (stressing that the system must be pronounced free of newly introduced holes, known as "Trojans," before a security incident can be classified as concluded).

104. In *Sablan*, the court specifically rejected inclusion of investigation expenses. *United States v. Sablan*, 92 F.3d 865, 870 (9th Cir. 1996); see *supra* note 95 and accompanying text. However, that was under the 1986 version of the Act. In the recent *LaGalante* case, a former employee who was accused of stealing sensitive data was assigned the cost of hiring a computer forensic specialist who helped collect the evidence used against that former employee. *Ingenix, Inc. v. LaGalante*, 2002 U.S. Dist LEXIS 5795, at \*26-27 (E.D. La. Mar. 28, 2002). This trend is likely to continue as investigations for the purpose of repairing the system, and for the purpose of collecting evidence against the attacker, are merging together in the IS community. This is particularly true in the case of outside specialists, who argue that properly containing the internal damage and public relations dangers from an intrusion involves gathering evidence. The already tenuous distinction between repairing and improving a system is further called into question by this development. See, e.g., Berni Dwan, *Nowhere to Hide*, COMPUTER FRAUD & SEC., Dec. 2002, at 13; Michael Goldberg, *Watching the Detectives: Computer Forensics can Help Companies Uncover the Digital Truth*, CIO MAG., June 1, 2002, available at [http://www.cio.com/archive/060102/et\\_note.html](http://www.cio.com/archive/060102/et_note.html); Cliff May, *Computer Forensics—the Morse or Clouseau Approach?*, COMPUTER FRAUD & SEC., Nov. 2002, at 14; Deniz Si-

izing in computer forensics has accelerated this trend. Such information-gathering activities are not even tangentially related to the attacker's culpability, however these companies contend that the gathering of evidence to be used against the attacker is part of containing the damage of a computer intrusion. Computer hackers are thus being criminally charged based on the cost of their victim's investigations.

What makes blaming hackers for these types of costs so problematic is how expensive they are relative to the felony monetary threshold. Jennifer Granick, a former computer crime defense attorney, contends that a large proportion of the costs calculated under the CFAA are due to work that bears little or no relationship to the actual attack.<sup>105</sup> Though it is a civil case, *EF Cultural Travel v. Explorica, Inc.*<sup>106</sup> is indicative of the type of abuse to which she is referring.<sup>107</sup> No actual harm was done to Explorica but the court still found a violation of the CFAA because of the high cost of diagnostic testing. Specifically, Explorica spent \$20,944.92 to determine if there was any damage and over \$40,000 to resecure their website and network.<sup>108</sup>

## **B. The Problem of Calculating Intangible Harms**

A separate problem involves the reliance on loss estimations from companies that have been hacked. While certain aspects of a company's response to an intrusion are standard, the reality is that the amount of time spent responding can vary widely depending on the capabilities of the IT staff, whether the company utilizes specialized assistance, and the company's general level of experience with security incidents.<sup>109</sup> According to Granick, a company responding to a website defacement might assess anywhere between one to forty hours of repair time.<sup>110</sup> Given this lack of uniformity, it is very difficult for a defendant to contest this portion of a

---

nangin, *Computer Forensic Investigations in a Corporate Environment*, COMPUTER FRAUD & SEC., June 2002, at 11.

105. Telephone Interview with Jennifer Granick, Director, Stanford Law School Center for Internet and Society (Nov. 4, 2002). Because so few criminal computer crime cases ever make it to trial, Granick was invaluable in providing practical information on how these prosecutions are handled.

106. 274 F.3d 577 (1st Cir. 2001).

107. Given the relative paucity of criminal decisions under the CFAA, civil cases provide important evidence of how courts are interpreting its provisions.

108. *Explorica*, 274 F.3d at 584.

109. Companies, particularly those that are smaller or have never previously experienced an attack, generally respond in an ad hoc and disorganized manner. Simone Kaplan, *It's Not Easy Being Breached*, CSO MAG., Dec. 2002, <http://www.csoonline.com/read/120902/cost.html>; May, *supra* note 104, at 14; Sinangin, *supra* note 104, at 12.

110. Granick, *supra* note 105.

company's estimate. More intangible aspects of the cost calculation, such as damage to reputation and lost productivity due to network downtime, are even harder for a defendant to dispute given their speculative nature. The 2002 CSI/FBI Computer Crime Survey reported that 80% of respondents had experienced financial losses emanating from computer attacks, but only 44% could quantify their losses.<sup>111</sup> This is a significant gap and coming from an anonymous survey it demonstrates how hard it is to compute intangible losses accurately. Even when companies list these types of losses, accuracy remains questionable. Thomas Varney, a former Secret Service agent specializing in computer crime provides an instructive example: "A company calls up and says, 'We've just been hacked. We've lost \$1 million.' They pull a number out of the air . . . I ask how they got that number, and it turns out they're just guessing."<sup>112</sup> Conceivably, the difficulty of calculating intangible harm could benefit computer crime defendants because they would be able to cast doubt on any figure that a company might produce. In practice, however, this has not been the case. Courts have interpreted the CFAA to include these types of costs, despite their inexact nature. Courts have also been reluctant to let doubtful cost estimates benefit defendants and have shown deference to the calculations of victim corporations.<sup>113</sup>

Allowing companies to define the damage they have suffered is dangerous because they have an incentive to choose a figure in excess of \$5,000. A large proportion of computer crimes are perpetrated by disgruntled or former employees who use their knowledge to bypass the company's security measures.<sup>114</sup> In such a situation, executives may construe the intrusion as personal and thus may be encouraged to inflate the damage assessment in a vindictive attempt to get back at the employee. For example, in *Ingenix, Inc. v. LaGalante*, the defendant refused to return a laptop to his former employer and proceeded to download sensitive data that he intended to use to ingratiate himself to a competitor.<sup>115</sup> Though it was prosecuted as a civil case, Ingenix estimated the cost of examining the laptop at \$7,000 and was given wide flexibility to determine their business

---

111. Power, *supra* note 100, at 11. Forty-four percent was the highest percentage of respondents who could quantify their losses in the survey's seven years.

112. Kaplan, *supra* note 109.

113. Granick, *supra* note 105 (explaining that corporations have been expected to provide little, if any, documentation of their costs).

114. Eric Shaw et al., Dep't of Def. Sec. Inst., *The Insider Threat to Information Systems: The Psychology of the Dangerous Insider*, SECURITY AWARENESS BULL., Sept. 1998, at 1, 7.

115. 2002 U.S. Dist LEXIS 5795 (E.D. La. Mar. 28, 2002).

losses from the copied data.<sup>116</sup> In a criminal trial, the \$7,000 would have been sufficient to ensure that LaGalante faced a serious felony conviction. LaGalante's former employer could easily have retaliated against him by being extra diligent in examining the laptop and thereby inflating their costs to surpass \$5,000.

There is also reason to believe the FBI is encouraging companies to inflate their damage assessments. Jennifer Granick reports that the FBI regularly informs companies that there must be over \$5,000 in damages in order to warrant prosecution. She believes that this prompting is responsible for many of the high estimates of damage from computer intrusions.<sup>117</sup> While Granick can only speak to her own experience, there is circumstantial evidence that this practice is widespread. *2600: The Hacker Quarterly*, a journal devoted to computer hacking, has letters on its website purported to be communications between the FBI and executives of companies that have been hacked.<sup>118</sup> These letters demonstrate that the monetary figure chosen for the actual harm from incidents was always computed after consultation with law enforcement, rather than being a figure that was determined prior to companies' awareness of the legal importance of their calculations.

## VI. THE USAPA AND THE PUNITIVE APPROACH TO CYBERCRIME

In addition to strengthening the internal provisions of the CFAA, Congress has increased the penalties for cybercriminals who run afoul of the Act's provisions. The USAPA makes these penalties particularly severe with up to ten years for a first violation and twenty years for a repeat offender.<sup>119</sup> The Act was intended to counter the threat from malevolent foreign crackers and cyberterrorists, whose very existence is not even established. Despite these goals, the real world impact of these new penalties will be on far less exotic computer criminals. These penalties are substantial. They are a product of a mindset that morally and instrumentally justifies strong criminal sanctions in the fight against computer crime. This Article next looks into the question of whether the twin goals of deterrence

---

116. *Id.* at \*26-27.

117. Granick, *supra* note 105.

118. *New Mitnick Evidence Reveals Corporate Fraud*, 2600: THE HACKER Q., Apr. 22, 1999, at <http://www.2600.com/news/display/display.shtml?id=357>. *2600: The Hacker Quarterly* is the main periodical devoted to computer hacking and has a good reputation for the general quality of its information.

119. USAPA, *supra* note 10, § 814(c)(3) (codified at 18 U.S.C. § 1030(c)(4)(A), (C) (2000)).

and retribution are furthered by the criminal sanctions that are now attached to the CFAA.

#### A. Deterrence and the Utilitarian Justification for High Penalties

It is highly doubtful that the USAPA will be successful in deterring the criminals who motivated its drafting. The nature of terrorism is such that it attracts passionate adherents, so the threat of criminal sanctions is not likely to dissuade such actors from their causes. Not all terrorists are willing to be suicide bombers, but their commitment is usually sufficiently strong to be uninfluenced by the computer crime laws of the United States. While the USAPA does add extraterritorial jurisdiction to the CFAA and there have even been a few successful prosecutions of foreign nationals, the level of international coordination and resources necessary to track down foreign computer criminals makes it doubtful that this type of prosecution will be commonplace.<sup>120</sup> The likelihood of being prosecuted under the CFAA is so remote that higher penalties will not sufficiently impact the decision calculus of foreign crackers. Thus, the two groups most feared by those advocating stiffer penalties are the ones least likely to be influenced by the USAPA changes.

Higher penalties might still be justified if they successfully cut down on more commonplace types of computer crime, but such a reduction in crime seems doubtful. The Antiterrorism and Effective Death Penalty Act of 1996 directed the Sentencing Commission to examine the deterrent effect of the CFAA. After a review of the then-available data and the general scholarship on deterrence, the Commission concluded that there was insufficient data to reach a conclusion on the deterrent effect of criminal sanctions.<sup>121</sup> The report stressed that the effectiveness of deterrence is contextual and that speculation about deterrence is difficult because of the inherent dissimilarities between the various individuals grouped under the rubric of computer crime.<sup>122</sup> In all likelihood, there is not enough informa-

---

120. See Bill Boni, *Crossing the Line or Making the Case?*, COMPUTER FRAUD & SEC., Dec. 2002, at 18, 19 (relating the numerous obstacles to effectively pursuing foreign computer criminals).

121. See U.S. SENTENCING COMM., REPORT TO CONGRESS: ADEQUACY OF FEDERAL SENTENCING GUIDELINE PENALTIES FOR COMPUTER FRAUD AND VANDALISM OFFENSES 9 (June 1996), available at [http://www.ussc.gov/r\\_congress/COMPFRD.PDF](http://www.ussc.gov/r_congress/COMPFRD.PDF) (“The limited empirical data available to the Commission and other factors preclude a definitive assessment of the deterrent effect of existing guidelines for computer fraud and computer vandalism.”).

122. See *id.* (“[R]esearchers who have studied general deterrence have found that it is very difficult to say with certainty the extent to which a given criminal sanction discourages criminal conduct.”); see also Sanford Sherizen, *Can Computer Crime Be Deterred?*,

tion available on the psychology of computer criminals and other variables to make a declarative statement about deterrence. However, there is some evidence available that suggests that deterrence is not very effective in the context of computer crime.

Deterrence theory needs to account for the empirical evidence that nineteen years under the CFAA has done little to slow the growth of computer crime.<sup>123</sup> A common response is that the Act has always been plagued by poor draftsmanship and insufficient criminal penalties, which have rendered it ineffective. Despite these problems, the community of computer criminals is small and the message that computer crime is a serious offense should have been sufficiently communicated to this group by now. Between 1992 and 1998, 196 people were convicted of computer crimes, with 84 receiving prison sentences.<sup>124</sup> This is not an insignificant number. Based on these figures it should be obvious to all interested parties that the legal system regards computer crime as a serious offense, worthy of incarceration. Additionally, a number of these prosecutions, such as those of Kevin Mitnick and Kevin Poulsen, were high profile and received widespread media attention.<sup>125</sup> It seems reasonable that the shift in penalties from parole to jail time in most computer crime cases is a more powerful signal to would-be computer criminals than the change from five to ten years of jail time. Despite these signals, the anticipated decrease in computer crime has not come, a trend that has not been confined to the U.S. experience. Britain, Malaysia, and Singapore all have strong computer crime legislation, but the computer crime rates of all three countries continue to climb.<sup>126</sup>

One explanation for the unabated increase in computer crime is that not enough time has passed to see the effects of deterrence on computer criminals. Essentially, it is unfair to assess the success or failure of sub-

---

6 SEC. J. 177, 180 (1995) (“As difficult as deterrence is to apply, computer crime makes an even more difficult target.”).

123. See Power, *supra* note 100, at 11 (survey results indicate that the amount of damage grew in comparison to past years).

124. See Banisair, *supra* note 66 (based on the statistics released under the Freedom of Information Act).

125. Wade Roush makes the interesting point that the criminal seriousness of computer hacking was apparent even before the Mitnick and Poulsen cases. See Roush, *supra* note 54, at 32. He finds that the 1989-1990 FBI crackdown on computer crime, Operation Sundevil, sufficiently conveyed the message to the cybercrime community that hacking cases would be prosecuted and would likely result in incarceration. *Id.*

126. Indira Carr & Katherine S. Williams, *Securing the E-Commerce Environment: Enforcement Measures and Penalty Levels in the Computer Misuse Legislation of Britain, Malaysia and Singapore*, 16 COMPUTER LAW & SEC. REP. 295, 304 (2000).

stantial penalties until a generation has matured under them. This point may have the most relevance with regard to script-kiddies, the group most likely to internalize a prohibition against hacking. They are casual participants in computer crime and their lower level of connection to the activity means that it may eventually be possible to inculcate a different set of values. However, their youth and general lack of sophistication also make them unlikely to consider the consequences of their actions, even the potential for significant jail time. While high penalties might eventually influence script-kiddies, any visible effect would likely take a long time to manifest.

Given the psychology of hackers and crackers, there is reason to believe that these categories of more dedicated computer interlopers will not be deterred by significant criminal penalties. Indira Carr and Katherine Williams contend that hackers are drawn to the mental challenge of bypassing security and as such do not utilize the cost-benefit analysis that underlies deterrence theory. Essentially, the only way these individuals feel they can prove their intellectual prowess is through hacking, so they will continue to do so regardless of the potential consequences.<sup>127</sup> One source of support for this argument comes from Paul Taylor's study of the hacking community. Taylor found that hackers have diverse motivations, but did not find any hackers who were motivated by the practical gains derived from breaking into computers. Instead, the hackers were driven by more benign motivations such as curiosity, feelings of power, and the camaraderie of belonging to a community.<sup>128</sup> In contrast, crackers hope to profit from their computer crimes, although this does not mean that personal enrichment is their sole motivation. They are often just as enamored with the mental challenges involved in breaking into secure systems as hackers, and financial gains are generally a secondary concern.<sup>129</sup> Furthermore, many hackers and crackers describe the mental rush of the activity as being so powerful that it is beyond their control. They are addicted to hacking.<sup>130</sup> It is probably premature to categorize hacking as a physical

---

127. Indira Carr & Katherine S. Williams, *A Step Too Far in Controlling Computers?: The Singapore Computer Misuse (Amendment) Act 1998*, 8 INT'L J.L. & INFO. TECH. 48, 56 (2000) (through their analysis is of the Singapore Act, they make this point generally); see also Raju Chebium, *Experts Say More Laws Won't Stop Computer Hackers*, CNN INTERACTIVE, May 8, 2000, at <http://www.cnn.com/2000/LAW/05/05/love.bug/>.

128. TAYLOR, *supra* note 57, at 46.

129. *Id.* at 19-22.

130. *Id.* at 46-50; see also Tom Mulhall, *Where Have All the Hackers Gone? Part 5—Conclusions*, 16 COMPUTERS & SEC. 304, 305 (1997) (Mulhall believes that legislation does have a deterrent effect, but finds it is undercut to a large degree by addiction).

addiction, however, there is sufficient support for this proposition for Paul Bedworth to successfully raise addiction as a defense in the first trial under the UK's Computer Misuse Act.<sup>131</sup> Bedworth was so pathologically beholden to hacking that he would lock himself in his room and stay fixated on his computer for days until he dropped from exhaustion.<sup>132</sup> Not every computer criminal will demonstrate this degree of attachment, but the Bedworth example does suggest that the cost-benefit foundation of deterrence theory may be ill-suited to the context of computer crime.

## **B. The Negative Side Effects of High Penalties**

Another problem with deterrence is that it ignores the makeup the hacker community. The main reason that hackers do not intentionally damage networks or commit fraud is a type of communal boundary formation.<sup>133</sup> Hackers do not see themselves as criminals and enforce a code of conduct that functions as a form of self-regulation. By not distinguishing between types of computer intruders and their crimes, the recent changes to the law will likely alienate hackers. Should hackers perceive that they are victimized by an unfeeling legal system where the punishment is not commensurate with the crime, this boundary formation may slip away. Such a process may have already started, as the hacker community was incensed by the legal system's treatment of Kevin Mitnick and responded in an uncharacteristically organized and political fashion.<sup>134</sup> This anger need not necessarily take a political form. Taylor found that hackers are under increasing pressure from third parties to use their skills for more traditionally criminal ends.<sup>135</sup> The potential now exists for an alienated hacker community to turn to more destructive crimes in response to the new penalty levels.

There are other indications that high penalty levels may actually exacerbate the problem of computer crime. It is generally accepted that the threat of being hacked has led to a revolution in computer security, forcing software companies to pay attention to the problem of how to effectively

---

131. *Id.*

132. Gillian Harris, *Daring Data Raider Dependent on Hacking Fix*, THE SCOTSMAN, Mar. 18, 1993.

133. TAYLOR, *supra* note 57, at 25-26; *see also* THOMAS, *supra* note 56, at 110 (arguing that the hacker ethic not only exists but is strengthening as the community has become more political).

134. THOMAS, *supra* note 56, at 232.

135. TAYLOR, *supra* note 57, at 19-22 (arguing that criminal groups are starting to draw upon the skills of hackers).

safeguard data.<sup>136</sup> Computer hackers play an under-appreciated role in raising awareness of security issues. The threat they pose has been instrumental to the development of new technologies such as encryption and biometrics.<sup>137</sup> This does not mean that these developments are efficient, since security is necessary only to the extent that it prevents a more socially harmful loss. Otherwise, it is a wasted expenditure of resources. On the surface, this situation appears analogous to other criminal endeavors—certainly the threat of bank robbery has led to the creation of better safes. The crucial difference is that there is not a benign form of bank robbery. Software producers do not want to be embarrassed by having hackers effortlessly break the security they have designed, thus the threat of benign hacks has probably been responsible for advances in software design and testing that are working to counter much more dangerous computer intrusions. This reaction may also not be economically efficient, but such an economic analysis is beyond the scope of this paper. This reaction does, however, reveal a crucial difference with other types of crime which only spur countermeasures designed to protect against the original crime.

Hackers have also been successful in pointing out security problems and suggesting improvements. On this point, Douglas Thomas notes, “hacks are often discovered, reported, and patched by hackers themselves without ever using them to compromise someone else’s computer or security.”<sup>138</sup> Hackers frequently help to close the very holes that crackers and cyberterrorists could exploit in pursuit of their criminal objectives.<sup>139</sup> Because hackers are attracted by the mental challenge of testing supposedly-secure systems or widely disseminated products such as Microsoft prod-

---

136. See JOHN VIEGA & GARY MCGRAW, BUILDING SECURE SOFTWARE: HOW TO AVOID SECURITY PROBLEMS THE RIGHT WAY 15-16 (2002) (“[Software vendors] start to worry about security only after their product has been publicly (and often spectacularly) broken by someone.”).

137. See Liz Duff & Simon L. Gardiner, *Computer Crime in the Global Village: Strategies for Control and Regulation—in Defence of the Hacker*, 24 INT’L J. SOC. L. 211, 220 (1996).

138. THOMAS, *supra* note 56, at 43.

139. This role is particularly important given the significant number of security holes in most software products. See, e.g., Abner Germanow et al., *The Injustice of Insecure Software*, @Stake Research Report (@stake, New York, NY), Feb. 2002, available at [http://www.atstake.com/research/reports/acrobat/atstake\\_injustice.pdf](http://www.atstake.com/research/reports/acrobat/atstake_injustice.pdf) (explaining that most applications are full of security holes); Rebecca T. Mercuri, *Security Watch: Computer Security Quality Rather than Quantity*, 45 COMM. OF THE ACM 11, 12 (October 2002); Bruce Schneier, *Foreword* to JOHN VIEGA & GARY MCGRAW, BUILDING SECURE SOFTWARE: HOW TO AVOID SECURITY PROBLEMS THE RIGHT WAY, at xix (2002) (“[T]he average large software application ships with hundreds, if not thousands, of security related vulnerabilities.”).

ucts, their contribution to system patches and product improvements is significant. Consequently, increasing the punishments for benign intrusions might actually be detrimental to the overall goal of reducing the damage from computer crime.

A final argument against increased sentences for computer crime comes from an interesting parallel with the war on drugs. An examination of the cases currently being pursued by the Department of Justice reveals that the majority of people who are indicted for computer crimes are either company insiders or unsophisticated computer users.<sup>140</sup> The preponderance of these types of cases may be due to the targeting of low-level offenders. This problem frequently occurs in the drug context. High mandatory minimum sentences for distribution of drugs encourage prosecutors to go after mules rather than the drug kingpins because mules are easier to catch yet still receive a serious sentence.<sup>141</sup> This does not impute cynicism or maliciousness to criminal justice professionals, but prosecutors are judged by their conviction rate and the distinction between morally guilty and provably guilty is often blurred.

Prosecutors are often under pressure to take only cases that will result in conviction and incarceration. Susan Kelley Koeppen, a former federal prosecutor, makes the point that the decision whether to investigate and prosecute a given cybercriminal is often based on the perceived possibility of a stiff sentence:

I speak from my own experience in saying that cyber criminals often don't get punished, because the applicable sentencing guidelines focus primarily on economic harm which is often difficult to calculate and may not reflect the true harm caused. Be-

---

140. The last statistics released on computer crime prosecutions under the CFAA are from 1998, so these releases represent the best available evidence of what types of offenders are being targeted. See CCIPS, *Legislative Analysis*, supra note 27. While the alleged amount of damage caused by the computer criminals seems to be extensive, the estimates are questionable as a number of them parallel the trophy problem demonstrated in the Mitnick and Neirdorf cases. Granick concurs with this assessment, as she believes that in these releases the DOJ is substantially inflating the harm caused. See Granick, *supra* note 105.

141. For a detailed analysis of how higher penalties that were supposed to be reserved for high-level offenders actually lead to greater targeting of low-level offenders in the drug context see U.S. SENTENCING COMMISSION, REPORT TO CONGRESS: COCAINE AND FEDERAL SENTENCING POLICY (May 2002), at [http://www.ussc.gov/r\\_congress/02crack/2002crackrpt.pdf](http://www.ussc.gov/r_congress/02crack/2002crackrpt.pdf).

cause these crimes do not merit stiff sentences, they may, in turn, not be investigated or prosecuted.<sup>142</sup>

Koeppen believes the solution is to make it easier to get harsh sentences by adjusting the sentencing guidelines, but perhaps it would be wiser to maintain the high threshold of culpability for severe penalties. The Department of Justice admits that it faces numerous obstacles to catching sophisticated cybercriminals, raising the possibility that resources could be shifted towards pursuing script-kiddies, who are now eligible for sufficiently long sentences.<sup>143</sup> Prosecution of script-kiddies represents a temptation, law enforcement's path of least resistance, but hardly a solution to the problem of computer crime.

There are also organizational tendencies that increase the potential for a focus on prosecuting low-level offenders. Because they are immersed in a world of crime, criminal justice professionals tend to employ cognitive maps which are rigidly bifurcated between good and bad. David Wall provides an example: "[F]or the police, objectives and places having routine uses are conceived of in terms of favorite misuses. Garbage cans are places in which dead babies are thrown, schoolyards are places where mobsters hang out, stores are places where shop lifters go, etc."<sup>144</sup> Applying these studies to cybercrime, Wall concludes that criminal justice professionals mentally group hackers together; the negative characteristics that they possess as a class are attached to all individuals categorized as belonging to that class irrespective of experience, potential for damage, or intent.<sup>145</sup> Bruce Sterling succinctly explains the implications of this argument by observing that, "police want to believe all hackers are thieves."<sup>146</sup> If one believes all computer intruders possess a significant, if not equivalent, degree of culpability, in a situation of limited resources it is logical to

---

142. *Hearing on H.R. 3482, supra* note 7, at 8 (statement of Susan Kelley Koeppen).

143. *Internet Denial of Service Attacks and the Federal Response: Hearing Before the Subcomm. on Crime, House Comm. on the Judiciary and the Subcomm. on Criminal Oversight of the Senate Comm. on the Judiciary*, 106th Cong. (2000) (statement of Eric Holder, Deputy Attorney General), available at <http://www.usdoj.gov/criminal/cybercrime/dag0229.htm> (explaining the technical and resource hurdles to catching sophisticated computer criminals); see also Marc D. Goodman, *Why the Police Don't Care about Cybercrime*, 10 HARV. J.L. & TECH. 465, 483-488 (1997); David S. Wall, *Catching Cybercriminals: Policing the Internet*, 12 INT'L REV. L., COMPUTERS & TECH. 201, 211 (1998).

144. Wall, *supra* note 143, at 212 (quoting Howard Sacks, *Notes on Police Assessment of Moral Character*, in *STUDIES IN SOCIAL INTERACTION* 292 (D. Sudnow ed., 1972)).

145. *Id.*

146. STERLING, *supra* note 65, at 63.

prioritize cases by the ease of apprehension. Consequently, resources are shifted towards pursuing the criminals that are easiest to catch, namely script-kiddies. Compounding this problem is a lack of technological sophistication on the part of criminal justice professionals. Although the focus on computer crime continues to intensify and more specialists are being committed to this area, the general level of computing knowledge remains very low.<sup>147</sup> The difference between kingpins and mules in the computer crime taxonomy may not be immediately apparent to a federal prosecutor, making a low-level offender focus all the more likely.

### **C. Retribution and the Morality of Punishing Cybercrime**

The other possible justification for severe penalties for computer crime is retribution, punishing behavior that offends societal norms. Although there are different theories of retribution, one common principle they share is proportionality: the punishment exacted must approximate the harm perpetrated.<sup>148</sup> Computer crime is nonviolent and results only in economic harm. Therefore, a victim corporation could be made whole by seeking a remedy in tort law or under the civil liability subsection of the CFAA. However, this Article does not contend that proportionality demands cybercriminals be exempt from criminal punishment or even incarceration. The harm from a computer attack can go beyond the victim corporation, as the damage could have severe effects for stockholders and the economy in general. There may also be indirect consequences. Attacks can create a climate of fear that can stifle online commerce or cause companies to inefficiently over-invest in security. Additionally, cybercriminals generally do not have sufficient funds to repay those they injure, making civil remedies insufficient for providing proper punishment.

While there is a general moral case for strong penalties, some countervailing factors call into question whether the current level of punishment is too high. It may be improper to assign complete moral culpability for the damage from computer attacks to cybercriminals. As was explained earlier, many companies purposely choose to under-invest in computer security and others negligently fail to repair widely known holes in their networks. Duff and Gardiner note that European law recognizes a duty on

---

147. Goodman, *supra* note 143, at 479-80 (focusing on police officers, but utilizing studies that are indicative of an overall lack of knowledge); Wall, *supra* note 143, at 211.

148. Philosophical support for proportionality can be traced back to Immanuel Kant and his critique of utilitarian approaches to punishment. The crux of his position is that no benefit accruing to the criminal or society will justify punishment that is not otherwise necessary to maintain the moral equilibrium. More contemporary support can be found in the theories of John Rawls, Andrew Von Hirsch, and Michael Walzer.

the part of the data holder to take sufficient security measures to protect its data.<sup>149</sup> They contend that holding the computer hacker fully culpable for economic damage when a company has been derelict with respect to this duty is not just.<sup>150</sup> Although no analogous affirmative duty exists in the United States, their argument is still forceful at a philosophical level. Admittedly, a problem for this position is that hackers have freely chosen to exploit these security holes. However, Duff and Gardiner's point is supported by the fact that a significant portion of the costs from a given attack are not directly attributable to the computer criminal. The high expense of resecuring results from the need to fix any security holes that existed prior to any action by the attacker. Furthermore, the damage to a company's reputation comes from the public perception that the company is negligent with regard to security and is vulnerable to further attacks, both of which are probably accurate. Hackers do not choose targets at random and, to a large degree, they do not have sufficient skill to penetrate adequately secure systems. Similar to how truth is always a defense against a libel claim, it is wrong to blame hackers for simply revealing the innate weaknesses of a company's security implementation.

Removing resecuring costs and lost customer goodwill from the damage calculation makes it far more difficult to justify harsh penalties on retributive grounds. Without these tangential harms, the damage from most attacks is fairly localized and does not justify the penalties that exist under the USAPA. Intentional cracking that causes significant financial losses should still be severely punished, but this would be possible under a CFAA with a different structure.

## VII. A WAY FORWARD

In the past twenty-five years we have witnessed a revolution in computing that first brought the computer into the home and then connected it to the world. Twenty-five years is a relatively brief time period for such dramatic technological change and society is still grappling with related social issues like computer hacking. Lawrence Lessig provides an excellent summary of how society has decided to make sense of hacking, and respond to it:

---

149. Duff & Gardiner, *supra* note 137, at 220-21; *see also* Chris Pounder, *The Emergence of a Comprehensive Obligation Towards Computer Security*, 21 COMPUTERS & SEC. 328, 328-9 (2002) (explaining the obligations of data controllers under both UK and EU statutes).

150. Duff & Gardiner, *supra* note 137, at 221.

It didn't take much to see that this world would not survive for long. This community of people who thought it fair to test the locks, enter someone else's machine if they could, and snoop their file structure—this community was not going to mesh with a Net where commerce could survive. It may have been fine to play these games in a world of geeks, but when money came on-line a better system of security was inevitable.

As these cultures came into conflict, real-space law quickly took sides. Law worked ruthlessly to kill a certain kind of online community. The law made the hackers' behavior a "crime," and the government took aggressive steps to combat it. A few prominent and well-publicized cases were used to redefine the hackers' "harmless behavior" into what the law would call "criminal." The law thus erased any ambiguity about the "good" in hacking.<sup>151</sup>

This Article is not responding to the criminalization of hacking, as defined by Lessig, but to the mindset with which it has been done. Lessig's words effectively capture the reactionary nature of the governmental response, how the foreignness of the threat was dealt with by simplistically defining computer hacking as unequivocally criminal. In 1986, the economic potential of online commerce was not yet apparent, and Congress was able to consider rationally how to balance the various issues involved without fear of alienating business interests. The result was a sensible piece of legislation built upon the distinction between computer trespass and harmful computer crime, and now it is time to revise the CFAA to resurrect this distinction.

Such a revision could take many forms, but there are a number of changes that are particularly important. The felony monetary threshold should be increased to \$10,000, with resecuring costs exempted. Reputational damage should also be exempted, unless it could be shown that the damage was caused intentionally and was a foreseeable consequence of the attack. The requisite intent for each section of the Act must also be clarified. In particular, the difference between recklessness and negligence for the purposes of subsection (a)(5) should be expounded. Such an explanation would aid those courts that might not be well-versed in technological issues and give script-kiddies, hackers, and crackers alike the fair warning that they deserve. Additionally, *Czubinski's* "idle curiosity" distinction should be codified into law as part of the (a)(4) fraud subsection in order to ensure that those fraud provisions are only applied to situations

---

151. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 194 (1999).

where there is a genuine illicit purpose. Finally, the USAPA sentencing changes should not be implemented until more is known about the deterrent effect of computer crime penalties and, even then, the Sentencing Commission should be instructed to adjust the Guidelines for the purposes of moderating the use of these long sentences. These changes, and others like them, can help ensure that the CFAA is an effective and balanced instrument in promoting computer and network security.