The Failure of the Computer Fraud and Abuse Act: Time to Take an Administrative Approach to Regulating Computer Crime

*Ric Simmons**

Abstract

Whenever a legislature creates a technology-specific crime, it faces a number of challenges. First, there is a risk that the new statute will merely duplicate existing crimes, thus over criminalizing the conduct and creating unnecessary confusion. Second, the legislature needs to ensure that it provides the proper guidance to prosecutors, citizens, and courts regarding the new concepts in the criminal statute. And finally, the legislature needs to ensure that the law can be amended and updated as the technology evolves.

The Computer Fraud and Abuse Act ("CFAA") is an example of a technology-specific criminal statute that fails all of these tests. Much of the CFAA is comprised of fraud, extortion, and theft provisions which prohibit conduct already covered by existing laws (or could be covered through minor changes to those laws). The only truly unique aspects of the CFAA are the concepts of "access" and "trespass," while other terms, such as "loss," "damage," and "authorization," need to be given specific meanings in the context of computer misuse. Unfortunately, the CFAA fails to adequately define any of these terms. And although Congress has amended the CFAA numerous times over the past thirty years, it has still been unable to keep up with the fast pace of technological change in this area.

The best solution to this problem is for Congress to stop trying to regulate computer misuse directly through legislation, and instead empower an administrative agency to set more detailed and technical rules. An administrative agency would have a number of advantages over legislatures and courts because it could develop and apply expertise in setting rules, generate and enforce separate rules for civil and criminal liability, respond quickly in creating or changing rules in response to changing conditions, and be insulated from political pressures.

Table of Contents

* Chief Justice Thomas J. Moyer Professor for the Administration of Justice & Rule of Law, Moritz College of Law at The Ohio State University. The Author would like to thank Angela Lloyd, Matthew Klugman, Michael J. Madison, Michael Levy, and the other participants in the Symposium for their comments and feedback on this Article. Also, thanks to Sara Coulter for excellent help tracking down sources. And finally, thanks to Orin Kerr and *The George Washington Law Review* for sponsoring the Symposium.

December 2016 Vol. 84 No. 6

INTRODUCTION

New technology frequently enables new criminal activity. The invention of the telephone led to wiretapping, while the invention of the automobile led to driving while intoxicated. Frequently, however, the "new" crime being committed with novel technology is merely a different version of an existing crime that has already been illegal for decades or even centuries.[1] Given time, police, prosecutors, and courts will use pre-existing traditional criminal laws to address this new criminal activity. Unfortunately, legislatures eager to keep the criminal code "current" often respond by passing new (and unnecessary) laws to ensure the new crimes are covered.

This legislative overreaction produces a number of negative consequences. Technology-specific crimes unnecessarily expand and complicate the criminal code.[2] They can also lead to overbroad or ambiguous laws as legislatures scramble to cover all possible harmful activity associated with a new technology before they truly understand how the technology is used and how it impacts society. Also, the new technology's swift evolution means that any law prohibiting a particular use of that technology must be updated frequently. Legislatures, however, do not always act swiftly and rarely have the technical expertise to understand how the technology is evolving.[3]

Thus, when a new technology is used to facilitate crime, legislatures should engage in a two-step process. First, the legislature must

---

1 For example, before the automobile was widespread, most states had statutes prohibiting reckless endangerment, which could have been interpreted (or slightly amended) to encompass reckless driving. *See* DUI: CRIME AND CONSEQ. IN TENN. § 14:12 (2015–2016 ed.), Westlaw (database updated Dec. 2015) (stating that Tennessee's reckless driving statute requires the use of a vehicle while felony reckless endangerment does not; however, a motor vehicle can be considered a deadly weapon, which means that a defendant can be prosecuted under either offense).

2 *See* Sara Sun Beale, *The Many Faces of Overcriminalization: From Morals and Mattress Tags to Overfederalization*, 54 AM. U. L. REV. 747, 755 (2005) (noting the "unprecedented expansion of the federal criminal code in recent years"); William J. Stuntz, *The Pathological Politics of Criminal Law*, 100 MICH. L. REV. 505, 513–14 (2001) (noting the increase in the Illinois Criminal Code from 131 crimes in 1856 to 421 in 2000).

3 *See* John P. Dwyer, *The Pathology of Symbolic Legislation*, 17 ECOLOGY L.Q. 233, 306 (1990) (stating that "[a]gencies have the technical expertise and knowledge, which courts and legislatures often lack, to evaluate the 'workability' of statutes").

ask whether there is anything truly unique about the criminal activity being committed with the new technology. If the conduct is already covered by existing law, the legislature need not create a new criminal statute,[4] although it may need to add a new term or broaden a definition in the existing law.[5] Second, if the conduct is not covered, the legislature should determine the best way to develop a new criminal prohibition and maintain its relevance in the face of rapidly changing technology. Frequently, the best option is not to pass a new criminal statute, but instead to delegate the role to an administrative agency.

The Computer Fraud and Abuse Act ("CFAA"),[6] which Congress passed in the 1980s[7] in response to the growing use and abuse of computers, provides an illustrative example of this phenomenon. This Article uses the CFAA as a case study by examining which parts of the CFAA were necessary to respond to new crimes, and by demonstrating that the CFAA has failed to keep pace as computers have become more sophisticated and ubiquitous, and as society's norms in relation to those computers transform. This Article concludes that most of the provisions in the CFAA are an unnecessary duplication of existing crimes, while the few necessary provisions have failed to provide appropriate guidance to courts. Thus, the CFAA represents a classic example of legislative overreaction to crimes committed using an emerging technology.

---

4 For example, many states have a criminal law prohibiting both reckless endangerment and reckless driving even though the behavior forbidden by the reckless driving statute is frequently already covered by the reckless endangerment statute. *Compare* CONN. GEN. STAT. ANN. § 14-222 (West 1990) (reckless driving), *with* CONN. GEN. STAT. ANN. § 53a-63 (West 1971) (reckless endangerment).

5 For example, the development and use of credit cards enabled criminals to steal credit card numbers and other intangible items of value so some jurisdictions responded by creating an entirely new crime to cover theft of credit cards, *see, e.g.*, VA. CODE ANN. § 18.2-192 (West 1975), however, other jurisdictions found there was nothing particularly distinct about these thefts other than the fact that the item being stolen was intangible so they responded by merely broadening the definition of "property" in their existing theft statutes, *see, e.g.*, UTAH CODE ANN. § 76-6-401(1) (West 1973) ("'Property' means anything of value, including . . . intangible personal property.").

6 Computer Fraud and Abuse Act (CFAA) of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030 (2012)).

7 Technically, the CFAA was passed in 1986, but the first federal crimes with regard to computer misuse were included in the Comprehensive Crime Control Act of 1984. *See* Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, 98 Stat. 1976 (codified as amended in scattered sections of 18 U.S.C.); Counterfeit Access Device and Computer Fraud and Abuse Act (CADCFAA) of 1984, Pub. L. No. 98-473, 98 Stat. 2190 (codified as amended at 18 U.S.C. § 1030 (2012)). The 1986 Act updated and broadened the criminal liability that Congress first set out in 1984. *See* CFAA of 1986, 100 Stat. 1213.

Part I of this Article evaluates the provisions of the CFAA, concluding that only the "damages" and "trespass" aspects of the CFAA are necessary. Part II argues that Congress failed to define these new terms properly, leading to confusion in the courts and instances of abuse by prosecutors. Finally, Part III explores the possibility of using an administrative agency to promulgate rules prohibiting "computer misuse" more effectively than Congress has done with the CFAA.

I. The Need for "Computer-Specific" Crimes

When new technologies create new opportunities for criminal behavior, legislatures have four possible ways to respond: (1) do nothing, (2) make minor changes to existing laws, (3) enhance the punishment if the new technology is used in committing the crime, or (4) create an entirely new crime.

In many cases, the legislature need not do anything at all because the existing criminal laws cover the new criminal behavior. A nineteenth century statute prohibiting murder can be used to prosecute a killer in the twenty-first century, even if the modern criminal used a weapon that had not existed at the time the statute was written. Similarly, a person who engages in fraud over the telephone can be convicted under fraud statutes passed before telephones were invented.

In some cases, the legislature may need to make minor changes to a criminal statute to ensure that the technology-enabled criminal activity is covered. Aggravated assault statutes may define "assault with a deadly weapon," and then provide a list of weapons that are included.[8] The emergence of new weapons such as Taser guns or pepper spray will force a legislature to amend the definition of "deadly weapon" in order to remove any ambiguity about whether the new weapons are covered.[9]

In other situations, the legislature may believe that committing an existing crime using a new technology makes the crime more severe and thus deserving of greater punishment. For example, a legislature may decide that harassment over the telephone causes more social harm than face-to-face harassment, and thus create a new statute that enhances the punishment when a telephone is used.[10]

---

8 *See, e.g.*, Ohio Rev. Code Ann. § 2903.11 (West 2011) (felonious assault); Ohio Rev. Code Ann. § 2923.11(A) (West 2015) (defining "deadly weapon").

9 *See, e.g.*, Md. Code Ann., Dangerous Weapons § 4-101(a)(3)(i) (West 2016) (defining "pepper mace").

10 *Compare, e.g.*, N.Y. Penal Law § 240.20 (McKinney 1967) (threatening someone in

Finally, there are some cases in which the legislature decides that an entirely new law is required because the technology enables a new form of criminal activity which is unregulated by existing criminal laws. For example, the invention of the automobile enabled the crime of driving while intoxicated. In theory, legislatures could have done nothing and allowed the broader crime of reckless endangerment to cover this activity.[11] However, the particular aspects of the crime—which include setting out specific levels of blood alcohol to determine whether a crime occurred and the degree of the infraction—meant that a new statute was required.[12]

Some commentators[13] and legislators[14] believe computer crime fits into this last category. Over thirty years ago, when Congress inserted the first computer crime provisions in the Comprehensive Crime Control Act,[15] its primary purpose was to ensure that prosecutors had the necessary tools to combat computer crime.[16] Specifically, Congress stated the criminal justice system was "bound by traditional legal machinery which in many cases may be ineffective against un-

---

person with the intent to harass is a mere violation), *with* N.Y. PENAL LAW§ 240.30 (McKinney 1967) (threatening a person over the telephone with intent to harass is a class A misdemeanor).

11 *See, e.g.*, TENN. CODE ANN. § 39-13-103(a) (West 2016) ("A person commits an offense who recklessly engages in conduct that places or may place another person in imminent danger of death or serious bodily injury.").

12 *See, e.g.*, TENN. CODE ANN. § 55-10-401 (West 2016).

13 *See, e.g.*, Carol R. Williams, Note, *A Proposal for Protecting Privacy During the Information Age*, 11 ALASKA L. REV. 119, 119 (1994) ("While conventional criminal statutes can be used against certain misues [sic] of computer resources, most do not address the difficulties of safeguarding computerized data.").

14 In addition to the CFAA on the federal level, every one of the fifty states has its own computer crime statute. Mary M. Calkins, Note, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 GEO. L.J. 171, 181 n.60 (2000).

15 *See* CADCFAA of 1984, Pub. L. No. 98-473, 98 Stat. 2190 (codified as amended at 18 U.S.C. § 1030 (2012)).

16 *See* H.R. REP. NO. 98-894, at 8–9 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3694–95. The legislative history also mentions a secondary purpose: to ensure that computer crimes would be taken seriously and not dismissed as mere "intellectual pranksterism." *Id.* at 11, *reprinted in* 1984 U.S.C.C.A.N. at 3696. As the House Report noted, "[p]eople can relate to mugging a little old lady and taking her pocketbook, but the perception is that perhaps there is not something so wrong about taking information by use of a device called a computer even if it costs the economy millions now and potentially billions in the future." *Id.* at 12, *reprinted in* 1984 U.S.C.C.A.N. at 3697. Today, this justification has become obsolete. Public awareness and anxiety about computer crime is now widespread as the vast majority of Americans now store and transfer sensitive information via computers, and large-scale computer viruses and computer theft have been well-publicized and have personally impacted millions of users. *See* Steve Durbin, *Cybercrime: The Next Entrepreneurial Growth Business?*, WIRED (Oct. 2014), http://www.wired.com/insights/2014/10/cybercrime-growth-business/.

conventional criminal operations."[17] For example, traditional criminal statutes prohibiting larceny were thought to be insufficient in the computer-crime context because the property stolen from a computer may exist "only in the form of magnetic impulses" and the person from whom the property is stolen usually still retains a copy.[18] Congress echoed these concerns two years later in 1986 when it expanded federal jurisdiction over computer crimes by enacting the CFAA.[19] For example, the Senate report noted that "[t]he proliferation of computers and computer data has spread before the nation's criminals a vast array of property that, in many cases, is wholly unprotected against crime."[20]

A few commentators disagree, arguing that pre-existing criminal laws could have been used to prosecute any of the conduct forbidden by the CFAA. Professor Joseph Olivenbaum has criticized the "computer-specific" approach taken by the CFAA and advocated for a more traditional "harm-centered" approach in which the focus of the legislation is on deterring and punishing harmful conduct, not on the tool the suspect used to cause the harm.[21] According to Professor

---

17 H.R. REP. NO. 98-894, at 9, *reprinted in* 1984 U.S.C.C.A.N. at 3695.

18 *Id.*

19 CFAA of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030 (2012)).

20 S. REP. NO. 99-432, at 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2480. The legislative history of the CFAA also shows that Congress wanted to ensure uniform federal jurisdiction over crimes committed with a computer. Prior to the CADCFAA, the federal government only obtained jurisdiction of such crimes if the defendant placed a communication across interstate lines during the commission of the crime (thus providing jurisdiction through the wire-fraud statute). H.R. REP. NO. 98-894, at 6, *reprinted in* 1984 U.S.C.C.A.N. at 3691–92. Since much of the illicit activity involving computers in the mid-1980s did not use interstate communication, enforcement of these crimes was often left to state criminal computer crime statutes, if they existed. Given the global reach of the Internet, the vast majority of modern computer crimes involve some kind of interstate connection, thus rendering this purpose of the CFAA obsolete. Although Congress claimed to be taking quick and preemptive action by identifying and addressing problems arising out of an emerging technology, its response to the emergence of computer crime was relatively slow. Computers had been used to commit crimes—some of them very serious—long before Congress or even the states began their efforts to create computer-specific criminal laws. *See* Richard C. Hollinger & Lonn Lanza-Kaduce, *The Process of Criminalization: The Case of Computer Crime Laws*, 26 CRIMINOLOGY 101, 116 & n.8 (1988) (noting a significant "temporal lag" between the emergence of computer crimes and the promulgation of computer-specific criminal laws while criminal activity that arose out of other new technologies (such as the invention of designer drugs or the use of automobiles in crimes) brought a much faster legislative response).

21 Joseph M. Olivenbaum, *<CTRL> <ALT> <DEL>: Rethinking Federal Computer Crime Legislation*, 27 SETON HALL L. REV. 574, 641–42 (1997) (arguing that the CFAA's computer-specific approach results in an unnecessary and overbroad statute because it criminalizes conduct that would not be criminal if the defendant were not using a computer).

Olivenbaum, all of what the CFAA prohibited could already be covered by traditional criminal statutes.[22] Similarly, Professor Susan Brenner has argued that there was nothing distinct about crimes committed with computers; even if the crime took place entirely in the virtual world, it was still analogous to a traditional crime like trespass or burglary.[23] A few years after the CFAA was passed, two prominent criminologists argued that the entire purpose of the law (and its state counterparts) was symbolic because "in many instances [the new laws] merely transformed existing criminal activity involving computers into 'computer crime.'"[24]

Professors Olivenbaum and Brenner are partially correct: many of the provisions of the CFAA merely copied language from pre-existing federal laws. For example, 18 U.S.C. § 1030(a)(4) combines the language of the existing federal fraud statute with the element of "access[ing] a protected computer without authorization, or [by] exceed[ing] authorized access,"[25] while § 1030(a)(7)(A) and (C) prohibit extortion through threatening to damage a computer,[26] a crime already covered by federal extortion laws.[27] In other words, much of the conduct prohibited by the CFAA is also covered by other federal criminal provisions, meaning that the CFAA merely provides an additional charge for prosecutors to bring if the defendant used a computer while committing the crime.[28]

However, there are two provisions of the CFAA that do not have any analogue in traditional federal crimes. The first is § 1030(a)(5), which criminalizes causing damage through "transmission of a program" or after "access[ing] a protected computer without authorization."[29] The second is § 1030(a)(2)(C), the anti-hacking provision, which criminalizes "intentionally access[ing] a computer without au-

---

22 *Id.* at 641.

23 Susan W. Brenner, *Is There Such a Thing as "Virtual Crime"?*, 4 CAL. CRIM. L. REV. 1, ¶¶ 77–86 (2001) ("[I]t is conceptually irrelevant whether the location that is unlawfully accessed exists in the physical world or in the virtual world; the harm to the owner of that area is logically indistinguishable.").

24 Hollinger & Lanza-Kaduce, *supra* note 20, at 116–17 (noting that the proliferation of computer-specific crimes on the state level went against the general trend to simplify and consolidate criminal codes, and that states could have accomplished the same result through "minor definitional amendments to preexisting criminal laws").

25 18 U.S.C. § 1030(a)(4) (2012).

26 *Id.* § 1030(a)(7)(A), (C).

27 *See id.* §§ 875(d), 1951. Another example is § 1030(a)(6) which prohibits trafficking in passwords, conduct which is also prohibited by § 1029 (access device fraud). *See id.* §§ 1029, 1030(a)(6).

28 *See* Olivenbaum, *supra* note 21, at 624–41.

29 18 U.S.C. § 1030(a)(5). Some of this conduct is prohibited by § 1362, which prohibits

thorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer."[30] This provision essentially criminalizes any unauthorized or exceeded access to a computer because a "protected computer" is defined as any computer "used in or affecting interstate or foreign commerce or communication," and anytime a person gains such access, she will usually "obtain[ ] information."[31]

In other words, § 1030(a)(5) focuses on "damage" that can be done in the virtual world, while § 1030(a)(2)(C) focuses on "trespass" in the virtual world.[32] Unlike fraud, extortion, or theft, the concepts of computer "damage" and "trespass" do not translate easily from existing criminal statutes which are meant to apply to the analog world.

To be sure, the federal criminal code does contain a number of criminal damage and trespass statutes. For example, § 1361 prohibits "willfully injur[ing] or commit[ting] any depredation against any property of the United States."[33] The terms "injure" and "commit depredation" are not defined in the statute, though courts have interpreted them to mean any actual physical damage or destruction of both real and personal property.[34] But computer crimes rarely involve physical damage or destruction, and so measuring "damage" in the virtual world is difficult. Sometimes, data that is destroyed can easily be restored from a backup, making the actual amount of damage hard to calculate. On the other hand, some forms of computer crime (such as denial of service attacks) may not damage any data at all, but merely cause it to be unavailable for a period of time, and thereby cause a significant loss to its owner. And the mere fact that a system has been accessed without authorization could force a company to spend significant resources to ensure that no data has been compromised and to prevent future attacks, which might (or might not) be measured as "damage" under traditional statutes.

These problems are even more severe with regard to "trespassing" in the digital world. Federal trespass statutes bear no relation-

---

willful interference with government communication systems, but the CFAA provision is much broader. *Id.* § 1362.

30 *Id.* § 1030(a)(2)(C).

31 *See id.* § 1030(a)(2)(C), (e)(2)(B).

32 *See id.* § 1030(a)(2)(C), (a)(5).

33 *Id.* § 1361.

34 *See, e.g.*, United States v. Jenkins, 554 F.2d 783, 785–86 (6th Cir. 1977). The court noted that this includes "the act or an instance of robbing, plundering, or laying waste"—a colorful description which is nonetheless rather unhelpful when applied to the digital context. *Id.* at 786.

ship to the act of "entering" a computer without authorization.[35] It is relatively easy to define the point at which an individual enters or remains on real property without permission, but in the virtual world, the concepts of "entry" and "without permission" become much more difficult to define. Does a potential hacker "enter" a computer when she views the homepage of a website, or when she enters a password on the website, or only when she accesses an area of the website that is not generally available to the public? And does the hacker lack "permission" if she merely violates the terms of service of the website or enters a valid password belonging to someone else? None of the common law of traditional trespass will help in resolving these questions.

Thus, although much of the CFAA was unnecessary, there were at least two areas in which legislative action was necessary to respond to computer-specific crimes—computer "damage" and "trespass." Unfortunately, Congress did a poor job in crafting its response, leading to confusion in the courts.

II. Grading the CFAA

As noted above, creating technology-specific crimes can serve an important purpose if the law covers new types of activities not effectively covered by existing traditional criminal prohibitions. In its original 1984 computer crime legislation, Congress attempted to address these problems by outlawing "unauthorized access" and "exceeding authorized access" to a computer that obtained classified or financial information, or used, modified, destroyed, or disclosed information that would affect the federal government—that is, it only focused on the crimes of "computer damage" and "computer trespass."[36] Thus, Congress's original computer crime legislation succeeded in focusing on two new legal concepts relating to computer crime that had not been sufficiently defined in the then-existing criminal code.

Unfortunately, this original legislation neglected to define the terms "authorization" and "access," or explain what it meant by "us[ing], modif[ying], destroy[ing], or disclos[ing] information,"[37] and thus failed to meet its intended purpose of updating the criminal code

---

35 *See, e.g.*, 18 U.S.C. § 1863 (2012) (prohibiting trespass into national forests); 42 U.S.C. § 2278a (2012) (prohibiting trespass into federally regulated facilities); 36 C.F.R. § 2.31 (2015) (prohibiting trespass into national parks).

36 *See* CADCFAA of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190, 2190–92 (codified as amended at 18 U.S.C. § 1030 (2012)).

37 *See id.*; Susan W. Brenner, Cybercrime and the Law: Challenges, Issues, and Outcomes 24–25 (2012) (noting that the CADCFAA defined only the term "computer").

in response to technological changes. This arguably left the situation worse than it was prior to the legislation's passage. Using a computer to cause damage or accessing a computer without authorization and obtaining information were now federal crimes, but neither the courts, prosecutors, nor everyday citizens were informed exactly what type of conduct was prohibited.

When the law was amended two years later, Congress again failed to provide any definitions for these terms,[38] and then compounded its mistake by adding the crimes of computer fraud and trafficking in computer passwords which were duplicative of existing laws.[39]

It was not until 1996—twelve years after the original legislation was passed—that Congress finally defined the term "damage" in the computer context.[40] "Damage" was defined as "any impairment to the integrity or availability of data, a program, a system, or information" that "causes loss aggregating at least $5000 in value during any 1-year period"[41]—a particularly broad definition considering nearly any instance of unauthorized hacking could be said to impair the integrity of a computer system. Although this definition provided much needed (and overdue) guidance to courts and prosecutors, it raised the new question of how to calculate "loss" in the context of computer crime. After some litigation on this question, Congress amended the CFAA yet again in 2001 to define "loss" as "any reasonable cost to any victim," including the cost of assessing damage and lost revenue due to interrupted service.[42] This definition is also quite broad considering nearly any amount of damage to even a small company could easily reach the statutory threshold, especially given the fact that the

---

38 *See generally* CFAA of 1986, Pub. L. No. 99-474, sec. 2(g), § 1030(e), 100 Stat. 1213, 1215 (codified as amended at 18 U.S.C. § 1030 (2012)).

39 *See* CFAA, sec. 2(d), § 1030(a)(4), (6). Congress apparently added these two new crimes, as well as expanded the criminal damaging provision, at the request of the Department of Justice, which was seeking new tools to combat computer crime. BRENNER, *supra* note 37, at 25.

40 National Information Infrastructure Protection Act of 1996, Pub. L. No. 104-294, sec. 201(4)(D), § 1030(e)(8), 110 Stat. 3491, 3493 (codified as amended at 18 U.S.C. § 1030 (2012)).

41 *Id.* Damage less than $5000 could also give rise to felony liability if it modified or impaired medical care, caused physical injury, or threatened public safety. *Id.* Later amendments created felony liability if the damage affected a United States government computer used for "the administration of justice, national defense, or national security," or if the "damage affect[ed] 10 or more protected computers." *See* 18 U.S.C. § 1030(c)(4)(A)(i).

42 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, sec. 814(d)(5), § 1030(e)(11), 115 Stat. 272, 384 (codified in scattered titles of U.S.C.) (codifying the definition of "loss" used in *United States v. Middleton*, 231 F.3d 1207, 1213 (9th Cir. 2000)).

dollar amount has not been updated for inflation since it was originally set nearly twenty years ago.[43]

However belated and overbroad these definitions of "computer damage" may be, they are certainly preferable to Congress's treatment of the terms "exceeds authorized access" and "without authorization." The CFAA defines "exceeds authorized access" as "access[ing] a computer with authorization and [using] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter,"[44] but the statute fails to define the term "authorization" or "access."[45] Professor Orin Kerr has argued that, at the time Congress passed the CFAA, it probably did not realize how complex these concepts were (and would become) in the computer context, resulting in a startling level of ambiguity.[46] Writing in 2003, Professor Kerr noted that the way individuals used computers in the 1970s made it relatively easy to determine whether another computer was being "accessed."[47] The user had to dial into another computer and then enter a username and password to communicate with it; thus, "[w]hile the concept of access may have made sense given 1975 computer technology, the technology of 2003 presents a different case."[48] This problem has only grown more severe in 2016 with the widespread use of cloud computing and the proliferation of apps on smart phones that automatically and sometimes continuously connect to the Internet. Similarly, Congress's failure to define the term "authorization" has led to wildly inconsistent applications of the term.[49]

In short, although Congress's primary purpose in creating a computer-specific law was to tackle the novel issues that arise in the unique context of computer crime, Congress has consistently failed to provide this guidance. The problem is not due to legislative neglect: Congress has amended the CFAA eight times since 1986,[50] and has still failed to fulfill this primary purpose.

---

43 $5000 in 2016 is only about $3300 in 1996 dollars. *CPI Inflation Calculator*, BUREAU OF LABOR STATISTICS, http://www.bls.gov/data/inflation_calculator.htm (last visited Sept. 11, 2016).

44 18 U.S.C. § 1030(e)(6).

45 *See generally id.* § 1030.

46 *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1616–17 (2003).

47 *Id.* at 1641.

48 *Id.*

49 *See, e.g.*, *id.* at 1643–44 (arguing for a "code-based" definition of "without authorization"); David Thaw, *Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement*, 103 J. CRIM. L. & CRIMINOLOGY 907, 945–46 (2013) (arguing that the CFAA should be amended to increase the *mens rea* requirement for unauthorized access).

50 U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 2 (2010).

Congress's failure to resolve these questions has led to confusion in the courts which have issued widely varied interpretations of key terms in the statute. For example, there is currently a circuit split as to whether or not an employee violates the CFAA if she is authorized to use a database for certain purposes (e.g., work related purposes) but instead uses the database for other purposes (e.g., personal use or to help a competitor).[51] Furthermore, most of the caselaw surrounding the CFAA has been generated in the context of civil suits. This raises the concern that courts will interpret the language of the statute broadly in the civil context, and then the broad interpretation will have precedential value in future criminal cases.[52] Conversely, there is concern that courts will interpret the language too narrowly in civil cases because they are concerned about the use of their holdings in future criminal cases.[53] Overall, the CFAA has failed to provide adequate guidance to courts, and thus has failed to effectively establish what constitutes "computer misuse."

III. A New Way Forward: Administrative Regulation of Computer Misuse

Another way to address a new type of criminal activity (especially one that is based on evolving technology) is to empower an administrative agency to create rules regulating the activity. Administrative agencies have a number of advantages over legislatures and courts because they can develop and apply expertise in setting rules, generate and enforce separate rules for civil and criminal liability, respond quickly in creating or changing rules in response to changing conditions, and be insulated from political pressures.

---

51 *Compare* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1130–34 (9th Cir. 2009) (applying a narrow view of liability and holding that an employee is still "authorized" to use an employer's computer even if he uses the computer contrary to the employer's interest), *and* Univ. Sports Publ'ns Co. v. Playmakers Media Co., 725 F. Supp. 2d 378, 384 (S.D.N.Y. 2010) (holding same and discussing circuit split), *with* Int'l Airport Ctrs. LLC v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (adopting a broad view of liability and holding that an employee who accesses a computer in a way that breaches her duty of loyalty to her employer loses her "authorization" to access the computer), *and* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581–84 (1st Cir. 2001) (adopting a broad view of liability and holding that an employee who accesses a computer in a way that breaches her confidentiality agreement violates the CFAA by "exceed[ing] authorized access").

52 *See* Kerr, *supra* note 46, at 1599, 1642.

53 *See, e.g.*, *Brekka*, 581 F.3d at 1134–35 (noting that the court's interpretation of the CFAA in the civil case is "equally applicable in the criminal context" and that the rule of lenity should apply for all criminal cases).

Congress has turned to administrative agencies to create and maintain criminal rules in a number of other contexts. In some contexts (such as the regulation of financial crimes by the Securities and Exchange Commission ("SEC")), Congress sets out broad principles to guide the agency's actions[54] and then delegates to that agency the power to promulgate rules pursuant to those principles.[55] In other contexts (such as the regulation of controlled substances by the Drug Enforcement Agency), Congress creates specific criminal prohibitions but allows administrative agencies to keep those prohibitions current by filling in certain details.[56] Generally, Congress chooses this route when the regulated activity is complex or rapidly evolving, thus making the regulation more appropriate for administrative agencies.

Another advantage of using an administrative structure is that an agency can more easily differentiate between civil and criminal violations, and create different definitions and degrees of punishment for each. If an administrative agency takes over all civil and criminal enforcement of computer misuse, the agency could create a more sophisticated framework of regulation that segregates language and definitions into each side.

---

54 *See* Mistretta v. United States, 488 U.S. 361, 372 (1989) (recognizing that Congress may "obtain[ ] the assistance of its coordinate Branches" in establishing law because with "our increasingly complex society, replete with ever changing and more technical problems, Congress simply cannot do its job absent an ability to delegate power under broad general directives").

55 *See, e.g.*, 15 U.S.C. § 78j(b) (2012) ("It shall be unlawful for any person . . . [t]o use or employ, in connection with the purchase or sale of any security . . . any manipulative or deceptive device or contrivance in contravention of *such rules and regulations as the [Securities and Exchange] Commission may prescribe* as necessary or appropriate in the public interest or for the protection of investors.") (emphasis added). The Securities Exchange Act of 1934 created the Securities and Exchange Commission ("SEC") and provides for criminal penalties for violating SEC rules or regulations. *Id.* § 78d, ff(a). Another example is the Occupational Safety and Health Act of 1970, which created the Occupational Safety and Health Administration ("OSHA"). *See* 29 U.S.C. § 655 (2012) (allowing the Secretary of Labor to promulgate rules relating to worker safety); *id.* § 666(e) (providing criminal penalties for violations of those rules).

56 The Comprehensive Drug Abuse Prevention and Control Act of 1970 creates criminal penalties for possessing or trafficking certain substances but then allows the Drug Enforcement Agency ("DEA") to list which drugs are regulated and to what degree. *See* 21 U.S.C. § 811 (2012) (giving the Attorney General (and DEA) the power to add or remove substances from the various schedules of controlled substances in the law). Another example is the Endangered Species Act of 1973 which prohibits interfering with any species on the endangered species list, but then gives various agencies the power to place (or remove) species from that list. *See* 16 U.S.C. § 1533 (2012) (allowing the relevant administrative agencies to designate specific species as endangered); *id.* § 1538 (prohibiting any interference with the species contained on the endangered species list). Also, the federal government prohibits giving support to terrorist organizations and then relies on an administrative agency to designate which organizations are "terrorist organizations." *See* 18 U.S.C. § 2339B(a)(1) (2012); 8 U.S.C. § 1189 (2012).

How would the agency operate in practice? The first step would be to pass enabling legislation to delegate rulemaking power and guide the agency. The courts have set surprisingly few limits on this process, allowing Congress to delegate criminal rulemaking power to an administrative agency as long as the enabling statute provides an "intelligible principle" to guide and limit the discretion of the agency.[57] The Supreme Court has provided multiple examples of such "intelligible principles," such as authorizing the War Department to recover "excessive profits" earned on military contracts,[58] the Price Administrator to fix "fair and equitable" commodities prices,[59] the Federal Communications Commission to regulate broadcast licensing in the "public interest,"[60] and the Drug Enforcement Agency to place new drugs on the prohibited drug schedules if they posed an "imminent hazard to the public safety."[61]

Given these relatively broad grants of authority, administrative delegation for computer trespass cases would certainly be feasible. In fact, the current text of the CFAA would be a good starting point: Congress could direct the appropriate agency to promulgate rules to punish "[w]hoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer."[62] The agency would then draft rules specifically explaining what is meant by "access" and "authorization," and could set different levels of punishment (both civil and criminal) for different types of prohibited activity.[63] For example, merely viewing information without interacting with the protected computer may constitute one level of punishment, while entering a password or directing the computer to carry out a command would lead to a higher level of punishment. Likewise, an agency could create

---

57 Touby v. United States, 500 U.S. 160, 165 (1991).

58 Lichter v. United States, 334 U.S. 742, 774–87 (1948).

59 Yakus v. United States, 321 U.S. 414, 426–27 (1944).

60 Nat'l Broad. Co. v. United States, 319 U.S. 190, 225–26 (1943).

61 *Touby*, 500 U.S. at 165. The Court suggested in *Touby* that there may be a higher standard for administrative regulations that create criminal penalties, but in the case of criminalizing designer drugs, it held that any higher standard was met by further guidance given by the statute which also directed the agency to consider "the drug's 'history and current pattern of abuse'; '[t]he scope, duration, and significance of abuse'; and '[w]hat, if any, risk there is to the public health.'" *Id.* at 166.

62 18 U.S.C. § 1030(a)(2)(C) (2012).

63 Like the Environmental Protection Agency, the agency handling computer misuse would have rulemaking power and the ability to handle administrative hearings, but would leave civil and criminal enforcement of its rules to the Department of Justice. *See* U.S. ENVIRONMENTAL PROTECTION AGENCY, ENFORCEMENT BASIC INFORMATION (2016), http://www.epa.gov/enforcement/enforcement-basic-information.

less severe (perhaps merely civil) penalties for individuals whose access is "unauthorized" or "exceeds authorization" because they violate terms-of-service provisions or employer restrictions on employee computer use (what Professor Kerr terms "contract-based theories of authorization"),[64] but more severe criminal penalties when such access involves "tricking" the violated computer by hacking into its code or entering a false password (so-called "code-based restrictions").[65]

The administrative agency would also be able to update its rules as technology evolves. Currently, every time computer hackers employ new tactics or use a new technology, prosecutors must go to Congress to request amendments to the CFAA. Within the next ten years, the concept of "access" or "computer" may change even more dramatically than it has in the last thirty years, requiring new definitions for these terms, or perhaps an entirely new regulatory structure. The definition of "authorization" may also need to be updated as new forms of interacting with third-party computers come into existence—just as the rise of email, social media websites, and cloud data storage have changed the ways we interact with computers. Future technological advances will create new ambiguities that we cannot yet even imagine—ambiguities that will be far better addressed by the expertise, speed, and political neutrality of an administrative agency rather than by Congress.

Most importantly, an administrative agency could anticipate specific types of computer trespass and assign the appropriate level of criminal liability for each situation. For example, consider the various scenarios discussed in Matthew Kugler's paper in this Symposium.[66] Kugler surveyed nineteen different scenarios, almost all of which involved some form of "unauthorized access" or "exceeding authorized access."[67] The survey respondents believed there should be significantly different levels of liability based on slight differences in the facts of the case.[68] For example, respondents believed that breaking into a secured Wi-Fi and looking at the files on the victim's iTunes

64 Kerr, *supra* note 46, at 1649.

65 *Id.* An administrative agency could also create different regulations for civil cases and thus segregate the civil and criminal law for computer trespass cases. Currently, most of the litigation surrounding the CFAA is brought by civil litigants, and so courts interpret the terms of the statute in the context of a civil case. Oftentimes this will result in definitions that are appropriate for assigning civil liability but too broad for criminal cases.

66 Matthew B. Kugler, *Measuring Computer Use Norms*, 84 GEO. WASH. L. REV. 1568, 1576–90 (2016).

67 *Id.*

68 *Id.*

account was significantly less blameworthy than breaking into a secured Wi-Fi and looking at the general files on the victim's computer.[69] The CFAA does not distinguish between many of these different scenarios.[70] Indeed, it would be impossible to design any statute that could effectively make such distinctions, not to mention keep those distinctions up-to-date as technology (and our relationship to technology) evolves.

To see how these fine distinctions might apply in an actual prosecution, consider the recent case of *United States v. Lowson*.[71] The defendants in this case ran a service called Wiseguys which purchased blocks of tickets from online vendors such as Ticketmaster and then resold them on its own website.[72] The government charged the defendants with multiple counts of violating § 1030(a)(2) of the CFAA, alleging that the defendants gained "unauthorized access" to the Ticketmaster site to purchase the tickets.[73] According to the indictment, the defendants conducted the following actions in order to buy their blocks of tickets:

(1) Violated Ticketmaster's terms of service for its website which prohibits using computer programs to purchase blocks of tickets;[74]

(2) Circumvented "proof of work" protections on the Ticketmaster site which are designed to prohibit spam, denial of service attacks, and other mass-produced requests of the site by requiring the requesting computer to do some amount of work before accessing the site;[75]

(3) Wrote automated software and special optical character recognition programs to defeat the CAPTCHA challenges on the Ticketmaster site which are designed to ensure that actual human beings are inputting information;[76]

---

69 *Id.* at [18]

70 *See generally* 18 U.S.C. § 1030 (2012). The CFAA does distinguish between some of the broadest types of behavior in Kugler's survey. For example, the survey differentiated between using a web crawler that did not interfere with the operation of the target website and using a web crawler that intentionally damaged the site's operation. *See* Kugler, *supra* note 66. The CFAA reflects this distinction by creating different levels of liability based on whether the unauthorized access causes damage. *See* 18 U.S.C. § 1030(a)(2), (a)(5), (c).

71 United States v. Lowson, No. 10-114 (KSH), 2010 WL 9552416 (D.N.J. Oct. 12, 2010).

72 *Id.* at *1–*2.

73 *Id.* at *4–*5.

74 *Id.* at *5.

75 *Id.*

76 *Id.*

(4) Used thousands of nonconsecutive internet protocol ("IP") addresses so the Ticketmaster software could not detect that the sales were all going to the same company;[77] and

(5) Hacked into Ticketmaster's purchase ticketing program to enable Wiseguys's automated programs to purchase tickets.[78]

The district court judge in the case had the unenviable job of deciding which of these actions by the defendants counted as "unauthorized access" of the Ticketmaster website.[79] Of these actions, the first is merely a "contract-based" violation which should probably be dealt with through civil lawsuits, and the fifth is a "code-based" violation which certainly constitutes criminal "unauthorized access." The second, third, and fourth raise some more complicated questions. If the defendants used special software to gain access to the site more frequently than an ordinary person could without such software, does this become a "code-based" violation or merely a more egregious "contract-based" violation? How sophisticated does the software have to be to rise to the level of "unauthorized access"? And, if the defendants merely hired a hundred employees to buy tickets all at once in the usual method, would that still count as "unauthorized access"?

But two other questions are even more troubling. First, how is a court meant to decide this case using nothing more than the minimal definitions in the CFAA and the conflicting caselaw from various circuit courts, almost all of which involve slightly different actions on the part of the defendant? And second, is it appropriate to treat all of these actions the same way? The CFAA makes no distinction between these different types of intrusions which are all covered under the same unauthorized access provision.[80]

An administrative agency, by contrast, would be able to list specific actions that constitute "unauthorized access," and then update the list as new forms of gaining access to websites arise. Furthermore, the agency could set (and adjust) punishments for different levels of

---

77 *Id.* at *2.

78 *Id.* at *5.

79 *Id.* at *6.

80 *See* 18 U.S.C. § 1030(a)(2)(C) (2012). Another question which must be asked is one which this Article discussed earlier: whether there even needs to be special computer crime liability in this case. The defendants were also charged with seventeen different counts of wire fraud for these same actions because they not only gained access to the Ticketmaster accounts, but did so with the intent to defraud Ticketmaster. *Lowson*, 2010 WL 9552416, at *2. Given these charges, it is not clear why there was a need to also charge the defendants with twenty-five additional counts of unauthorized access under the CFAA. *See id.* at *5–*6.

unauthorized access. Thus, courts, prosecutors, and potential defendants would not have to guess whether certain conduct is prohibited, and those who do violate the regulations would receive a punishment more closely tailored to their level of wrongdoing.

Another benefit to this proposal is that an administrative agency overseeing issues of computer misuse could also serve in an advisory capacity for other agencies in the executive branch who have to deal with the growing economic and social impact of computers and software in the United States. As Professors Paul Ohm and Blake Reid argue in this Symposium, there are many administrative agencies in the executive branch that started out as regulators of machines, chemicals, or medicine, but which are now struggling with the regulation of computers and software.[81] The Federal Drug Administration must now regulate robotic surgical instruments,[82] the Department of Transportation must deal with autonomous driving cars,[83] and nearly every agency that regulates consumer products must now come to terms with the "internet of things" as more and more products are run by software, connected to the Internet, and thus subject to hacking.[84] Because existing agencies may lack the expertise to optimally regulate their field in this new environment, an agency regulating computer misuse could provide much needed guidance.

Professor Ryan Calo has made a similar argument in his recent proposal for a Federal Robotics Commission—a new federal agency that could channel government research dollars, convene stakeholders on the growing field of robotics, and advise other agencies as they deal with the growing influence of robots in society.[85] Calo notes that new technologies have frequently generated a need for new administrative agencies: For example, the invention of the radio spurred the creation of the Federal Radio Commission and ultimately the Federal Communications Commission, and the introduction of vaccines led to the creation of the Centers for Disease Control and Prevention.[86] Calo also

---

81 *See* Paul Ohm & Blake Reid, *Regulating Software When Everything Has Software*, 84 GEO. WASH. L. REV. 1672, 1673 (2016).

82 *See* U.S. FOOD & DRUG ADMIN., DISCUSSION PAPER: ROBOTICALLY-ASSISTED SURGICAL DEVICES (2015), http://www.fda.gov/downloads/MedicalDevices/NewsEvents/WorkshopsConferences/UCM454811.pdf.

83 *See* U.S. DEP'T OF TRANSP., DOT/NHTSA POLICY STATEMENT CONCERNING AUTOMATED VEHICLES (2016).

84 *See* Ohm & Reid, *supra* note 81, at 1673.

85 RYAN CALO, THE CASE FOR A FEDERAL ROBOTICS COMMISSION 11–12 (2014).

86 *Id.* at 3. Professor Calo also gives the examples of railroads and cars necessitating the creation of the Department of Transportation, and of airplanes leading to the creation of the Federal Aviation Administration. *Id.*

notes numerous examples of federal agencies (who lack the expertise in robotics) doing a poor job of responding to new technology, including the Federal Aviation Administration's clumsy efforts at regulating drones and the SEC's inability to properly deal with high-speed trading finance algorithms.[87] Similarly, neither Congress nor the various existing agencies have the expertise to deal with the myriad ways in which computer "damage," "trespass," and other forms of computer misuse impact society.

One objection to turning over the regulation of computer misuse to an administrative agency is that the executive branch would assume the primary rulemaking authority for computer crimes. Some have argued that the executive branch, in the form of federal prosecutors, has abused its authority under the CFAA.[88] An administrative agency empowered to create specific rules for terms such as "access" and "authorization" might create broad definitions that would codify existing prosecutorial practices, or perhaps even permit a greater range of prosecutions. Even worse, these broad definitions would be entitled to *Chevron*[89] deference by the courts, making judges even more reluctant to limit prosecutorial overreach.

There are two responses to this objection. One is that a centralized administrative agency tasked with creating these regulations (even one located in the Department of Justice itself) would be more inclined to implement moderate and narrow rules than individual federal prosecutor's offices.[90] As Professor Dan Kahan has argued, shifting from the de facto rulemaking authority of local United States Attorneys to the actual centralized rulemaking power of the Department of Justice can help reign in prosecutorial abuse because "[d]istant and largely invisible bureaucrats within the Justice Department lack the incentives that individual U.S. Attorneys have to bend the law to serve purely local interests."[91]

---

87 *Id.* at 8–9.

88 *See* Thaw, *supra* note 49, at 921–23, 944–45; *see also, e.g.*, United States v. Swartz, 945 F. Supp. 2d 216, 217–18 (D. Mass. 2013) (charging Aaron Swartz, a computer programmer, with two counts of wire fraud and eleven violations of the CFAA after he broke into a closet at the Massachusetts Institute of Technology to install a device to download academic journal articles from JSTOR, a subscription-only database); United States v. Drew, 259 F.R.D. 449, 452 (C.D. Cal. 2009) (charging Lori Drew under the CFAA after she created a fictitious MySpace account allegedly belonging to a sixteen-year-old boy in order to gain the trust of and then harass a former friend of her teenage daughter).

89 Chevron v. Nat. Res. Def. Council, 467 U.S. 837 (1984).

90 Dan M. Kahan, *Is* Chevron *Relevant to Federal Criminal Law?*, 110 HARV. L. REV. 469, 498 (1996).

91 *Id.* at 497 (arguing that "[b]ecause the [Justice] Department, through the President, is

Second, assigning rulemaking authority to an administrative agency would actually make the process more responsive and transparent. Administrative procedures call for significant notice-and-comment periods during which various interests groups can evaluate and provide feedback on the proposed rules,[92] making it easier for these interest groups to affect the rulings of an agency than it would be to lobby Congress for changes in a statute. And unlike today, when the meaning of "unauthorized access" may vary between federal districts and depend on the individual decision of a United States Attorney or district court judge, the specific definitions of each rule will be clearly defined for the entire country.

Conclusion

Whenever a legislature creates a technology-specific crime, it faces a number of challenges. First, there is a risk that the new statute will merely duplicate existing crimes, thus over criminalizing the conduct and creating unnecessary confusion. Second, the legislature needs to ensure that it provides the proper guidance to prosecutors, citizens, and courts regarding the new concepts in the criminal statute. And finally, the legislature needs to ensure that the law can be amended and updated as the technology evolves.

The CFAA is an example of a technology-specific criminal statute that fails all of these tests. Much of the CFAA is comprised of extortion, fraud, and theft provisions which prohibit conduct already covered by existing laws (or could be covered through minor changes to those laws). Meanwhile, the critical concepts of "loss," "access," and "authorization" still remain poorly defined or completely undefined by the statute thirty years after it was first passed. This failure of Congress has made the unique provisions in the CFAA prohibiting computer "damage" and "trespass" ineffective as courts are left to enforce them without clear guidance.

The best solution to this problem is for Congress to stop trying to regulate computer misuse directly through legislation, and instead empower an administrative agency to set more detailed and technical rules regarding what constitutes "computer misuse." Thirty years of

---

accountable to the national electorate, it is more likely to be responsive to interests hurt by adventurous readings, particularly readings that discourage socially desirable market activities").

92 *See* 5 U.S.C. § 553 (2012). The Administrative Procedure Act requires notice of proposed rulemaking in the Federal Register and an opportunity for interested persons to "participate in the rule making through submission of written data, views, or arguments with or without opportunity for oral presentation." *Id.* § 553(b)–(c).

the CFAA have demonstrated that Congress lacks the expertise or inclination to define the relatively new concept of "computer misuse," and the challenge is only becoming greater as the types of digital devices, and the ways of communicating with them, increase every year.