NOTE

Hacking Through the Computer Fraud and Abuse Act

TABLE OF CONTENTS

INTRODUCTION

Do crimes in cyberspace[1] worry you? Do you worry about strange "hackers"[2] invading your life through the Internet?[3] Regardless of whether you are worried, Congress is worried. Concerns over rising computer crime pushed Congress to enact the Computer Fraud and Abuse Act ("CFAA").[4] CFAA is a criminal statute that contains an anti-hacking provision.[5] Under the anti-hacking provision, the government can punish computer users who gain unauthorized access into a computer system and cause damage.[6]

Since enacting CFAA in 1984, Congress has attempted to increase CFAA's effectiveness by changing it numerous times.[7] In particular, Congress has repeatedly changed the level of mens rea — the mental state component for particular crimes — required to commit computer crimes.[8] Most recently, Congress lowered the mens rea requirements for computer crimes defined in CFAA.[9] However, Congress overlooked important public policies that it should address through higher mens rea requirements. Specifically, CFAA fails to protect innocent outside users. Moreover, CFAA does not encourage the private sector to protect itself.

---

[1] *See* Michael P. Dierks, *Computer Network Abuse*, 6 HARV. J.L. & TECH. 307, 307 n.1 (1993) (noting that term "cyberspace" initially referred to fantasy electronic world in William Gibson's novel Neuromancer). The term "cyberspace" describes electronic computer networks. *See id.*

[2] *See* JAMES V. VERGARI & VIRGINIA V. SHUE, FUNDAMENTALS OF COMPUTER — HIGH TECHNOLOGY LAW 361 (1991) (defining term "hacker" as talented computer user who gains or attempts to gain unauthorized access to computer systems). The term "hacker" may negatively refer to a computer criminal. *See* Dierks, *supra* note 1, at 310 n.7.

[3] *See* MTV Networks v. Curry, 867 F. Supp. 202, 203 n.1 (S.D.N.Y. 1994) (stating that Internet is network of thousands of independent networks with several million "host" computers providing information services). The Internet is the world's largest computer network. *See id.* About 25 million individuals have Internet access. *See id.*

[4] *See* 18 U.S.C. § 1030 (1984).

[5] *See* S. REP. NO. 104-357, at 9 (1996) (describing § 1030(a)(5) as measure that protects computers from hackers).

[6] *See* 18 U.S.C. § 1030(a)(5) (1996) (stating that unauthorized access users who damage protected computers are breaking law).

[7] *See* S. REP. NO. 104-357, at 6-14 (describing changes made in CFAA).

[8] *See id.* at 10-11 (discussing changes in mens rea level).

[9] *Compare* 18 U.S.C. § 1030(a)(5)(A)-(B) (1994) (defining mens rea as intentional, knowing, and reckless) *with id.* § 1030(a)(5)(A)-(C) (1996) (defining mens rea levels at intentional, knowing, reckless, and strict liability).

This Note examines CFAA's mens rea requirements and discusses its problems. Part I provides a general discussion of the mens rea concept and explores the Internet's history. Part I also discusses Congress's amendments to CFAA and how courts have addressed the mens rea requirements. Part II examines the mens rea requirements in the current version of CFAA. Part III analyzes section 1030(a)(5) of CFAA and considers the impact of the current mens rea requirements on public policy concerns regarding computer crimes. Part III concludes that the current mens rea requirements are flawed. Finally, Part III proposes that Congress should amend CFAA to require intentional mens rea.

I. BACKGROUND

The advent of the Internet brought about new forms of computer crimes.[10] In response, Congress considered legislation to address these crimes.[11] As a result, Congress enacted CFAA in 1984.[12] However, the public criticized the first version of CFAA because of its limited impact.[13] Subsequently, Congress made changes to CFAA to correct its perceived deficiencies.[14] In its attempts to refine CFAA, Congress followed court precedent and lowered the mens rea requirements.[15] Accordingly, CFAA now criminalizes hacking if hackers gain unauthorized access to computer systems, whether they intend to damage the system or not.[16] CFAA accomplishes this through low mens rea requirements.

---

[10] *See infra* note 32 and accompanying text (discussing new computer crimes).

[11] *See* S. REP. NO. 99-432, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2481 (discussing enactment of CFAA to address computer crimes).

[12] *See id.*

[13] *See* Glenn D. Baker, Note, *Trespassers Will Be Prosecuted: Computer Crime in the 1990s*, 12 COMPUTER/L.J. 61, 63-66 (1993) (explaining that critics felt CFAA was too vague and too limited).

[14] *See* S. REP. NO. 104-357, at 4, 10 (1996) (discussing changes to CFAA in 1986 and 1994).

[15] *See infra* note 73 and accompanying text (discussing how Congress codified mens rea standard interpreted by courts).

[16] *See* S. REP. NO. 104-357, at 10 (indicating Congress's desire to punish hackers who unintentionally cause damage to computer systems).

A. Mens Rea Concept

Two elements exist in all crimes: actus reus and mens rea.[17] Actus reus defines the action of a crime while mens rea defines the mental state.[18] The mens rea requirement is the central component of most crimes.[19] In particular, mens rea describes the specific mental state required to commit certain crimes.[20] The Model Penal Code ("MPC") lists four levels of mens rea — purposely, knowingly, recklessly, and negligently.[21] The MPC categories range from the highest level, purposely, to the lowest

---

[17] *See* LEO KATZ, BAD ACTS AND GUILTY MINDS 81 (1987) (stating that two elements exist in criminal offenses); JAMES MARSHALL, INTENTION IN LAW AND SOCIETY 6 (1968) (stating that intent and act must concur for crime); Martin R. Gardner, *The Mens Rea Enigma: Observations on the Role of Motive in the Criminal Law Past and Present*, 1993 UTAH L. REV. 635, 637 (1993) (indicating that mens rea fails to capture all mental activity for criminal culpability and that actus reus is needed). Generally, actus reus refers to the physical element of criminal offense. *See* KATZ, *supra*, at 81; *see also* MARSHALL, *supra*, at 8 (stating that actus reus is evil deed or evil hand). For example, in murder, actus reus is the act of killing. *See* KATZ, *supra*, at 81. Mens rea refers to the mental part of the criminal offense or the guilty mind. *See id.* Therefore, in murder, mens rea is the intent to kill. *See id.*

[18] *See* KATZ, *supra* note 17, at 81 (describing actus reus as physical element of crime and mens rea as mental element of crime); *see also* Gardner, *supra* note 17, at 641-84 (tracing development of mens rea from earliest ancient Hebrew law and early English common law to modern Model Penal Code); Kenneth W. Simons, *Rethinking Mental States*, 72 B.U. L. REV. 463, 469-70 (1992) (discussing innovative categorization of Model Penal Code). The current concept of mens rea has evolved throughout history. *See* Gardner, *supra* note 17, at 641-84 (discussing common law evolution of mens rea requirement in crime and punishment). Early Christian ethics emphasized moral guilt. *See id.* at 654-55. Therefore, mens rea embodied the notion that only the "guilty minds" should be punished. *See id.* (stating that behavior cannot be judged without attention to state of mind). The courts have used an array of words, such as "malicious," "willful," or "fraudulent" to describe the evil motive. *See* Morissette v. United States, 342 U.S. 246, 252 (1952) (acknowledging that courts used unscientific terms to describe evil purpose or mental culpability).

[19] *See* MODEL PENAL CODE § 2.02 (1995).

[20] *See id.* § 2.02(1)-(2) (listing four categories of mens rea); KATZ, *supra* note 17, at 186 (stating that modern drafters now use four basic mental elements); Gardner, *supra* note 17, at 697, 716 (stating that evil motive concept of mens rea was abandoned for structured system and describing development away from normative concept of mental state). The present structure of mental state requirements is not perfect. *See generally* Simons, *supra* note 18 (discussing structure of present mental state requirements and its flaws). But the Model Penal Code hierarchy generally works well. *See id.* at 490 (stating that reigning hierarchy translates underlying approaches such as blameworthiness or utilitarianism); *see also* Gardner, *supra* note 17, at 684 (indicating that Model Penal Code still reflects subjective culpability while moving toward objective categorization).

[21] *See* MODEL PENAL CODE § 2.02(2)(a)-(d). The Model Penal Code describes the four levels of mens rea in terms of conduct, circumstances, or result of a criminal offense. *See* Gardner, *supra* note 17, at 682; Simons, *supra* note 18, at 469-70.

level, negligently.[22] These mens rea levels are further divided into high and low mens rea requirements.[23] The high mens rea levels include acts criminals do intentionally and knowingly.[24] The low mens rea levels include acts criminals do recklessly, negligently, and with strict liability.[25] Criminals have a higher level of mens rea when their intent is more specific; therefore, they are more blameworthy.[26] With these differing mens rea categories in mind, Congress drafted CFAA to address computer crimes occurring on the Internet.[27]

---

[22] *See* MODEL PENAL CODE § 2.02(2)(a)-(d) (indicating purposely and knowingly require specific awareness but recklessly and negligently do not).

[23] *See* KATZ, *supra* note 17, at 186 (stating that intention or purpose and knowledge are most important). Purposely is the highest level of mens rea. *See id.* This level requires that a person act with a "conscious object to engage in conduct . . . or to cause such result." *See* MODEL PENAL CODE § 2.02(2)(a)(i). A person must also be aware of his circumstances. *See id.* § 2.02(2)(a)(ii). The second highest level of mens rea is knowingly. *See* Gardner, *supra* note 17, at 725, 727. It requires that a person is practically certain his action will cause a result. *See* MODEL PENAL CODE § 2.02(2)(b)(ii). A person acts knowingly when:

> (i) if the element involves the nature of his conduct or the attendant circumstances, he is aware that his conduct is of that nature or that such circumstances exist; and
> (ii) if the elements involves a result of his conduct, he is aware that it is practically certain that his conduct will cause such a result.

Id. § 2.02 (2)(b)(i), (ii). The next level, recklessly, requires conscious disregard of a substantial and unjustifiable risk. *See id.* § 2.02(2)(c). This disregard must be a gross deviation from the standard of a law abiding person. *See id.* Recklessly may be the most important culpability term because this is the default level when the statute specifies no mental state. *See* Simons, *supra* note 18, at 470 (stating that common law requires that defendants have at least reckless intent). Negligence requires that a person should have been aware of a substantial and unjustifiable risk. *See* MODEL PENAL CODE § 2.02(2)(d). Besides the Model Penal Code categories, the courts have also recognized the non-existence of a mens rea requirement in strict liability. *See Morissette*, 342 U.S. at 254-56 (describing why certain regulations require no intent level). Generally, strict liability only exists for public welfare offenses. *See id.*

[24] *See* KATZ, *supra* note 17, at 186 (using purposely and intentionally interchangeably). The purposeful level will be referred to as an intentional level in this Note.

[25] *See supra* note 23 and accompanying text (discussing low levels of mens rea).

[26] *See* Simons, *supra* note 18, at 495-96 (stating that higher mental state is more culpable and blameworthy than lower mental state).

[27] *See* S. REP. NO. 104-357, at 9-12 (1996) (discussing effect of different mens rea requirements and intended effect from using different mens rea).

B. Internet and Crime

The Internet is an outgrowth of Arpnet, an experimental communications network.[28] Initially, researchers and educators used the Internet for the free exchange of information.[29] The Internet rapidly grew in popularity and currently has twenty-five to forty million users.[30] Today, most Internet users access it for mainstream commercial purposes.[31] As the Internet expands, however, so does a new type of crime — computer crime.[32]

---

[28] *See* Robert L. Dunne, *Deterring Unauthorized Access to Computers: Controlling Behavior in Cyberspace Through a Contract Law Paradigm*, 35 JURIMETRICS J. 1, 2 (1994) (stating that Internet developed during Cold War, and Arpnet's sole goal was to maintain communication between important sites in event of nuclear war).

[29] *See* Catherine Therese Clarke, *From CrimINet to Cyber-Perp: Toward an Inclusive Approach to Policing the Evolving Criminal Mens Rea on the Internet*, 74 OR. L. REV. 191, 195 (1996) (stating that Internet was for research and education); Brenda Nelson, Note, *Straining the Capacity of the Law: The Idea of Computer Crime in the Age of the Computer Worm*, 11 COMPUTER/L.J. 299, 317 (1991) (stating that Internet allows free exchange of information).

[30] *See* MTV Networks v. Curry, 867 F. Supp. 202, 203 n.1 (S.D.N.Y. 1994) (estimating 25 million users); Clarke, *supra* note 29, at 196 (estimating that less than 40 million people use Internet). One court predicts that about 100 million people will use the Internet in a matter of years. *See* Intermatic Inc. v. Toeppen, 947 F. Supp. 1227, 1230 (N.D. Ill. 1996). Despite its enormity, no single entity controls or regulates the Internet. *See Curry*, 867 F. Supp. at 203 n.1 (stating that no one owns Internet). Thus, the attributes of the Internet include chaos and free information. *See* Clarke, *supra* note 29, at 194-95 (stating that Internet's greatest asset and weakness is chaos).

[31] *See* Clarke, *supra* note 29, at 195-96. In particular, the World Wide Web helped to commercialize the Internet. *See id.* at 195 (noting that Internet's commercial growth has focused around World Wide Web).

[32] *See* Dunne, *supra* note 28, at 2-3 (discussing Internet's growth). The host computers grew from four in 1969 to 2,217,000 in 1994. *See id.* Furthermore, the number of the Internet users doubles each year. *See Curry*, 867 F. Supp. at 203 n.1; Dunne, *supra* note 28, at 4 (discussing increasing reports of computer security problems to Computer Enforcement Response Team). In 1988, Defense Advanced Research Projects Agency formed the Computer Enforcement Response Team ("CERT") to coordinate law enforcement agencies' responses to computer security problems. *See CERT Coordination Center 1996 Annual Report (Summary)*, ¶ 15 (visited Nov. 30, 1997) <http://www.cert.org/pub/annual-reports/cert_rpt_96.html>. CERT handled 1334 security incidents in 1993, which generated 21,267 e-mails and 2282 phone calls. *See id.* In 1996, CERT handled 2573 security incidents, which generated 31,268 e-mail and 2062 phone calls. *See id.*; *see also* Dierks, *supra* note 1, at 314-19 (detailing different hacker cases); Jo-Ann M. Adams, Comment, *Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet*, 12 SANTA CLARA COMPUTER & HIGH TECH. L.J. 403, 409-11 (1996) (discussing different computer crimes and rise in computer crimes each year). Because of the nature of computer crimes, they do not fit within the framework of traditional crimes. *See* Scott Charney, *Computer Crime: Law Enforcements Shift from a Corporeal Environment to the Intangible, Electronic World of Cyberspace*, 41 FED. B. NEWS & J. 489, 489-90 (1994) (explaining uniqueness of computer crime because of lack of physical boundaries). To describe these

People commit computer crimes for different reasons.[33] The media has portrayed hackers as the major computer criminals.[34] In so generalizing, however, the distinctions between types of hackers are lost. Traditional hackers are outsiders who generally maintain hacker ethics.[35] As outsiders, they do not have authorization to access a particular system.[36] These hackers access systems generally out of curiosity and to learn, not for financial gain.[37] Traditional hackers do not intend to damage computer systems.[38]

---

new crimes, new classifications emerged. *See* David Carter, *Computer Crime Categories: How Techno-Criminals Operate*, 64 L. ENFORCEMENT BULL. 21, 21-24 (1995) (explaining four different categories of computer crimes). One main difference between computer crimes and traditional crimes is that a computer can occupy several different roles in a crime. *See id.* First, computers themselves can be targets or objects of the crime. *See* Xan Raskin & Jeannie Schaldach-Paiva, *Computer Crimes, Eleventh Survey of White Collar Crime*, 33 AM. CRIM. L. REV. 541, 543 (1996) (defining object computer crime). Second, computers can also be the subject of the crime. *See* VERGARI & SHUE, *supra* note 2, at 351 (defining computer crime as subject). When computers are the subject of a crime, the physical site of the crime or source for the crime is the computer itself. *See id.* An example of this category is when somebody releases a virus, disrupting the operations of the computer systems. *See* Raskin & Schaldach-Paiva, *supra*, at 543. Third, a computer can be an instrument used to commit crimes. *See id.* (discussing crimes where computer is instrument). For example, hackers can use a computer to create a fake bank account and embezzle funds. *See id.*

[33] *See* VERGARI & SHUE, *supra* note 2, at 361-63 (explaining terms "hackers," "phreakers," and "phrackers"; discussing youth of some criminals); Dierks, *supra* note 1, at 314-21 (detailing different hacker cases and asserting that insiders cause more damage); *see also* Clarke, *supra* note 29, at 206-13, 219-23 (discussing hackers, CrimINets, and Cyber-Perps).

[34] *See* Dierks, *supra* note 1, at 314-21 (detailing media's focus on different hacker cases); Raskin & Schaldach-Paiva, *supra* note 32, at 542 (stating that young computer hackers have received most press coverage).

[35] *See* Dierks, *supra* note 1, at 320-21 (explaining hacker ethics and harmlessness of many hackers). Hacker ethics include the interest in exploring the Internet and creating a perfect system by correcting the Internet's flaws. *See* Clarke, *supra* note 29, at 206-07. Most hackers place high value on sharing information freely. *See* Dorothy E. Denning, *Concerning Hackers Who Break into Computer Systems*, ¶ 20 (visited Nov. 30, 1997) <http://guru.cosc.georgetown.edu/~denning/hackers/Hackers-NCSC.txt>. However, hackers view malicious break-ins such as breaking into hospital systems as morally wrong. *See id.* ¶ 36-37.

[36] *See* S. REP. NO. 104-357, at 9 (1996) (referring to outsiders without authorization as hackers).

[37] *See* Denning, *supra* note 35, ¶ 23. In fact, the creators of Apple and Microsoft developed much of their knowledge by hacking. *See* David F. Geneson, *Recent Developments in the Investigation and Prosecution of Computer Crime*, 301 PLI/PAT 45, 61 (1990) (claiming that Steve Jobs and Steve Wozniak, creators of Apple, and Bill Gates, creator of Microsoft, learned by hacking).

[38] *See* Dierks, *supra* note 1, at 320-21 (explaining harmless intent of most hackers).

On the other hand, profit drives a new breed of computer criminals.[39] They are generally insiders who abuse their authorized access to computer systems.[40] These criminals illegally enter computer systems with an intent to cause damage.[41] Unlike traditional outside hackers, insiders generally possess malicious intent and seek financial gain.[42] Not surprisingly, they cause major losses for business and government.[43]

Whether ill-intended or not, the private sector loses about $550 million per year because of computer criminals.[44] In response to these enormous losses, the private sector has increased security and taken other preventive measures.[45] Additionally, Congress responded by passing CFAA.[46]

C. Mens Rea Requirement Under the 1986 Version of CFAA

In 1984, CFAA criminalized accessing computers without authorization and using illegally obtained information.[47] CFAA

---

[39] *See* Clarke, *supra* note 29, at 219-23 (discussing new computer criminals who break into computer systems for financial gain).

[40] *See id.* at 222 (stating that about 80% of computer criminals are insiders with malicious criminal intent).

[41] *See id.* (discussing insiders and outsiders who commit computer crimes for profit). Although the new breed of criminals includes some outsiders, it primarily consists of company insiders who cause damage for financial or malicious reasons. *See id.* at 221-22 (describing outsiders who start breaking into systems for profit). The outsiders involved in these crimes may be security experts gone astray. *See id.* at 221. Other criminals may be outsiders who infiltrated the computer system by obtaining sufficient information from insiders. *See id.* at 222. Because outsiders use insider information, their method is equivalent to insider exploitation. *See id.*

[42] *See id.* at 223 (stating that certain individuals arguably possess criminal mens rea because they break into computer systems for profit).

[43] *See* Dierks, *supra* note 1, at 320 (stating that losses come from insider abuse); Raskin & Schaldach-Paiva, *supra* note 32, at 542 (indicating that insider crimes have caused far more damage than crimes committed by outsiders).

[44] *See* Dierks, *supra* note 1, at 319 (estimating that unauthorized alteration and theft of computer data results in annual loss of $550 million).

[45] *See generally* Michelle Schoenung, *Protecting Against Hackers*, PC MAGAZINE (Feb. 18, 1997) <http://www.zdnet.com/pemag/issues/1604/pcmg0014.htm> (discussing various products that heighten security). One such security measure is a firewall. *See generally* CERFnet News, *Firewalls: The Network Moat*, (Apr. 1995) <http://www.cerf.net:80/cerfnet/cerfnet_news/firewalls.html> (discussing how firewall works to protect private networks from intrusion).

[46] *See* Raskin & Schaldach-Paiva, *supra* note 32, at 544 (stating that computer-related crimes are federal offenses).

[47] *See* 18 U.S.C. § 1030 (1984).

was a welcomed first step toward fighting computer crimes.[48] However, careful scrutiny by critics soon revealed problems in CFAA, such as its limited scope and vagueness.[49] In efforts to solve these perceived problems, Congress significantly changed CFAA three times over the next twelve years.[50]

Congress first amended CFAA in 1986.[51] The 1986 Act expanded the scope of the 1984 Act by creating three new crimes, including the anti-hacking provision under section 1030(a)(5).[52] Additionally, Congress raised the mens rea requirements from knowingly to intentionally in various sections.[53] By changing the mens rea levels, Congress intended to exclude users who mistakenly accessed computer networks.[54]

However, Congress worded the mens rea requirements for the 1986 Act ambiguously.[55] The anti-hacking provision of the 1986

---

[48] *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 (1990) (stating that leaders in computer industry hailed 1984 Act as important first step to fighting computer crime).

[49] *See* Baker, *supra* note 13, at 65-66 (explaining that critics felt statute was too vague and too limited). A major criticism focused on the limited scope of the legislation, which protected only the federal interests. *See id.* at 66 (stating that Act did not affect access to private computers and computer networks). Furthermore, the Act did not define some key terms. *See id.* Such criticisms led Congress to amend CFAA in 1986. *See id.*

[50] *See* S. REP. NO. 104-357, at 4 (1996) (stating that before 1996, Congress significantly changed CFAA in 1986 and 1994); Griffith, *supra* note 48, at 473, (stating that Congress attempted to address criticisms of 1984 Act in 1986 Act). Congress recently indicated that CFAA will continue to change. *See* S. REP. NO. 104-357, at 5 (stating that 1996 amendment will not likely be final change).

[51] *See* Baker, *supra* note 13, at 66.

[52] *See* 18 U.S.C. § 1030(a)(4)-(6) (1986); Baker, *supra* note 13, at 68-70. The three new crimes are theft of property by using computers, damage to federal interest computers by outsiders, and use of unauthorized passwords. *See id.* However, Congress failed to include crimes by insiders of computer network. *See id.* at 68. These insiders are accountable for most of the computer crimes. *See* Dierks, *supra* note 1, at 320 (commenting that insiders cause most damage). By defining CFAA's offense as accessing a computer "without authorization," Congress excluded insiders of computer networks from potential liability. *See* Raskin & Schaldach-Paiva, *supra* note 32, at 547. Because insiders generally have authorization, CFAA does not apply to them. *See id.* (noting that 1994 Act included insiders without authorization language).

[53] *See* 18 U.S.C. § 1030(a)(2)-(3) (1986); Baker, *supra* note 13, at 68 (stating that subsections (a)(2) and (a)(3) changed mens rea requirement from knowingly to intentionally).

[54] *See* S. REP. 99-432, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2483; *see also* Baker, *supra* note 13, at 68 (explaining that Congress did not believe knowingly level excluded users making careless mistakes).

[55] *See* United States v. Morris, 928 F.2d 504, 509 (2d Cir. 1991) (admitting some ambiguity in 1986 Act's wording and interpreting 1986 Act's mens rea requirement by

Act indicated that a person would be penalized if she "intentionally accesse[d] a Federal interest computer" and "such conduct . . . damage[d]" such computer.[56] Congress placed "intentionally" in front of the access clause but not the damage clause.[57] Because "intentionally" does not appear in front of the damage clause, two circuits have interpreted "intentionally" as modifying only the first phrase, the access clause.[58]

The Second Circuit was the first circuit to interpret the ambiguous mens rea requirement of the 1986 version of CFAA.[59] In *United States v. Morris*,[60] Robert Tappan Morris released a "worm," a type of the malicious code or program,[61] into the Internet.[62] As a first-year graduate student in Cornell University's computer science Ph.D. program, Morris was attempting to demonstrate the weakness of the computer network's security.[63] Although Morris thought the worm was benign,[64] he miscalculated the rate at which the worm would multiply.[65] When Morris realized the miscalculation, he tried to stop the worm by releasing a solution into the Internet.[66] However, he released the solution too late, causing computers around the country to crash.[67]

Despite Morris's efforts to disable the worm, the trial court convicted him under CFAA's intentional standard, and the Second Circuit affirmed his conviction.[68] The Second Circuit

---

looking at grammar and legislative history).

[56] *See* 18 U.S.C. § 1030 (a)(5).

[57] *See id.*

[58] *See Morris*, 928 F.2d at 509; United States v. Sablan, 92 F.3d 865, 868 (9th Cir. 1996) (construing intentional mens rea to only apply to access clause).

[59] *See Morris*, 928 F.2d at 507-09 (admitting ambiguity in 1986 Act's wording, interpreting 1986 Act's mens rea requirement by looking at grammar and legislative history and concluding that it provides no mens rea requirement for damage clause).

[60] 928 F.2d 504 (2d Cir. 1991).

[61] *See id.* at 505 n.1 (noting that worm is computer program which disrupts computer as it migrates from computer to computer, but does not attach itself to any computer); Lawrence E. Bassham & W. Timothy Polk, *Threat Assessment of Malicious Code and Human Computer Threat*, ¶ 4 (visited Nov. 30, 1997) <http://bilbo. isu.edu/security/isl/threat.html> (explaining virus and worms as malicious code).

[62] *See Morris*, 928 F.2d at 505.

[63] *See id.*

[64] *See id.*

[65] *See id.* at 506.

[66] *See id.*

[67] *See id.*

[68] *See id.* at 506, 511. The trial court concluded that Morris violated CFAA because he

held, however, that because the term "intentionally" only applied to accessing a computer system,[69] no mens rea requirement exists for damaging a system.[70] Therefore, under the 1986 Act, even if a person does not intend to damage the computer system, liability will attach if the person intended to access the computer system.[71] The only other circuit to rule on this issue, the Ninth Circuit, recently agreed with the Second Circuit's reasoning.[72]

Congress amended the Act again in 1994 by codifying judicial precedent that clearly criminalized reckless behavior.[73] The 1994 Act also distinguished the different levels of mens rea required for felonies and misdemeanors.[74] The felony

---

intended to access the computer network. *See id.* at 506. His lack of intent to damage the system was irrelevant. *See id.*

[69] *See id.* at 509. The court indicated that the term "intentionally" seems to modify only the access clause and not the damage clause. *See id.* The 1986 Act applies to a person who "intentionally [accesses] a Federal interest computer without authorization, and . . . alters, damages, or destroys information." 18 U.S.C. § 1030(a)(5) (1986). The court also traced the legislative history. *See Morris*, 928 F.2d at 507 (quoting S. REP. NO. 99-432, at 6 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2483). Congress expressed concern that the knowingly standard might encompass the acts of individuals accidentally stumbling into another computer file or system. *See id.* Therefore, the court concluded that the intentional mens rea requirement only applies to the access of the computer system. *See id.* at 509.

[70] *See Morris*, 928 F.2d at 509.

[71] *See id.*

[72] *See* United States v. Sablan, 92 F.3d 865, 868 (9th Cir. 1996) (adopting Second Circuit's reasoning). In *Sablan*, Bernadette H. Sablan broke into her former work site, a bank, by using her old key. *See id.* at 866. Sablan was intoxicated at the time. *See id.* She logged into the bank's mainframe and damaged several bank files. *See id.* The Ninth Circuit Court of Appeals adopted the Second Circuit's reasoning that "intentionally" only applies to the access clause, not the damage clause. *See id.* at 868. The *Sablan* court acknowledged that the punctuation itself is not decisive in construing statutes. *See id.* at 867 (citing Constanzo v. Tillinghast, 287 U.S. 341 (1932)). In interpreting CFAA, the court noted that the 1984 Act contained a mens rea requirement in both the access and the damages clauses. *See id.* at 868. However, Congress chose not to repeat the mens rea requirement for the damage clause in section 1030(a)(5) for the 1986 Act. *See id.* In contrast, other subsections retained the dual-intent language by placing the mens rea requirement in front of both the access and the damage clauses. *See id.* Hence, the court reasoned that in the 1986 Act, Congress intended not to impose an intent requirement in the damage clause. *See id.* Therefore, the intent to access a system suffices for a conviction under the 1986 Act. *See id.*

[73] *See* 18 U.S.C. § 1030(a)(5)(B)(i) (1994) (creating misdemeanor for reckless damage); *see also* Raskin & Schaldach-Paiva, *supra* note 32, at 549 (discussing Congress's affirmance of *Morris*'s judicial reasoning in new sections of 1994 Act).

[74] *See* 18 U.S.C. § 1030(a)(5)(A)-(B).

subsection required knowing and intentional mens rea[75] while the misdemeanor subsection required only reckless mens rea.[76] However, because the 1994 Act was still too limited in scope, Congress amended CFAA yet again in 1996.[77] In these most recent amendments, Congress lowered the mens rea even further.[78]

II. 1996 AMENDMENTS TO CFAA: SECTION 1030(A)(5)

In 1996, Congress amended CFAA and codified the *Morris* court's standard regarding mens rea.[79] The 1996 Act dramatically changed the structure of CFAA.[80] Congress divided section

---

[75] *See id.* § 1030(a)(5)(A)(i).

[76] *See id.* § 1030(a)(5)(B)(i). Additionally, Congress expanded section 1030(a)(5) by including computers used in interstate commerce or communication. *See id.* § 1030(a)(5)(A); Raskin & Schaldach-Paiva, *supra* note 32, at 546. Congress also included insiders as a potentially liable class under CFAA by removing the unauthorized access requirement. *See* 18 U.S.C. § 1030(a)(5)(A). Furthermore, Congress made conduct evincing "reckless disregard of a substantial and unjustifiable risk" of damage to the computer system a misdemeanor. *See id.* § 1030(a)(5)(B), (c)(4) (punishing offense under § 1030(a)(5)(B) for fine, imprisonment up to one year, or both). The 1994 Act also provides for civil remedies as an incentive to report computer crimes. *See id.* § 1030(g); Raskin & Schaldach-Paiva, *supra* note 32, at 547.

[77] *See* S. REP. NO. 104-357, at 4, 10 (1996) (explaining gaps and problems in 1994 Act). Congress perceived at least three significant weaknesses in the Act. *See id.* First, the 1994 Act failed to include intra-state Federal government and financial institution computers, or state, local, and civilian computers. *See id.* at 10. Second, the 1994 Act did not cover any foreign hackers. *See id.* at 4 (describing specific foreign hackers intruding into American computer systems). Third, no protection existed for the loss of computer time. *See id.*

[78] *Compare* 18 U.S.C. § 1030 (a)(5)(A)-(B) (1994) *with id.* § 1030(a)(5)(A)-(C) (1996) (reducing levels of mens rea).

[79] *See id.* § 1030(a)(5)(b), (c)(4); *see also supra* note 73 and accompanying text (describing Congress's actions in 1994 and 1996 to codify *Morris*).

[80] *Compare* 18 U.S.C. § 1030(a)(5)(A)-(B) (1994) *with id.* § 1030(a)(5)(A)-(C) (1996) (altering structure by increasing number of subsections). First, Congress divided the elements into three subsections. *See id.* § 1030(a)(5)(A)-(C) (1996). Congress now punishes whoever:

> (5) (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
> (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
> (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage.

Id. § 1030(a)(5)(A)-(C).
Second, Congress expanded CFAA to cover the broader category of "protected computers"

1030(a)(5) into three subsections,[81] consisting of two felony subsections and one misdemeanor subsection.[82] Each of these subsections contains different mens rea requirements.[83]

The different mens rea requirements of the section 1030(a)(5) subsections reflect Congress's intent to have CFAA cover a broad range of criminals.[84] The first felony subsection penalizes anyone who knowingly transmits harmful programs and intends to cause damage.[85] While all three subsections apply to

---

rather than "a computer used in interstate commerce." *Compare id.* § 1030(a)(5)(A) (1994) *with id.* § 1030(a)(5) (1996). Congress made this change because in the 1994 Act it had inadvertently failed to protect the federal government and certain financial institution computers. *See* S. REP. NO. 104-357, at 10. The protected computers include computers:

> (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
>
> (B) which is used in interstate or foreign commerce or communication.

18 U.S.C. § 1030(e)(2). Third, a new section broadens the definition of "damage" to anticipate future technological advances and harms. *See* S. REP. NO. 104-357, at 11.

[81] *See* 18 U.S.C. § 1030(a)(5)(A)-(C) (1996).

[82] *See id.* § 1030(a)(5)(A)-(B); *see also id.* § 1030(c)(3)(A) (defining § 1030(a)(5)(A) and (a)(5)(B) as felony provisions). Courts can penalize a person convicted for the first time under sections 1030(a)(5)(A) or 1030(a)(5)(B) with a fine, imprisonment up to five years, or both. *See id.* Courts may penalize a person convicted for the first time under section 1030(a)(5)(C) with a fine, imprisonment up to one year, or both. *See id.* § 1030(c)(2)(A). Congress used the same damage element for both the felony and misdemeanor subsections. *See id.* § 1030(e)(8) (defining "damage"). Damage definitions apply to both felony and misdemeanor subsections. *See id.*

[83] *See id.* § 1030(a)(5)(A)-(C) (modifying access and damage clauses in two felony subsections but retaining only one mens rea requirement for misdemeanor subsection). Unlike the 1994 Act, the felony subsections under CFAA include reckless damage as well as intentional damage. *Compare id.* § 1030(a)(5)(A) (1994) (indicating that offenders must intend to cause damage for felony subsection) *with id.* § 1030(a)(5)(A)-(B) (1996) (adding reckless damage for felony offense). The 1994 Act allowed punishment for reckless damage only as a misdemeanor. *See id.* § 1030(a)(5)(B)-(B)(i), (c)(4) (1994). However, CFAA lowered the 1994 Act's mens rea requirement for misdemeanors from reckless damage to no mens rea requirement at all. *See id.* § 1030(a)(5)(C) (1996). Congress, therefore, required intentional access but no mens rea requirement for damage. *See id.* Legislative history shows that Congress wanted to create strict liability for misdemeanors and intentionally left out any mens rea. *See* S. REP. NO. 104-357, at 11 (discussing Congress's intent to punish hackers for any intentional, reckless, negligent, accidental, or other damage).

[84] *See* S. REP. NO. 104-357, at 11 (expressing Congress's intent to capture any hackers, regardless of intent).

[85] *See* 18 U.S.C. § 1030(a)(5)(A). The subsection punishes whoever "knowingly causes the transmission of a program, information, code, or command, and as a result of such

outsiders, this first felony subsection is the only subsection that applies to insiders.[86] However, section 1030(a)(5) excludes innocent insiders altogether.[87]

For example, suppose person *Z* does not know that a particular e-mail message has a virus attached.[88] Therefore, *Z* does not intend to transmit the attached virus to another computer when sending the e-mail, but rather only intends to transmit the e-mail itself.[89] In this case, *Z*'s mental state does not satisfy the knowing part of the first felony subsection's transmission clause. However, *Z* may know that sending an e-mail with a virus attached is harmful.[90] If so, and *Z* also knows a virus is attached to that particular e-mail, then *Z*'s mental state satisfies the knowing part of the first felony subsection's transmission clause.[91]

To be liable under the first felony subsection, *Z* must also intend to cause damage.[92] If *Z* intends to destroy data by transmitting the virus attached to the e-mail, then *Z*'s mental state satisfies the intent part of the damage clause. Thus, *Z* satisfies the mens rea requirements for both the transmission and damage clauses.[93] However, if *Z* does not know that the virus is harmful, then *Z* has not intended to damage the computer. Therefore, although *Z* may intend to send the virus, he has not met the intent requirement of the damage clause.[94]

---

conduct, intentionally causes damage without authorization, to a protected computer." *Id.*

[86] *See* S. REP. NO. 104-357, at 11 (stating that § 1030(a)(5)(A) applies to insiders and outsiders whereas § 1030(a)(5)(B)-(C) only apply to outsiders).

[87] *See id.* (commenting that first felony subsection covers both insiders and outsiders who have specific intent).

[88] *See* Bassham & Polk, *supra* note 61, ¶ 9 (noting that virus is malicious code that replicates itself by attaching copies to existing files).

[89] *See id.* ¶ 33 (discussing worm infection through transmission of e-mail); Dorothy E. Denning, *Protection and Defense of Intrusion*, ¶ 22 (visited Feb. 21, 1994) <http://guru.cosc.georgetown.edu/~denning/infosec/USAFA.html> (noting that malicious codes can be attached to electronic mail).

[90] *See* Bassham & Polk, *supra* note 61, ¶ 33 (explaining that sending e-mail with virus attached will cause damage).

[91] *See* 18 U.S.C. § 1030(a)(5)(A) (1996) (stating that knowing causation is one of two mens rea requirements for this felony).

[92] *See id.* (requiring intentional damage).

[93] *See id.* (requiring both knowing transmission and intentional damage by conjunction).

[94] *See id.*

The second felony and misdemeanor subsections of the 1996 Act differ from the first felony subsection in two ways. Both have lower mens rea requirements than the first felony subsection,[95] and both apply to those who intentionally access a computer system.[96] The second felony subsection applies to hackers who recklessly cause damage[97] while the misdemeanor subsection contains no mens rea requirement for the resulting damage.[98]

Because the second felony and misdemeanor subsections penalize those who illegally access a computer, they apply only to outsiders.[99] For both of these subsections, a person must intend to send an e-mail, visit a website, or otherwise access a particular computer system.[100] For example, suppose *X* has just learned how to use e-mail and has sent an e-mail to a specific address. *X*'s mental state satisfies the requirement of specific intent to access a computer system because *X* intended to access that specific address through an e-mail.[101] If the same e-mail had a virus attached that caused damage, but *X* thought the virus was harmless,[102] *X*'s mental state satisfies the second felony subsection's reckless requirement.[103] If *X* had absolutely no idea that a virus was attached, *X*'s mental state satisfies the misdemeanor subsection, and *X* is guilty without intending to cause any harm.[104]

The second felony and the misdemeanor subsections of the 1996 Act codified *Morris*.[105] Unlike the intentional damage requirement of the first felony subsection,[106] the second felony

---

[95] *See id.* § 1030(a)(5)(B)-(C) (imposing either recklessness as mens rea requirement or no mens rea requirement for damage).

[96] *See id.* (requiring intentional access).

[97] *See id.* § 1030(a)(5)(B).

[98] *See id.* § 1030(a)(5)(C).

[99] *See* S. REP. NO. 104-357, at 10-11 (1996) (describing how subsections impact only outsiders by using term "access").

[100] *See* Denning, *supra* note 89, ¶ 22 (discussing transmission of malicious code through web browsers and execution of malicious codes without user's knowledge).

[101] *See* 18 U.S.C. § 1030(a)(5)(B) (requiring specific intent). CFAA provides for punishment only if the computer system that the criminal accesses is a protected computer as specifically defined in CFAA. *See id.* § 1030(e)(2).

[102] *See* Bassham & Polk, *supra* note 61, ¶ 18 (explaining that benign viruses exist).

[103] *See* 18 U.S.C. § 1030(a)(5)(B) (requiring only reckless intent to damage computer).

[104] *See id.* § 1030(a)(5)(C) (containing no mens rea requirement for damage).

[105] *See supra* notes 55-72 and accompanying text (discussing cases resolving ambiguous mens rea requirements in 1986 Act).

[106] *See* 18 U.S.C. § 1030(a)(5)(A) (requiring knowing transmission and intentional dam-

subsection requires the much lower mens rea level of recklessness.[107] The misdemeanor subsection requires no mens rea at all for the damage clause.[108] Therefore, although the first and second felony subsections differ greatly in the intent requirements,[109] only a small difference exists between the second felony and misdemeanor subsections.[110]

The punishment levels, however, fail to accurately reflect these different mens rea requirements.[111] While the second felony and misdemeanor subsections have a lower mens rea requirement, both still entail harsh punishments.[112] In particular, although the second felony subsection has a lower mens rea requirement than the first felony subsection, the same level of punishment exists for both.[113] Regarding the misdemeanor subsection, the punishment for a first time offender is less harsh.[114] For example, the heaviest sentence a court can impose on a first time offender under the misdemeanor subsection is only a year of imprisonment and a fine.[115] Nevertheless, the 1996 Act created equally harsh punishments for repeat offenders under the misdemeanor subsection and the felony subsections.[116]

---

age).

[107] *See id.* § 1030(a)(5)(B) (requiring reckless damage).

[108] *See id.* § 1030(a)(5)(C).

[109] *Compare id.* § 1030(a)(5)(A) (requiring intentional damage for first felony) *with id.* § 1030(a)(5)(B) (imposing only reckless damage for second felony).

[110] *See supra* notes 88-104 and accompanying text (illustrating differences in mens rea requirements through hypotheticals).

[111] *See* 18 U.S.C. § 1030(c)(2)(A), (3)(A)-(B) (requiring different levels of punishment). A person convicted of a felony for the first time can be imprisoned for up to five years, fined, or both. *See id.* § 1030(c)(3)(A). A person convicted under the misdemeanor subsection for the first time can be imprisoned for up to a year, fined, or both. *See id.* § 1030(c)(2)(A). However, a person convicted more than once under any felony or misdemeanor can be imprisoned up to 10 years, fined, or both. *See id.* § 1030(c)(3)(B).

[112] *See supra* note 26 and accompanying text (discussing degree of blameworthiness associated with different levels of mens rea); *see also supra* note 111 and accompanying text (stating levels of punishment for each section).

[113] *See* 18 U.S.C. § 1030(a)(5)(A)-(B), (c)(3)(A) (stating that conviction under either § 1030(a)(5)(A) or (a)(5)(B) can result in punishment of up to five years, fine, or both). *Compare id.* § 1030(a)(5)(A) (requiring intentional damage for first felony) *with id.* § 1030(a)(5)(B) (allowing reckless damage for second felony). The same subsection covers the punishment of both felonies. *See id.* § 1030(c)(3)(A).

[114] *See id.* § 1030(c)(2)(A) (imposing penalty of up to one year in prison, fine, or both).

[115] *See id.*

[116] *See id.* A first misdemeanor offense results in up to one year imprisonment, a fine, or

III. ANALYSIS OF SECTION 1030(A)(5) OF THE 1996 ACT

CFAA as amended in 1996 sparks pertinent public policy concerns. First, the new mens rea requirements impact insiders and outsiders differently.[117] Second, the new mens rea requirements will probably discourage private security measures.[118] In light of these public policy concerns, Congress should amend CFAA to adopt uniformly high mens rea requirements.[119]

A. Impact of Mens Rea Requirements in Section 1030(a)(5)

In 1996, Congress amended CFAA to require either high or low mens rea, depending upon the offense.[120] Congress intended that CFAA have differing impacts on the prosecution of insiders and hackers through different mens rea levels.[121] Although Congress excluded innocent insiders from prosecution under CFAA, it included both innocent and guilty outsiders, or hackers, as well as guilty insiders seeking illegal gains.[122]

The high mens rea requirement in the first felony subsection limits the prosecution of insiders to those with intent to damage a computer system.[123] Therefore, innocent insiders are not liable under this subsection.[124] One can see the impact of this

---

both. *See id.* A repeat felony or misdemeanor offense results in punishment of up to 10 years, a fine, or both. *See id.* § 1030(c)(3)(B).

[117] *See infra* notes 120-33 and accompanying text (discussing impact of lower mens rea).

[118] *See infra* notes 155-80 and accompanying text (discussing private security policy and impact that low mens rea would have on private security measures).

[119] *See infra* notes 139-80 and accompanying text (discussing public policy and advocating that legislature change mens rea requirement in CFAA to intentional mens rea requirements).

[120] *Compare* 18 U.S.C. § 1030(a)(5)(A)-(B) (requiring intentional or reckless mens rea for damage in felony subsection) *with id.* § 1030(a)(5)(C) (requiring no mens rea for damage in misdemeanor subsection).

[121] *See* S. REP. NO. 104-357, at 11 (1996) (discussing Congress's intent to protect innocent insiders but not innocent outsiders from prosecution).

[122] *See id.*

[123] *See* 18 U.S.C. § 1030(a)(5)(A) (requiring intentional damage); S. REP. NO. 104-357, at 11 (indicating that insiders face criminal liability only if they intentionally cause damage).

[124] *See* S. REP. NO. 104-357, at 11 (discussing prosecution of insiders who have intent to damage). Congress intended to protect only the innocent users who are also insiders. *See id.* (explaining that Congress wanted to punish outsiders for any reckless, negligent, or accidental damages, but not to punish insiders for negligent or reckless damage). Congress had previously opted for the intentional standard to protect innocent users without discriminating against outsiders. *See* S. REP. NO. 99-432, at 5-6 (1986), *reprinted in* 1986

change by applying the new mens rea requirements to the *Morris* case. If Morris was an insider, the government could not prosecute him under the first felony subsection of CFAA because he had no intent to cause damage.[125]

Congress, however, excluded innocent insiders from CFAA's coverage.[126] As to outside hackers, innocent or not, CFAA allows prosecution under the entire spectrum of mens rea levels.[127] Therefore, any innocent hacker who stumbles into someone else's computer file or computer data by accident may be strictly liable.[128] Since Morris was an outsider, a court could still convict him under the second felony subsection and the misdemeanor subsection.[129]

Thus, CFAA impacts insiders and outsiders differently through the 1996 Act's mens rea requirements.[130] The high mens rea

---

U.S.C.C.A.N. 2479, 2483 (stating Congress's intent to protect innocent users from prosecution by using highest mens rea).

[125] *See* United States v. Morris, 928 F.2d 504, 505-06 (2d Cir. 1991) (indicating that Morris possessed no intent to cause damage); *supra* note 124 and accompanying text (explaining that Congress did not intend to protect innocent outsiders). Because Morris was an outsider, the government could prosecute him under the second felony subsection or the misdemeanor subsection, both of which have lower mens rea requirements. *See* 18 U.S.C. § 1030 (a)(5)(B)-(C) (requiring only reckless damage for felony and no mens rea requirement for damage in misdemeanor).

[126] *See supra* note 124 and accompanying text (explaining Congress's intent toward insiders and outsiders).

[127] *See* 18 U.S.C. § 1030(a)(5)(A)-(C) (criminalizing intentional, reckless damage, or any damage); S. REP. NO. 104-357, at 11 indicating that Congress wanted to catch any outside hackers). Congress intended to criminalize all computer trespass, which includes accidental or negligent damage. *See id.* But in 1986, Congress wanted to limit the prosecution of both insiders and outsiders to those with specific intent. *See* S. REP. NO. 99-432, at 5-6 (expressing concern to limit prosecution without differentiating insiders and outsiders).

[128] *See* S. REP. NO. 104-357, at 11 (indicating that outside hackers may never be innocent). According to Congress, only the "intentional act of trespass" matters in determining criminality. *See id.* Even if unintentional damage occurs, Congress intended to punish outside hackers for trespassing. *See id.* Congress believed that requiring intentional or reckless damage would invite hackers to break into computer systems. *See id.*; *see also* 18 U.S.C. § 1030(a)(5)(C) (imposing no mens rea requirement for misdemeanor).

[129] *See* 18 U.S.C. § 1030(a)(5)(B)-(C) (requiring only reckless damage for felony and imposing no mens rea requirement for misdemeanor). The current CFAA's low mens rea requirements in the second felony subsection and the misdemeanor subsection allow the government to prosecute innocent hackers. *See id.; cf. Morris*, 928 F.2d at 506 (stating that Morris had no intent to damage computer system).

[130] *See* S. REP. NO. 104-357, at 10-11.

requirement excludes innocent insiders.[131] However, low mens rea requirements allow courts to prosecute innocent hackers.[132] The impact of low mens rea requirements on hackers reflects Congress's failure to address major policy implications.[133]

B. Public Policy and the Significance of Mens Rea in CFAA

CFAA and its low mens rea requirements reflect Congress's concern about computer crimes and hackers.[134] Congress enacted CFAA hoping to punish as many computer criminals as possible.[135] However, CFAA currently ignores two policy implications in its zeal to rid the Internet of computer criminals.[136] First, CFAA fails to protect innocent outside users.[137] Second, CFAA does not encourage the private sector to protect itself.[138] A careful exploration of these policies will demonstrate the importance of high mens rea requirements.

---

[131] *See id.*; *see also* 18 U.S.C. § 1030(a)(5)(A).

[132] *See* S. REP. NO. 104-357, at 11 (discussing Congress's intent to prosecute all hackers); *see also* 18 U.S.C. § 1030(a)(5)(B)-(C) (criminalizing conduct of outsiders if they recklessly or intentionally cause damage).

[133] *See infra* notes 134-80 and accompanying text (discussing public policy issues).

[134] *See* S. REP. NO. 104-357, at 11 (implying that criminalizing all computer trespass will send appropriate message to hackers). A Senate report that explains the change in mens rea requirements and the need to catch hackers illustrates Congress's concern:

> Although those who intentionally damage a system, without authority, should be punished regardless of whether they are authorized users, it is equally clear that anyone who knowingly invades a system . . . should be punished as well, even when the damage caused is not intentional. In such cases, it is the intentional act of trespass that makes the conduct criminal. To provide otherwise is to openly invite hackers to break into computer systems . . . . Rather than send such a dangerous message . . . , it is better to ensure that section 1030(a)(5) criminalizes all computer trespass.

Id.

[135] *See* 18 U.S.C. § 1030(a)(5)(B)-(C) (imposing low mens rea requirement, whether reckless or intentional, for damage); *supra* note 84 and accompanying text (discussing Congress's intent to punish hackers).

[136] *See infra* notes 139-80 and accompanying text (discussing policies other than punishing all computer criminals).

[137] *See* S. REP. NO. 99-432, at 21 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2494 (stating that intentional standard will preclude criminal liability for inadvertent acts). In 1986, Congress did consider such a policy and wanted CFAA to cover only those who evince a clear intent. *See id.*

[138] *See infra* notes 155-77 and accompanying text (discussing how low mens rea may reduce private sector's incentive to take security measures).

1. Protecting Innocent Users

In setting mens rea requirements, Congress should seek to avoid incarcerating innocent people.[139] The legislative history of CFAA indicates that the policy of excluding innocent users played a vital role in setting the mens rea requirements in the 1986 Act.[140] This policy is consistent with the idea that we punish the guilty because society demands retribution.[141] By requiring intentional mens rea, Congress effectively excludes innocent users and addresses the underlying concern of retribution.[142]

Critics may argue that low mens rea requirements are not inconsistent with the goals of retribution.[143] They may reason that all hackers intend to do wrong because they intend to break into computer systems.[144] Therefore, they may conclude that requiring low mens rea requirements does not violate retributive goals because hackers are not innocent users.[145]

However, few outside hackers intend to cause damage.[146] In fact, most hackers break into systems to learn or to challenge themselves.[147] Strict hacker ethics prohibit hackers from

---

[139] *See* Charles Victor Lang, Note, *Stolen Bytes: Business Can Bite Back*, 1986 COLUM. BUS. L. REV. 251, 253 (1986) (explaining that our society would rather let 10 guilty persons escape than punish one innocent person).

[140] *See* S. REP. NO. 99-432, at 21 (expressing desire to exclude inadvertent users by setting highest mens rea requirement).

[141] Because people should receive punishment when they truly deserve it, retribution theory forbids punishment when people do not deserve it. *See* WAYNE R. LAFAVE & AUSTIN W. SCOTT, JR., CRIMINAL LAW § 1.5(a)(6) (2d ed. 1986). Retribution requires criminals to have chosen to do wrong. *See* Nelson, *supra* note 29, at 307.

[142] *See infra* notes 151-54 and accompanying text (discussing policy to exclude innocent users).

[143] *See* Nelson, *supra* note 29, at 307 (stating that retribution requires criminals' intent to do wrong).

[144] *See* Dierks, *supra* note 1, at 310 n.7 (stating that term "hacker" is synonymous with computer criminal and carries strong negative connotations). Most hackers, however, lack the requisite malicious intent. *See* Clarke, *supra* note 29, at 206-08 (describing hackers as those who exhibit playful cleverness and intellectual exploration of Internet); Denning, *supra* note 35, ¶ 23 (stating that hackers break into systems to learn). In fact, most Internet users maintain the mentality of freely exchanging information and exploring the Internet as if it were a big library. *See* Rebecca Quick, *Web Sites Find Members Don't Keep Secrets*, WALL ST. J., Feb. 21, 1997, at B1 (discussing how commercial users trade passwords to share information and explaining mentality of Internet users).

[145] *See generally* Clarke, *supra* note 29 (describing evolution of criminal intent among hackers and how some of them transformed into malicious hackers).

[146] *See supra* notes 35-38 and accompanying text (discussing harmless motives of most hackers).

[147] *See* Clarke, *supra* note 29, at 207 (discussing hackers' intent to exercise intellect by

damaging the accessed systems.[148] These types of hackers possess a lower level of mens rea and should be punished less than those with the intent to damage. However, the 1996 Act includes not only hackers who truly intend to cause damage, but even the outsiders who accidentally cause damage.[149] By punishing hackers who lack criminal intent in the same manner as those who possess criminal intent, Congress has overlooked the goal of retribution.[150]

To effectively address retributive goals, Congress should use the lower mens rea requirements to target only those outsiders possessing the intent to damage.[151] In 1986, Congress addressed this policy by increasing the mens rea level from knowing to intentional and, thus, excluding innocent users.[152] In fact, Congress worried that a mens rea requirement lower than the intentional standard might allow the government to prosecute users who had no criminal intent.[153] Congress should continue to maintain the policy of excluding innocent users by amending CFAA to require uniformly high mens rea. In so doing, Congress will better address the retributive goal behind the enforcement of CFAA.[154]

---

exploring Internet fully and eliminating flaws in systems); Denning, *supra* note 35, ¶¶ 23, 31-32, 35 (describing hackers' innocent motives).

[148] *See* Denning, *supra* note 35, ¶¶ 36-37 (commenting that hackers strive to avoid damaging or deleting any files).

[149] *See* S. REP. NO. 104-357, at 11 (1996) (stating that low mens rea reflects Congress's desire to catch even outside hackers who negligently or accidentally cause damage).

[150] *See* Nelson, *supra* note 29, at 307 (noting that in absence of criminal's choice to do wrong, no evil has been committed and no retribution is owed). CFAA imposed the same punishment on hackers who intentionally cause damage and those who recklessly cause damage. *See* 18 U.S.C. § 1030(c)(3)(A)-(B) (1996).

[151] *See supra* notes 139-42 and accompanying text (discussing heightened mens rea requirements and their underlying considerations); *see also* Clarke, *supra* note 29, at 219-23 (discussing specific criminal intent that new breed of malicious hackers possess). Additionally, punishing users making mistakes will have no deterrent effect. *See* Adams, *supra* note 32, at 426-27 (stating that 1984 Act did not result in greater number of prosecutions although it had lower mens rea requirement than 1986 Act).

[152] *See* S. REP. NO. 99-432, at 21 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2494 (expressing intent to exclude inadvertent users by setting highest mens rea requirement). In crafting CFAA in 1986, Congress tried to exclude any users who may have accidentally "stumbled into" somebody else's computer files or data on the system. *See id.*

[153] *See id.*

[154] *See supra* notes 149-51 and accompanying text (stating that present mens rea requirements fail to meet retributive goals).

2. Encouraging Private Security Measures

A second policy consideration requires Congress to encourage private security measures.[155] Because of government's limited ability to police the Internet, private security measures are more practical and efficient at preventing computer crimes than federal criminal enforcement.[156] Indeed, Congress has acknowledged that the private sector will be more secure if the private sector takes preventive measures itself.[157]

The federal government faces a number of practical obstacles in enforcing CFAA.[158] Unlike traditional crimes, computer crimes are hard to detect.[159] Additionally, victims may not report computer crimes because they fear resulting embarrassment or negative publicity.[160] The low enforcement rates of computer crimes reflect these practical limitations.[161] Therefore, the most effective way to combat computer crimes is through private security measures.[162]

---

[155] *See* S. REP. NO. 99-432, at 3 (expressing Congress's desire to encourage private security measures).

[156] *See id.* (stating that private sector can most effectively prevent computer crime through security). Congress encouraged educational programs and security improvements in the private sector to prevent and deter computer crimes. *See id.*

[157] *See id.*

[158] *See infra* notes 159-61, 166-67 and accompanying text (discussing practical limitations).

[159] *See* Dierks, *supra* note 1, at 332-33 (stating problems that transient nature of information creates). Unlike the real world, cyberspace exists without physical limits, and information can be replicated with little detection. *See id.* at 332-36 (discussing reasons for difficulty in detecting computer crimes). Because hackers connect into the computer system, they are virtually untraceable. *See* Bassham & Polk, *supra* note 61, ¶ 70. Additionally, hackers use technology to hide their identity, activities, and location. *See* Denning, *supra* note 89, ¶ 25 (explaining methods of hiding criminal's identity). The basic problem in detection lies in the complete anonymity that hackers can assume. *See* Bryan Frink, *Computer-Crime: The Computer Fraud and Abuse Act: Taking a Byte Out of Crime?*, ¶ 53 (visited Nov. 30, 1997) <http://www.libraries.wayne.edu/~jlitman/pfrink.html>.

[160] *See* Griffith, *supra* note 48, at 485-86 (giving reasons for under-reporting of computer crimes). Another factor that deters reporting is low cost-effectiveness of prosecution. *See id.*

[161] *See* Dierks, *supra* note 1, at 329-30 (noting that few computer abusers were prosecuted); *see also* Adams, *supra* note 32, at 426-27 (stating that 1984 Act did not result in greater number of prosecutions than 1986 Act despite lower mens requirements). Additionally, because many hackers are juveniles, the government may have problems prosecuting them. *See* Robert J. Sciglimpaglia, Jr., Comment, *Computer Hacking: A Global Offense*, 3 PACE Y.B. INT'L L. 199, 208 (1991).

[162] *See* Dierks, *supra* note 1, at 336-42 (proposing ex-ante measures as appropriate legislation to combat computer crimes). *See generally* Denning, *supra* note 89 (describing differ-

Private security measures may also lower the computer crime rate by allowing the government to spend its resources more efficiently.[163] The policy of encouraging private policing of computer systems may not materialize if the federal government pursues all computer criminals regardless of their intent.[164] The private sector may falsely assume that private security is unnecessary.[165] Additionally, the lower mens rea requirements may spread the resources for enforcement too thin.[166] Therefore, the federal government will be less likely to find hard-to-catch criminals.[167] Instead, the low mens rea requirement will increase the conviction rates for relatively harmless and less sophisticated computer users.[168]

Critics may argue that the incentive for private policing will remain unaffected even if the government pursues all types of computer criminals.[169] They might reason that regardless of the government's enforcement rate, the private sector will continue to lose money from computer criminals breaking into computer systems.[170] Thus, these critics may conclude that private security will remain a constant, regardless of the government's efforts.[171]

---

ent security measures); Schoenung, *supra* note 45 (discussing various products that heighten security).

[163] *See* Dierks, *supra* note 1, at 341-42 (describing possible efficiency gains from mandating preventive security); Griffith, *supra* note 48, at 484, 487-90 (stating that federal law enforcement resources are scarce and recommending legislation requiring private security measures and mandatory reporting).

[164] *See* Dierks, *supra* note 1, at 341-42 (advocating more computer security rather than new computer crime legislation); *see also* Griffith, *supra* note 48, at 484 (stating that because federal law enforcement resources are scarce, federal government needs to use resources efficiently).

[165] *See infra* notes 172-74 and accompanying text (discussing private sector's limited resources in security measures).

[166] *See* Griffith, *supra* note 48, at 484 (stating that federal enforcement has limited resources which should be spent efficiently).

[167] *See* Adams, *supra* note 32, at 426-27 (stating that 1984 Act did not result in more prosecutions than 1986 Act despite lower mens rea requirement).

[168] *See* S. REP. NO. 104-357, at 10-11 (1996) (indicating Congress's desire to punish innocent hackers by lowering mens rea requirement).

[169] *But see* Denning, *supra* not 89, ¶ 6 (stating that organizations do not demand perfect security and may, therefore, take risks).

[170] *See* Dorothy E. Denning, *Postscript to Concerning Hackers Who Break into Computer Systems*, ¶ 2 (visited Nov. 30, 1997) <http://guru.cosc.georgetown.edu/~denning/hackers/Hackers-Postscript.txt> (discussing disruptions that hacking causes and costs of restoring systems).

[171] *But see id.* ¶ 3 (noting that real world constraints and budgets limit investments in

However, this argument overlooks the fact that the private sector has limited resources.[172] Because of these limited resources, the private sector is willing to take risks.[173] The government's higher conviction rates for less dangerous computer criminals may deter the private sector from taking all possible preventive measures possible.[174]

By requiring the highest mens rea standards possible, the government will send a clear signal to private industry that it should take the most stringent measures.[175] This increased security would deter hacking for profit.[176] Furthermore, freed from the costs of prosecuting users not intending to cause damage, the government can focus its resources more efficiently on more destructive computer criminals.[177]

CFAA's low mens rea requirements fail to address the policies of excluding innocent users from prosecution and of encouraging the private sector to take preventive measures.[178] Both policy considerations strongly support adopting the intentional mens rea requirement.[179] Addressing these concerns through a high mens rea requirement will uultimately help to reduce computer crime.[180]

---

security).

[172] *See* Denning, *supra* note 89, ¶ 7 (stating that organizations and system developers have limited resources).

[173] *See id.* ¶¶ 6-7 (stating that organizations take risks and resources are limited).

[174] *See* Dierks, *supra* note 1, at 335-37 (proposing mandatory preventive measures to lower crime). Congress can only achieve a socially optimal enforcement rate through appropriate mens rea levels by considering factors such as private information cost and the optimal level of private investment. *See* Jeffrey S. Parker, *The Economics of Mens Rea*, 79 VA. L. REV. 741, 769-77 (1993) (explicating economic model of mens rea and socially optimal enforcement). Therefore, in setting the appropriate mens rea level, Congress should consider the resulting behavior of the private sector.

[175] *See* S. REP. NO. 99-432, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2481 (indicating that most computer crimes can be prevented privately). *See generally* Dierks, *supra* note 1 (proposing federal legislation requiring private security); Griffith, *supra* note 48 (arguing that requiring private sector to protect itself will heighten its awareness of need for computer security).

[176] *See* Sciglimpaglia, *supra* note 161, at 241 (indicating that better security would deter hackers).

[177] *See* Griffith, *supra* note 48, at 484 (stating that federal law enforcement has scarce resources).

[178] *See supra* notes 134-77 and accompanying text (explaining policy considerations and how present CFAA fails to address them because of its low mens rea requirements).

[179] *See supra* notes 134-77 and accompanying text (discussing policies and advocating high mens rea requirements).

[180] *See* Griffith, *supra* note 48, at 485-87 (stating that Congress failed to acknowledge

CONCLUSION

CFAA punishes hackers.[181] In particular, because of its low mens rea requirements, section 1030(a)(5) establishes a heavy penalty against cyberspace intruders who do not intend to cause damage.[182] Such low mens rea requirements, however, fail to consider some important policies. First, Congress should exclude innocent users from prosecution. Second, the private sector, rather than the federal government, should take security measures to prevent computer crimes. Therefore, Congress should adopt the intentional mens rea requirement to effectively address these important policy concerns.

Haeji Hong

---

other ways to deter computer crimes).

[181] *See* 18 U.S.C. § 1030(a)(5)(A)-(C) (1996).

[182] *See id.* § 1030(c)(3)(A).