<CTRL> <ALT> <DEL>: RETHINKING FEDERAL COMPUTER CRIME LEGISLATION

Joseph M. Olivenbaum[*]

[*]Associate Professor of Law, Pace University School of Law; B.A. New York University, 1970; J.D. Northeastern University School Of Law, 1981.

> The law has rested on a perception of technology that is sometimes accurate, often inaccurate, and which changes slowly as technology changes fast.
>
> Ithiel de Sola Pool[1]

INTRODUCTION

The emergence of computer technology in the late twentieth century has opened vast new possibilities and presented new challenges to almost every social, cultural, commercial, and political institution of modern life.[2] Computer technology has fostered enormous changes, particularly in information processing and communications, which in turn change in important respects the way we experience the world. Most striking, perhaps, is that computers remove some of the limitations of time and place that the familiar physical world has always imposed.[3]

As virtually every aspect of social life has had to respond to the impact of widely available computer technology, so too has the law. The greatly enhanced ease of access to, and large-scale reproduction of, legally protectible materials presents new challenges to the law of intellectual property and copyright. The rights of individuals to freedom of speech, protected by the First Amendment, may collide with the regulations imposed on commercial publishers and distributors when individuals themselves become "publishers" or mass distributors of text, pictures, or other materials. Questions of privacy protection can be raised by the ease with which large numbers of uninvited strangers can "invade" an individual's home or presumably personal environment.

The availability and widespread use of computers also present challenges to the criminal law. Computers offer both new ways to commit old crimes and the means of committing crimes unknown to a pre-digital justice system. But the distinction between familiar crimes accomplished by means of new electronic technology, and "new" crimes made possible only by technology, has been unnecessarily and confusingly blurred by recent federal computer-crime legislation. Legislators and others apprehensive about the misuse of technology too often have perceived a need to enact statutes to counteract "computer crimes"[4] that are in fact al-

---

[1] TECHNOLOGIES OF FREEDOM 7 (1983).

[2] "The content on the Internet is as diverse as human thought." ACLU v. Reno, 929 F. Supp. 824, 842 (E.D. Pa. 1996).

[3] *See, e.g.*, Josh L. Wilson, Jr., *Electronic Village: Information Technology Creates New Space*, 6 COMPUTER/L.J. 365, 370 (1985). *See generally* M. ETHAN KATSH, THE ELECTRONIC MEDIA AND THE TRANSFORMATION OF LAW (1989) (discussing broad changes in the law resulting from electronic transmission of data).

[4] One significant obstacle faced by any researcher into the area of computer crimes

ready-existing crimes accomplished with new techniques. To the extent that such statutes merely prohibit conduct that is already criminal, they are simply redundant. To the extent that they are drafted in "technology-specific" language, the pace of technological change and the ingenuity of computer-literate criminals guarantee that those statutes will be obsolete almost as soon as they are enacted. To the extent that they focus on technological means, rather than on the harm caused by a defendant's conduct, those statutes tend towards overbreadth by sweeping within their ambit anyone who uses the means regardless of result. To the extent that computer-specific statutes are enacted by legislators unfamiliar or uncomfortable with technology, such statutes tend to reflect a lack of clarity or understanding or, sometimes, simply fear. Thus, a "computer-specific" approach results, too often, in criminal statutes that are unnecessary, imprecise, clumsy, over-inclusive, or ineffective.

State and federal legislatures have been drawn to the idea that new statutory prohibitions are necessary by an array of sociological and political concerns, including legislators' own technological education and comfort level.[5] In addition to those extra-legal considerations, however, the nature of the criminal law itself can seem to demand a wholly new statutory response to computer crime. Specifically, digital technology presents challenges to two related notions that underlie the criminal law as it has been traditionally understood: the concept of property and the importance of physical location.

Much of the criminal law seeks to deter and punish transgressions against property. A very broad range of criminal statutes—from felonies

---

is the dearth, indeed the absence, of reliable and comprehensive statistical data sufficient to provide an accurate profile of the subject. The number of prosecutions for computer-related crime apparently remains quite small; the number of cases that have gone to trial is smaller yet; and the number of appellate decisions in the area is such as to leave vast areas of statutory interpretation and application unresolved. Estimates as to the amount of computer crime vary so enormously as to make any figure suspect. Apparently no governmental or private agency maintains a reliable compilation of the number of crimes, or prosecutions, or convictions involving computer-related conduct. This problem stems, in large part, from the fact that the federal government, and most of the states, have both computer-specific criminal statutes and statutes of more general application under which computer-related conduct can, and has been, prosecuted. Another major complicating factor is the reluctance of targets of such crimes, particularly corporate, governmental, and other institutional victims, to report publicly either the fact or the extent of intrusions into sensitive programs and databases. Overriding all of these significant problems is the protean difficulty of defining a computer crime. The theft of a computer from a retail store may be defined as a computer crime by some, and as garden-variety theft by others. Stealing a wallet that contains both cash and an automatic teller machine card with an access code written on its back, and then using the card to obtain additional cash, may or may not constitute a computer crime.

[5] *See* Amalia M. Wagner, Comment, *The Challenge of Computer-Crime Legislation: How Should New York Respond?*, 33 BUFF. L. REV. 777, 781 n.22 (1984).

such as burglary or forgery, to misdemeanors such as vandalism by graffiti—are designed to protect various kinds of property interests. The notion of property is, of course, central to the definition of those crimes. Computer-related criminal conduct presents a challenge to the criminal law, in significant part, precisely because it involves electronic impulses that cannot be seen, touched, moved, or copied as those terms have traditionally been defined, and that therefore seem to fall outside the idea of "property" as defined over centuries of Anglo-American jurisprudence.

Computer technology also alters the significance of physical location. While computers can perform a vast array of tasks, almost all of the legal issues relevant to "computer crime" arise from one category of computer functions: communications. Computer-related criminal conduct typically involves the accessing, transfer, and/or distribution of information on one computer by means of software operating on another remote computer. The central characteristic that distinguishes electronic communications in these situations is remoteness: physical proximity becomes irrelevant.

The crimes of trespass and larceny provide useful illustrations of the problems posed by computer technology. Typical criminal statutes define trespass as the unlawful entry onto another's property.[6] Larceny is typically defined as the taking of another's property with the intent to deprive.[7] Central to the definition of both crimes is the idea of property. With trespass, the property is geographical. A person commits trespass by physically moving into a specified geographical space. The paradigm of trespass, descended from centuries-old common law, is the unlawful entry onto real estate. Larceny too has traditionally been defined in terms of tangible property. The simplest conception of larceny, again springing from old common law and the social circumstances from which it arose, is the unlawful seizing and carrying off of one's neighbor's sheep. Both of these ancient crimes rest on the notion of property as physical property: property one can grab and walk off with, property one can stand on, property that can be fenced off or tied down.

Computers—the machines themselves—are, of course, tangible property that exists in the familiar physical world. But the interactions that the machines make possible do not involve tangible property and do not take place in the familiar physical world. Computer interactions occur, instead, in "cyberspace,"[8] the same "place" in which telephone

---

[6] *See, e.g.*, N.Y. PENAL LAW § 140.05 (McKinney 1995); MODEL PENAL CODE § 221.2 (1980).

[7] *See, e.g.*, N.Y. PENAL LAW § 155.05 (McKinney 1995); MODEL PENAL CODE § 223.2 (1980).

[8] William Gibson coined this now-familiar phrase. Although usually attributed to his

conversations occur.[9] The notion of geographical place is irrelevant to those interactions. They do not occur "in" a machine, but rather only by means of the machine. The geographical location of the persons involved in the interaction is irrelevant: the same operations can be executed on, or from, any similarly-equipped machine regardless of place. The notion of physical property is similarly irrelevant. Interactions in cyberspace consist of electromagnetic impulses, which may be "matter" as understood by a physicist, but do not easily correspond to "property" in the ordinary sense or as defined by the law.

Perhaps the simplest example of a computer crime is the unauthorized accessing of a computer, and the manipulation or copying of information stored on that computer. Does such an occurrence involve a trespass? In some sense, of course, there has been an unlawful entry onto the property of another. But "property" is precisely where the application of the law of trespass becomes problematic. The electronic intruder has not entered the property of anyone, certainly not in the old common-law sense of entry onto real estate. If the intruder copies or downloads information without authorization, has a larceny occurred? The old notion of larceny does not easily fit the situation. If the original data remain stored on the accessed machine, nothing has been "taken" from the owner: the owner still has exactly what she had prior to the "entry." And even if our intruder copies the information and then deletes the original, exactly what has been taken? The intruder has simply caused the reproduction of a series of electronic impulses—digital ones and zeroes—that can be read and then displayed by another machine. Such a description is far from the idea of property as typified by a neighbor's livestock.

When faced with the problematic application of traditional crimes to the brave new digital world, legislatures typically respond with statutes aimed specifically at the use of computers and defined in terms of specific technology. Legislators have tended to view computers as different, and crimes committed with the use of computer technology as fundamentally different from crimes committed with other kinds of tools. But other responses are possible and indeed are frequently preferable.

This Article argues that legislatures can respond more effectively to most computer-related crimes by modifying existing criminal statutes, rather than by enacting new computer-specific laws. Computers are not so unique that the criminal law must be rewritten to account for them; in-

---

novel NEUROMANCER (1984), it first appeared in his short story *Burning Chrome*, *reprinted in* BURNING CHROME (1986).

[9] *See* John Perry Barlow, *Coming Into the Country*, 34 COMMUNICATIONS OF THE ACM 19 (March 1991) <http://www.eff.org>. *See infra* note 15.

deed, most "computer crimes" correspond quite closely to older crimes, notably trespass or larceny. Simply by redefining "property," or broadening other statutory language, legislatures can bring "computer crimes" under those existing statutory prohibitions. Enacting wholly new statutes, aimed solely at crimes committed with the aid of electronic technology, too often produces unnecessary and ineffective legislation. Moreover, a legislative focus on the computer, rather than on the harm caused by conduct, can lead to the misconceived conclusion that conduct undertaken by means of a computer amounts to a crime, even though analogous conduct undertaken by other, less high-tech means does not. With few exceptions, legislatures should focus on results, rather than on the means employed. If the result warrants a criminal penalty, then a penalty should be imposed. To a great extent, traditional criminal statutes will achieve that result. If the result does not warrant a criminal penalty, then the involvement of a computer should not transform innocent activity into criminal conduct.[10]

Part I of this Article provides a brief history of the emergence and proliferation of computer technology, including the historical context in which computer-law issues arise. Part II analyzes the provisions of the major federal computer-crime statute, the Computer Fraud and Abuse Act of 1986.[11] Part III presents a critical view of the computer-specific approach reflected in that statute, in other computer-related legislation, and in prosecutions commenced under other federal statutes. Part IV advocates an alternative approach to computer-crime legislation, arguing that reliance on traditional criminal statutes of general application is more effective and more legislatively sound.

I. AN HISTORICAL PERSPECTIVE: THE GOOD OLD DAYS

> Some degree of abuse is inseparable from the proper use of every thing.
>
> James Madison[12]

Computers were invented in the 1940s, as part of the war effort; but until the 1960s they were available only to a very small number of military, scientific, and university researchers.[13] Although the idea of com-

---

[10] *See* Joshua Quittner, *Computer Rights: Advocates Worry About Overzealousness in the Crackdown on Hackers*, NEWSDAY, Sept. 4, 1990, at 1.

[11] 18 U.S.C. § 1030 (1995).

[12] *Gertz v. Welch*, 418 U.S. 323, 340 (1974) (citing *The Report on the Virginia Resolutions of 1798*, *in* 4 J. ELLIOT, DEBATES ON THE FEDERAL CONSTITUTION OF 1787, 571 (1876)).

[13] *See* ACLU v. Reno, 929 F. Supp. 824, 831 (E.D. Pa. 1996); *see also* HOWARD RHEINGOLD, THE VIRTUAL COMMUNITY 65-89 (1993) (notable among the many accounts

puters, and a vague notion of their capabilities, gradually became part of the cultural landscape, to virtually everyone outside the very small computer community they were enormous, unwieldy number-crunching machines with little relevance to the lives of ordinary people. From the late 1960s to the early 1980s, the community of computer users slowly expanded; more businesses made use of them in office settings, personal computers became available, and, to a small but growing portion of the population of the United States, the computer opened an exciting, unexplored, untamed world.

This period in the development of the computer has been analogized to the opening of the frontier in the American West:

> Cyberspace . . . has a lot in common with the 19th Century West. It is vast, unmapped, culturally and legally ambiguous, verbally terse, . . . hard to get around in, and up for grabs. Large institutions already claim to own the place, but most of the actual natives are solitary and independent, sometimes to the point of sociopathy. It is, of course, a perfect breeding ground for both outlaws and new ideas about liberty.[14]

The comparison is intriguing, illuminating, and appropriate. In its formative years, the Western frontier, like the electronic frontier, was populated by knowledgeable and decidedly independent explorers, rugged individualists with little interest in formalized control structures who lived instead by their own rough-hewn "code." Much as the legendary Western pioneers had to develop an array of survival skills and highly valued the self-sufficiency the frontier demanded, so too electronic explorers had to develop flexible, adaptive, often seat-of-the-pants techniques for surviving in cyberspace. Early Westerners were drawn to the wildness and openness of the region; they wanted neither themselves nor the land to be "fenced in," and resented attempts by others to do so. Quite similarly, one oft-repeated motto of the electronic frontierspeople was that "information wants to be free;"[15] they resented any effort to restrict access to information, any attempt to fence in the wide-open

---

of the development and proliferation of computers).

[14] John Perry Barlow, *Crime and Puzzlement: In Advance of the Law on the Electronic Frontier*, 68 WHOLE EARTH REV. 44, 45 (1990). In 1990, Barlow, along with Mitch Kapor, founder of Lotus Development Corp., founded the Electronic Frontier Foundation, one of the first advocacy groups concerned with legal issues of the computer age and in particular the protection of civil liberties in computer-related settings. The organization's on-line site, http://www.eff.org, provides a valuable source of information, legal and otherwise, pertaining to computer-related issues.

[15] *Cf.* Terri A. Cutrera, Comment, *The Constitution in Cyberspace,* 60 UMKC L. REV. 139, 141 (1991): "[T]he 'hacker ethic' . . . postulates that 'access to computers . . . should be unlimited and total'; . . . 'all information should be free.'" *Id.* at nn.13, 14 (citing Dorothy E. Denning, Concerning Hackers Who Break Into Computer Systems (Oct. 1990) (paper presented at 13th National Computer Security Conference)).

reaches of cyberspace. These electronic pioneers felt they had the right, indeed the duty, to explore every corner of this new territory; but their unwritten code, the "hacker ethic," prohibited causing damage to any computer or to information.[16]

The unwritten code of the Old West may have worked well enough when the pioneers were few and largely self-sufficient, established settlements virtually non-existent, and the inhabitants willing to abide by the general strictures of the pioneer ethic. But that loose arrangement became untenable when, on the one hand, settlers arrived to start farms, establish towns and businesses, and generally bring civilization to the frontier, and on the other, when outlaws arrived to plunder these assets in the absence of visible law-enforcement mechanisms.

Similarly, the electronic frontier became increasingly populated by persons who neither had nor wanted to develop extensive technological expertise; they wanted an easy-to-use, efficient tool without having to battle a challenging, cantankerous environment; they wanted to set up businesses and start "towns"—bulletin boards, chat lines, newsgroups—and wanted some security and predictability for their forays into the territory. And "outlaws" appeared, who did not subscribe to the hacker ethic of doing no damage, but instead wanted to take advantage of the absence of external controls to plunder the growing abundance of on-line assets.

As the mythical Wild West inevitably came under the rule of law and order, so too the electronic frontier could not have continued forever by relying only on informal self-policing by the on-line community. Doing business electronically required the same kinds of law enforcement as did business in the three-dimensional world. The digital world thus poses legal and social issues that have surfaced in other contexts throughout American history: the tension between freedom of individual conduct and the need for order and control; the impulse towards openness, freedom of speech and public access in conflict with the need for security and privacy; the tendency towards a freewheeling, government-off-our backs, slightly anarchic democracy versus the perceived need for regulation to make the digital world safer and more predictable.

The age of relative innocence in cyberspace ended during the 1980s; the wide-open electronic frontier had to be made safe for tamer and, significantly, commercial[17] pursuits, and law enforcement therefore had to

---

[16] *See id.*

[17] Hacking helped energize both the personal computer industry and the software industry. Steve Jobs and Steve Wozniak, whose creation of the Apple computer made the machine accessible to average people, gained most of their knowledge from hacking. The same holds true for Bill Gates, whose fascination with software eventually led to the creation of Microsoft Corp., now the world's leading producer of operating programs for IBM

make its presence felt. Several notable events marked the transition from frontier to marketplace during this period. The first federal computer-crime legislation was proposed in 1979;[18] Congress enacted the first such statute, a rather primitive model, in 1984;[19] in 1986, Congress revised the statute[20] to set up a more comprehensive legal framework for the prosecution of computer crimes. In 1983, the movie "War Games" was released, providing a point of cultural reference regarding the dangers of computers and their users; that reference, perhaps like stories of legendary gunslingers, continues to appear in accounts of real incidents. Serious, and potentially serious, incidents of theft by computer increased significantly. And in 1990, the first massive federal law-enforcement action, Operation Sun Devil, took place.

The mission of Operation Sun Devil was to combat crime in cyberspace; in particular, it focused on persons who made a practice of "trespassing" by accessing information without authorization. Many of those targeted by the operation[21] were no more than hackers, or, if one prefers, pioneers: many of them subscribed to the notion that "information wants to be free," and that accessing information, without causing damage, economic or otherwise, was natural behavior in the electronic landscape. Operation Sun Devil was a coordinated effort involving the Federal Secret Service, numerous local law enforcement agencies, and the security resources of MCI, Sprint, the regional Bell companies, American Express, and other companies heavily invested in on-line business activity.[22] Considerable evidence, in fact, suggests that the telecommunications industry was the driving force behind the operation.[23] It is not surprising that commercial entities trying to do business

---

> personal computers. But with the increasing dependence of business and society upon electronic networks, the incursions of hackers became less and less tolerable.

Willie Schatz, *The Terminal Men: Crackdown on the 'Legion of Doom' Ends an Era for Computer Hackers*, WASH. POST, June 24, 1990, at H1.

[18] *See infra* note 32.

[19] *See infra* Part II.

[20] *See infra* Part II.

[21] See *infra* note 24 *et seq.*

[22] *See* Barlow, *supra* note 14, at 49.

[23] *See* BRUCE STERLING, THE HACKER CRACKDOWN 1-39 (1992) (examining in detail the central role of the telecommunications industry, and in particular of AT&T and the Bell regional companies, in computer-related law enforcement generally and in Operation Sun Devil in particular); *see also* Mark Lewyn & Evan I. Schwartz, *Why the "Legion of Doom" Has Little Fear of the Feds*, BUS. WEEK, Apr. 15, 1991, at 31 (quoting AT&T's corporate security manager to the effect that, with regard to one indictment stemming from an Operation Sun Devil raid, without AT&T's help, the government "would have had no case").

in the electronic "neighborhood" wanted the law to be a strong and visible presence.

Several analogies seem inescapable in describing the sweep of Operation Sun Devil. As in the Old West of legend, it was time to clean up the town so that decent folk—shopkeepers—could carry on their business without having to put up with untamed, peculiar, and unpredictable rowdies; the solution was to jail those who acted in untamed, peculiar, or rowdy fashion, whether or not they caused actual harm. To suggest a more recent urban analogy, it was time to get the gangs off the streets, so that law-abiding citizens could conduct their affairs in safety; the solution was to jail those who flaunted gang colors, or hung out on the street corner, or stayed out too late making too much noise, whether or not they caused actual harm.

Operation Sun Devil first came to public attention in January 1990, only days after the AT&T "crash,"[24] with the arrests of several persons well-known in the hacker "underground," and then struck most visibly on May 8, 1990, with the execution of twenty-eight search warrants in fourteen cities across the country.[25] Secret Service agents carried out raids, often at gunpoint, confiscated approximately forty computer systems and other high-tech tools from homes and businesses,[26] seized some 23,000 computer disks[27] and disrupted the digital lives of their targets. The operation represented an unmistakable statement by law enforcement officials that as far as the law was concerned the frontier was closed: they would prosecute not only serious computer crimes, but also the mere disregarding of property lines.

The operation was an overreaction.[28] None of the targets were shown to have engaged in serious criminal activity, or to have caused any actual harm. The number of reported prosecutions was no more than

---

[24] On January 15, 1990, Martin Luther King, Jr. Day, AT&T's long-distance telephone system "crashed," disrupting service for millions of users. Although AT&T officials acknowledged that the massive outage resulted from an internal computer system error, speculation surfaced about the possibility of the involvement of outside hackers. *See* STERLING, *supra* note 23, at 32-39. Sterling argues that the crash gave law enforcement and industry officials a "cause celebre" to justify the implementation of Operation Sun Devil. *See id.* at 1-39.

[25] *See* John Markoff, *Drive to Counter Computer Crime Aims at Invaders*, N.Y. TIMES, June 3, 1990, at 1.

[26] The items seized included answering machines and telephones. *See* Barlow, *supra* note 14, at 55-56; STERLING, *supra* note 23, at 147-55.

[27] *See* Markoff, *supra* note 25.

[28] "Every time there is a perceived crisis, law-enforcement agencies and legislators overreact, and usually due process and civil liberties suffer." *Id.* (quoting Rep. Don Edwards (D-Calif.)).

seven,[29] a very small number given the size of the operation. The major tangible consequence of the operation was the seizure of equipment and data, and the shutting down of numerous bulletin boards. Most important was the sending of the clear message that "the law has come to cyberspace."[30] If the early years in cyberspace were marked by lawlessness, then a major law-enforcement operation, even an overly harsh and punitive operation, may seem an inevitable response. The pendulum had swung too far in the direction of unrestricted freedom; the time had come to impose order and predictability.

Seen in this light, computers do not represent something entirely new in the legal world; the electronic domain is, instead, a new arena in which the same tensions that have always informed the law, and the criminal law in particular, must be played out.

The law of computer crime thus reflects, in a new technological environment, conflicts that have arisen in many other, more traditional settings. In the 1990s, the challenge is to find an acceptable, constitutional balance between encouraging and utilizing the freedom of cyberspace and preventing its exploitation for criminal purposes.

II. THE CONGRESSIONAL RESPONSE: THE COMPUTER FRAUD AND ABUSE ACT

The Computer Fraud and Abuse Act (CFAA)[31] was the first federal statute aimed specifically at computer crimes.[32] Originally enacted in 1984,[33] the statute provided specific authority for the prosecution of certain crimes accomplished by means of a computer. Reporting the Act[34]

---

[29] *See* Cutrera, *supra* note 15, at 153.

[30] *See* Barlow, *supra* note 14, at 55.

[31] 18 U.S.C. § 1030 (1995).

[32] Senator Abraham Ribicoff of Connecticut introduced the first proposed computer-specific criminal statute, the Federal Computer Systems Protection Act, in Congress in 1977 as S. 1766, 95th Cong. (1977); subsequently revised and introduced as S. 240, 96th Cong. (1979). *See* John Roddy, *The Federal Computer Systems Protection Act*, 7 RUTGERS COMPUTER & TECH. L.J. 343 (1979); Joseph B. Tompkins, Jr. & Linda A. Mar, *The 1984 Federal Computer Crime Statute: A Partial Answer to a Pervasive Problem*, 6 COMPUTER/L.J. 459 (1986); Darryl C. Wilson, *Viewing Computer Crime: Where Does the Systems Error Really Exist?*, 11 COMPUTER/L.J. 265, 268 (1991). The proposed statute would have criminalized the "manipulation or attempted manipulation" of any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce, for the purpose of "devising or executing any scheme or artifice to defraud," or of "obtaining money, property, or services . . . by means of false or fraudulent pretenses, representations, or promises. . . ." S.240, 96th Cong. (1979).

[33] Enacted as The Counterfeit Access Device and Computer Fraud and Abuse Act, Pub. L. No. 98-473.

[34] *See* Pub. L. No. 98-473.

to the full House of Representatives, the House Committee on the Judiciary noted that, "[t]here is no specific Federal legislation in the area of computer crime. Any enforcement action in response to computer-related crime must rely on statutory restrictions that were designed for other offenses, such as mail fraud (18 U.S.C. § 1341) or wire fraud (18 U.S.C. § 1343) statutes."[35] Concluding that reliance on such statutes would frustrate prosecutors and allow computer-related crimes to go unpunished,[36] the Committee recommended, and Congress enacted, § 1030 as a "computer-specific" criminal statute. In so doing, the lawmakers rejected the possibility of amending existing legislation and opted instead to attack this "new" kind of criminal conduct by enacting a new, particularized kind of criminal statute.

The CFAA[37] prohibits a variety of acts involving the use of computers. However, with the partial exception of one section,[38] all six sections of the CFAA focus on unauthorized computer access which leads to, or furthers, some additional criminal end.

Paragraph (a)(1) prohibits obtaining information "that has been determined by the United States government, pursuant to executive order or statute, to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in . . . the Atomic Energy Act of 1954," when that information is obtained by gaining knowingly unauthorized access to a computer, and when the person who obtains that information has the "intent or reason to believe that such information so obtained is to be used to the injury of the United States or to the advantage of any foreign nation." Thus, in essence, section (a)(1) prohibits obtaining "what generically is considered to be classified information."[39]

Paragraph (a)(2) provides for punishment of

> whoever intentionally accesses a computer without authorization, or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution[40] or of a card issuer as defined in § 1602(n) of Title 15, or contained in a file of a consumer

---

[35] H.R. REP. NO. 98-984 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3691.

[36] *See id.* at 3691-92.

[37] As detailed *infra*, the statute was amended in 1986 and again in 1994. Of the current statute's six provisions, three remain unchanged or nearly so from the 1984 enactment. Two were added in 1986; one section was added by the 1994 amendments. For a description and analysis of the 1984 act, see Glenn D. Baker, *Trespassers Will Be Prosecuted: Computer Crime in the 1990s*, 12 COMPUTER/L.J. 61 (1993). *See also* Tompkins & Mar, *supra* note 32.

[38] *See* § 1030(a)(3) (discussed *infra*).

[39] H.R. REP. NO. 98-894 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3706.

[40] Defined in § 1030(e).

> reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. § 1681 *et seq.*).

Like paragraph (a)(1), this provision does not penalize simply accessing a computer, but only obtaining certain information by means of such access. The statute prohibits the act of obtaining such information without authorization, but its language is explicitly limited to the obtaining of information by means of unauthorized access to a computer.

Paragraph (a)(3) is the only provision of § 1030 which, at least in part, prohibits simple unauthorized access. That section prohibits intentional unauthorized access of any computer that is "exclusively for the use of the Government of the United States." It also prohibits unauthorized access of any computer used not exclusively by the federal government, but only when such access "adversely affects the use of the Government's operation of such computer." Thus, a hacker's accessing of a computer used exclusively by the government would itself be a federal crime. If that computer is shared by the federal government and some other entity, however, the access is criminal only if it "adversely affects"[41] the government's use. The first part of paragraph (a)(3), the "trespass" provision, prohibits "entry" into a computer. As such, it is the only provision of federal law that criminalizes a result possible only with the use of a computer.

Paragraph (a)(4) of the CFAA punishes fraud by computer. Despite the title of the statute, this is the only subsection that directly addresses fraudulent conduct. Conviction under this provision requires proof that a defendant actually obtained "anything of value," acted with intent to defraud, and accessed a government computer as part of the fraudulent scheme.

Paragraph (a)(5), as amended in 1994, is the "virus statute." That section prohibits the unauthorized transmission, by means of a computer used in interstate commerce or communications, of "a program, information, code or command" that causes loss or damage of the value of $1000 or more, or that "modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care" of any individual. If the transmission is accomplished with intent to cause damage or to "withhold or deny" use of a computer, the conduct amounts to a felony; if done with reckless disregard, it is a misdemeanor.

The 1994 amendment completely revised the previous section (a)(5), which itself had been added to the CFAA in 1986. The 1986 Act focused

---

[41] The 1984 statute referred only to the "affecting" of a government computer, language that was criticized as overly broad and vague. *See infra* note 109.

on actions stemming from unauthorized access of a "federal interest computer." As with virtually all of the provisions of the CFAA, this section did not prohibit simple unauthorized access. Instead, (a)(5) prohibited unauthorized access only when it resulted in the alteration, damage, or destruction of information in a federal interest computer that caused loss of value of $1000, or in the alteration, damage, or destruction of certain medical information[42] located in a federal interest computer; or when it prevented authorized use of that computer and thereby either caused the loss of value over $1000 or the modification or impairment of medical information.

The final substantive provision of the CFAA, § 1030(a)(6), imposes liability upon whoever "knowingly and with intent to defraud traffics (as defined in § 1029) in any password or similar information through which a computer may be accessed without authorization." This subsection is "aimed at penalizing conduct associated with 'pirate bulletin boards' where passwords are displayed that permit unauthorized access to others' computers."[43] While Congress's concern with "trafficking" in passwords is related to other concerns addressed in § 1030, this provision does not directly punish unauthorized access nor, despite the title of § 1030, does it punish fraud.

The only reported appellate decision interpreting § 1030 arose under subsection (a)(5).[44] In *United States v. Morris*,[45] the court upheld a conviction under the portion of that section which prohibited intentionally accessing "federal interest computers" without authorization and thereby damaging or preventing authorized use of those computers, causing a loss of $1000 or more. The defendant, a computer-science graduate student and the son of a computer security expert at the National Security Administration, had a particular interest in the security of computer networks and had identified several "security defects"[46] in the nationwide Internet network.[47] Morris developed and then released onto the Internet

---

[42] Defined in the same language as the "medical" provision of the current § 1030(a)(5)(B).

[43] S. REP. No. 99-432 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2490.

[44] Congress substantially amended paragraph (a)(5) in 1994. *See infra* note 56 and accompanying text.

[45] 928 F.2d 504 (2d Cir. 1991).

[46] *Id.* at 505.

[47] The Internet was described by the *Morris* court as "a group of national networks that connect university, governmental, and military computers around the country. The network permits communications and transfer of information between computers on the network." *Id.* The court's limited description of the Internet was already somewhat outdated in 1991.

a "worm,"[48] a program designed to travel from one computer to another by exploiting the security lapses he had uncovered.[49]

Morris was convicted under § 1030(a)(5), for intentionally accessing a "federal interest computer" without authorization, and thereby damaging or preventing the authorized use of that computer. On appeal to the Second Circuit, Morris raised two issues of statutory construction, both matters of first impression under the CFAA: (1) whether the statute required proof not merely of intent to gain access, but of intent to damage or prevent authorized use, and (2) what evidence would establish "access without authorization" within the meaning of the statute.[50]

The intent issue arose from the ambiguous language of the statute: (a)(5) penalized one who "intentionally accesses . . . and by means of . . . such conduct . . . damages . . . or prevents authorized use." The question on appeal was whether "intentionally" applied merely to the access or to the results of that access. The issue was crucial here, as in

---

[48] As the *Morris* court explained, "In the colorful argot of computers . . . a 'worm' is a program that travels from one computer to another but does not attach itself to the operating system of the computer it 'infects.' It differs from a 'virus,' which is also a migrating program, but one that attaches itself to the operating system of any computer it enters and can infect any other computer that uses files from the infected computer." *Id.* n.1. Interestingly, Morris himself referred to the program as a virus, KATIE HAFNER & JOHN MARKOFF, CYBERPUNK: OUTLAWS AND HACKERS ON THE COMPUTER FRONTIER 321 (1991); but the repeated use of the term "worm" by the media, by "expert" commentators, and ultimately by the court, caused Morris's program to be dubbed indelibly "the Internet worm."

[49] Morris released the worm on the evening of November 2, 1988, from a computer at the Massachusetts Institute of Technology. He had designed the program to move from one computer to another at a controlled rate and to "occupy little computer operation time, and thus not interfere with normal use of the computers." *Morris*, 928 F.2d at 505-06. However, Morris miscalculated both the rate at which the program would spread and its capacity for accumulating multiple copies of itself on a single computer. *See* HAFNER & MARKOFF, *supra* note 48, at 303, 339. The worm replicated itself so quickly that "many machines at locations around the country either crashed or became 'catatonic.'" *Morris*, 928 F.2d at 506. When Morris realized, later that night, that the worm had reproduced on this unforeseen scale, he attempted to send instructions for "killing" the worm; but the network was so clogged by the worm that the messages failed to arrive in timely fashion. *See id.* During the hours after the worm's release, computer operators and programmers at universities and government facilities watched in horror—and fascination—as their machines became inoperable. Presented with this unprecedented challenge, programmers succeeded quickly in isolating the worm, "decompiling" its code, and ultimately killing it. *See* HAFNER & MARKOFF, *supra* note 48, at 258. No data were lost from any computer; no files were "stolen;" Morris neither obtained nor sought to obtain anything. Nevertheless, the value of the computer "down" time was considerable. *See Morris*, 928 F.2d at 506. More important than any actual damage, or even inconvenience, the incident was experienced by the computer community, and was presented in the popular media, as a dramatic illustration of the vulnerability of computers and computer networks. *See* HAFNER & MARKOFF, *supra* note 48, at 312-13.

[50] *See Morris*, 928 F.2d at 504.

many other computer-related prosecutions, because the evidence clearly established that Morris intended no damage. His intent was instead "to demonstrate the inadequacies of current security measures on computer networks."[51] Morris regarded the exercise as a game, a challenge to his technological prowess, and a means of improving network security by pointing out its weaknesses.[52] The court, relying heavily on legislative history as well as the language of the statute itself, held that proof of intentional access was sufficient to establish liability.[53] The court held damage, in effect, to be a strict-liability element of (a)(5).[54] The 1994 amendments to (a)(5), enacted in substantial part as a response to this incident and the threat it was perceived to represent (although not as a response to the decision actually rendered in the case), significantly altered the law on this point. As amended, the statute no longer requires proof of "intentional access," but does require proof of scienter as to damage or denial of authorized use. Liability now is established by evidence that the defendant without authorization "knowingly" caused the transmission of a program, with intent to damage or deny use of a computer or network,[55] or with reckless disregard of the substantial and unjustifiable risk of doing so.[56] Under the 1994 statute, ironically, Morris would have been guilty at most of a misdemeanor, rather than the felony of which he was convicted.

The statutory meaning of "access without authorization" was a significant appellate issue because, as the court noted, Morris was authorized to use computers at Cornell, Harvard, and Berkeley, all of which were on the Internet. As a result, Morris was authorized to communicate with other computers on the network, at least for some purposes.[57] Because it was undisputed that he was authorized to access the network, Morris argued that "his conduct constituted, at most, 'exceeding authorized access,' rather than the 'unauthorized access' that [(a)(5)] pun-

---

[51] *Id.* at 505.

[52] Such "demonstrations" had been typical of the computer community since computers first became available, and comprised an important tool for improving performance and security. *See* HAFNER & MARKOFF, *supra* note 48, at 266-67, 280, 337; Anne W. Branscomb, *Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime*, 16 RUTGERS COMP. & TECH. L.J. 1 (1990). Morris's father and his colleagues had engaged in many such "demonstrations" in the infancy of the computer age. *See* HAFNER & MARKOFF, *supra* note 48, at 266-67, 280. The manager of the Berkeley computer facility testified at trial that the network was more secure as a result of Morris's "demonstration." *See id.* at 335.

[53] *See Morris*, 928 F.2d at 506-09.

[54] *See id.* at 509.

[55] *See* 18 U.S.C. § 1030(a)(5)(A) (1995).

[56] *See* § 1030(a)(5)(B).

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

ishes,"[58] an argument that would appear to have considerable force. The court held, however, that because Morris used certain features in ways unrelated to their intended functions,[59] his conduct amounted to "access without authorization." This dubious reasoning[60] was accompanied by a more forceful, and certainly more widely applicable, rationale. The Second Circuit cited with approval the trial court's reasoning that the worm was designed to spread to other computers at which he had no account and no authority to gain access to computers at which he had no account by guessing their passwords. Accordingly, the evidence did support the jury's conclusion that defendant accessed without authority as opposed to merely exceeding the scope of his authority.[61]

Morris was authorized to enter the network, but he did not thereby have authority to enter every computer connected to that system. He had gained access without authorization, and had thus properly been found guilty.[62]

The Second Circuit's opinion in *Morris* remains the only reported appellate decision to date under § 1030. While the 1994 amendments to the CFAA substantially modified and clarified the law regarding intent to cause damage, the decision retains a unique place in the developing law of computer crime.

III. THE COMPUTER-SPECIFIC APPROACH

The approach adopted by federal lawmakers and most state legislatures has been to enact statutes aimed specifically at criminal conduct that involves the use of computers, such as computer-specific criminal statutes. This approach proceeds from the view that criminal conduct accomplished with the use of a computer is inherently different from con-

---

[58] *Id.*

[59] *See id.* at 510.

[60] The statute prohibited unauthorized access, not the creative use of computer programs.

[61] *Morris*, 928 F.2d at 510.

[62] It was undisputed that Morris had no intent to cause damage to any computer, and that he neither gained nor sought to gain anything of value for himself. His crime was his unauthorized access, coupled with the unforeseen and unintended "crashing" of numerous computers. Had he correctly calculated the rate of the worm's reproduction, and had the worm's presence been discovered only by a few observant systems managers, he would have committed no crime at all under the 1986 statute. The lack of his intent to cause harm probably explains the relative leniency of the sentence imposed. *See* Brenda Nelson, *Straining the Capacity of the Law: The Idea of Computer Crime in the Age of the Computer Worm*, 11 COMPUTER/L.J. 299, 308 (1991); HAFNER & MARKOFF, *supra* note 48, at 345-46. Although Morris's violation was punishable by imprisonment of up to five years under § 1030(c)(3)(A), he was sentenced instead to probation, community service, and a fine.

duct accomplished by other means; and therefore criminal statutes of general application inadequately address computer-related crime. However, legislative action premised on that view leads to the enactment of statutes that are unnecessary and ineffective, and the criminalization of conduct that, if done without a computer, would not be criminal.

A. The Rationale

Congress's rationale in enacting the computer-specific CFAA is amply documented in the legislative history. The 1984 House Judiciary Committee Report noted that "[t]here is no specific Federal legislation in the area of computer crimes. Any enforcement action in response to computer-related crime must rely on statutory restrictions that were designed for other offenses . . . ."[63] Similarly, the Senate Report on the 1986 amendments[64] stated that prior to 1984, "[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."[65] Both reports thus reflect the view that computer-related criminal conduct is inherently different from other criminal conduct, that crimes involving the use of a computer comprise an entirely new category of criminal conduct, and therefore that "non-computer-specific" criminal statutes are inadequate to combat computer-related crime. The same concern was voiced with regard to the earlier proposed legislation:[66] "Federal prosecutors have been handicapped because they have had to construct their cases on laws that did not envision the technical aspects of computer crime."[67]

To illustrate this concern, the House Report cited *United States v. Seidlitz*,[68] one of the earliest computer-related prosecutions. Seidlitz had designed a communications software program for a federal agency; he subsequently resigned his job. Several months later, he was detected accessing his former employer's computer in Maryland by modem from his own office in Virginia, and downloading restricted information about that program. Because no computer-specific federal statute existed, the jury convicted Seidlitz of wire fraud under 18 U.S.C. § 1343.

That statute prohibited, among other things, transmission by wire communication of any "writings, signs, signals, pictures or sounds" for

---

[63] H.R. REP. NO. 98-894 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689.

[64] See S. REP. NO. 99-432 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, which was written to accompany both the House and Senate bills.

[65] *Id.* at 2480.

[66] *See* S. 240, 96th Cong. (1979).

[67] 125 CONG. REC. H710 (January 23, 1979).

[68] 589 F.2d 152 (4th Cir. 1978).

the purpose of executing a scheme to defraud or to obtain money or property by means of false or fraudulent pretenses or representations." Seidlitz's use of another employee's user access code[69] constituted the "false or fraudulent pretenses or representations" prohibited by the statute. His use of telephone lines to gain access to the system and his typing of computer commands were so obviously sufficient to constitute "transmi[ssion] by means of wire communication" of "writings, signs, [or] signals," that no issue was raised on appeal with regard to these elements of the statute. Moreover, no question was raised even as to whether the electronic information that Seidlitz downloaded amounted to "property" within the meaning of § 1343. In short, the case presented no substantial legal questions as to the applicability of the wire-fraud statute to the computer setting. Seidlitz was convicted, and his conviction upheld.

Despite the fact that § 1343 had proven adequate to address Seidlitz's conduct, the House Report explicitly pointed to *Seidlitz* as an example of the need for computer-specific legislation. In explaining why *Seidlitz* demonstrated that need, the Report noted the Justice Department's opinion that "there would have been no basis for Federal prosecution" had the defendant not accessed the computer using interstate telephone lines.[70] The Report made much the same point as to the only other example cited, *United States v. Langevin*.[71] According to the Report, the defendant, a financial analyst, used an employee's password to access by telephone and modem financial information from a computer at the Federal Reserve Board.[72] The defendant was convicted under § 1343 but, the Report noted, there would have been no conviction had his access calls not crossed state lines.[73] The clear thrust of the Report is that but for the happenstance of interstate phone access calls, neither of these incidents would have constituted a crime; therefore a technology-specific statute was necessary.

---

[69] Described unblinkingly by the court as "the user's personal initials." *See id.* at 153-54 n.2. The science of computer security was then in its infancy.

[70] *See* H.R. REP. NO. 98-894 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3692.

[71] *See generally* H.R. REP. NO. 98-894 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3692 (discussing *Langevin*, an unpublished decision).

[72] *See also* Jonathan Fuerbringer, *Details on Fed Data Theft*, N.Y. TIMES, Jan. 12, 1983 at D1; Al Kamen, *Former Fed Aide Pleads Guilty to Tapping Files*, WASH. POST, Jan. 12, 1983 at F6. Both newspapers reported that, following this incident, the Federal Reserve Board had altered its computer security system, so that "access from the outside is no longer possible." Thus, no one would be able to repeat Langevin's crime.

[73] *See* H.R. REP. NO. 98-894 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3692.

B. *Problems with the Computer-Specific Approach*

1. Redundancy

The CFAA, and indeed most computer-specific legislation, is duplicative of existing criminal statutes.

The two cases cited in support of the CFAA, *Seidlitz* and *Langevin*,[74] could have been prosecuted under a number of federal statutes that were in effect prior to 1984 and that were not computer-specific. By using the password of a federal employee to gain access to the Federal Reserve computer, Langevin could well be described as having "falsely assume[d] or pretend[ed] to be an officer or employee of the United States . . . (and thereby) demand[ed] or obtain[ed] any . . . thing of value," a felony under 18 U.S.C. § 912. The same might be said of Seidlitz, because he used the access code of an employee assigned directly to a project of a federal agency.

Both might have been convicted of felonies under 18 U.S.C. § 1001, which punishes anyone who, "in any matter within the jurisdiction of . . . the United States, knowingly and willfully falsifies, conceals or covers up by any trick, scheme, or device a material fact, or makes any false, fictitious or fraudulent statements or representations, or makes or uses any false writing or document. . . ." Langevin, arguably, could have been convicted under 18 U.S.C. § 1005 for making a "false entry in any book, report or statement of [any Federal Reserve] bank," or under 18 U.S.C. § 1344 for executing or attempting to execute a scheme fraudulently to "obtain any . . . property owned by, or under the custody or control of, a financial institution." Both Seidlitz and Langevin might have been criminally liable for theft of government property under 18 U.S.C. § 641, which prohibits the embezzlement or knowing conversion of "any record, voucher, money, or thing of value of the United States . . . or any property made . . . under contract for the United States."

These cases do not provide the asserted support for the conclusion that enactment of computer-specific legislation was, or is, the only way to combat computer-related crime. Seidlitz and Langevin were successfully prosecuted under other federal statutes, and could have been prosecuted under any of several others.[75]

---

[74] *See supra* notes 68-72 and accompanying text.

[75] Moreover, the statute that was enacted, in part on the strength of those cases, does not and cannot reach every computer-related crime. Federal jurisdiction under § 1030 is triggered only by conduct that involves some specified federal interest. The 1986 Senate Report accompanying the amendments to the CFAA explicitly notes the Judiciary Committee's rejection of the idea that "Congress should enact as sweeping a Federal statute as

Section (a)(1) of the CFAA prohibits the unauthorized use of a computer to obtain classified information.[76] Federal law prohibited obtaining such protected or restricted data, whether by use of a computer or otherwise, even before 1984. Under 18 U.S.C. § 793, it is a crime for any person "for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation," to copy, take, make, or obtain any "sketch, photograph, . . . map, . . . document, writing, or note of anything connected with the national defense."[77] This statute proscribes a wide range of activities designed to obtain classified or defense-related information, and at the same time proscribes obtaining or attempting to obtain "*anything* connected with the national defense." It therefore encompasses the more specific conduct prohibited by § 1030(a)(1) (accessing a computer) and the more specific result (obtaining restricted "information"). Moreover, both statutes prohibit virtually the same criminal intent and purpose.[78] Indeed, in its report on the 1984 version of (a)(1), the Judiciary Committee specifically noted that the language of that provision[79] had been altered to conform with existing espionage laws.[80]

Thus, these two federal statutes seek to prohibit precisely the same evil: obtaining national-defense information with the intent that that information be used against the interests of the United States. One of those statutes, 18 U.S.C. § 793, attacks that evil by focusing on the act of obtaining information; the other, 18 U.S.C. § 1030(a)(1), does so by focus-

---

possible so that no computer crime is potentially uncovered. The Committee . . . prefers instead to limit Federal jurisdiction over computer crime to those cases in which there is a compelling Federal interest, i.e., where computers of the Federal Government or certain financial institutions are involved, or where the crime itself is interstate in nature." S. REP. NO. 99-432 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2482. It is not the use of a computer per se that triggers federal jurisdiction over "computer crimes," but the presence of some "compelling federal interest," a circumstance common to all federal criminal jurisdiction. Thus, the statute presents the same jurisdictional limitations that Congress found to be fatal flaws in the wire fraud and other non-computer-specific statutes.

[76] *See supra* note 39 and accompanying text.

[77] 18 U.S.C. § 793 (1995). Also prohibited is a host of other activities undertaken for the same purpose. *See id.*

[78] "Whoever, for the purpose of obtaining information respecting the national defense, with intent or reason to believe that the information is to be used to the injury of the United States or to the advantage of any foreign nation . . . ." § 793. "Whoever, . . . by means of [accessing a computer] obtains [restricted national-defense] information, with the intent or reason to believe that such information so obtained is to be used to the injury of the United States or to the advantage of any foreign nation." 18 U.S.C. § 1030(a)(1) (1995).

[79] Designated at that time as 18 U.S.C. § 1030(a)(2).

[80] *See* H.R. REP. NO. 98-894 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3707.

ing on one specific manner of obtaining the information. Thus, any potentially criminal conduct prohibited by § 1030(a)(1) would concomitantly be prohibited by § 793; thus, the proscriptions of § 1030(a)(1) are simply superfluous.

No reported prosecutions have been commenced under the provisions of (a)(1), even though at least potential violations have occurred,[81] thus suggesting that the statute may be unnecessary to combat computer-related espionage.

Indeed, the only reported "espionage" case involving the unauthorized use of computers was prosecuted under § 793, the much older, pre-electronic espionage statute,[82] and not under § 1030(a)(1). In 1989, a federal grand jury in San Jose, California, indicted Kevin Poulsen on numerous charges of computer-related criminal activity. A superseding indictment, filed in 1992, added a count charging Poulsen with "gathering of defense information," under 18 U.S.C. § 793(e), arising from his possession of computer tapes containing United States Air Force Air Tasking Orders.[83] The indictment alleged that Poulsen obtained ac-

---

[81] In May 1994, British authorities arrested a 16-year-old hacker (known as "Datastream") who had gained access to numerous Pentagon computers in the United States and abroad, including more than 150 intrusions into the U.S. Air Force "superlab" in Rome, New York; he had obtained access, inter alia, to files containing confidential U.S. reports regarding nuclear inspections in North Korea. He was also reported to have gained access to "top secret files on ballistic weapons research." Nick Hopkins, *War Games Boy, 16*, DAILY MAIL, Jan. 3, 1995, at 27. An Air Force spokesman, however, stated that "there was nothing confidential, nothing classified on the computers." *British Teen-Ager Tapped U.S. Defense Computers*, BALTIMORE SUN, Jan. 9, 1995, at 3A. He was charged under the British Computer Misuse Act, but not under § 1030 or any other U.S. law, despite the fact that U.S. law enforcement agencies, including the FBI and the Air Force Office of Special Investigations, had been probing the "attack" for months and succeeded in tracking down his address. *See* Carl Weiser, *Details Unfold on Hacking of Air Force Computers*, GANNETT NEWS SERV., May 17, 1995.

In an apparently separate episode, officials of the Department of Defense reported ongoing computer intrusions in 1994 in which hackers "stole, altered, and erased records, and . . . obtained access codes to over 100,000 computer accounts," including accounts at the Pentagon's unclassified military network. *See* Bob Brewin and Elizabeth Sikorowsky, *Hackers Storm DOD Nets*, FED. COMPUTER WK., July 11, 1994, at 1; *Pentagon Pirates Remain Untraced*, HOUSTON CHRONICLE, July 22, 1994, at A16. No prosecutions have been reported in connection with these intrusions. The actual extent of these intrusions, and the damage, if any, that they caused was the subject of wildly varying published accounts. Newspaper accounts published on the same day cited Pentagon officials as saying that hackers had not endangered vital defense information, that the "command and control of the Defense Department is in no danger." *Hackers Keep Eyes on Defense*, ROCKY MOUNTAIN NEWS, July 22, 1994, at 46A. The intruders had taken over whole defense systems and were affecting the defense department's military readiness, and that "estimating exactly the extent of the intruder activity is very difficult." *Hackers Elude Pentagon, Tap Into Files*, ORLANDO SENTINEL, July 22, 1994, at A10.

[82] Originally enacted in 1917.

[83] *See* United States v. Poulsen, 41 F.3d 1330, 1333 (9th Cir. 1994). The court ex-

cess codes to a United States Army computer network, and used them to obtain the tasking orders.

Assuming that the orders constituted information that "require[d] protection against unauthorized disclosure for reasons of national security," and assuming that Poulsen could have been charged with obtaining that information by using the access codes without authorization, his conduct appears to fall precisely within the intended scope of (a)(1). Yet the U.S. Attorney determined that the prohibition of § 793 against "unauthorized possession of . . . information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States"[84] was adequate to prosecute Poulsen. Thus, even though the alleged espionage activities were conducted by computer, and even though the information obtained thereby was on computer tapes, the prosecution bypassed the computer-specific provisions of § 1030(a)(1) and relied successfully on the more general proscriptions of § 793.

If § 1030(a)(1) is unnecessary as a tool to prosecute unauthorized obtaining of classified information by computer, it may be worth examining the reason for its enactment in the first place.[85] The 1984 Act[86] was introduced on the floor of Congress in 1983, only months after the release of the popular film "War Games." That film depicted a teenaged computer hacker who, thinking he was merely playing a game, inadvertently accessed a Department of Defense computer system and nearly precipitated thermonuclear war.[87] The film, although an early example of the presentation of computer "crime" in the popular media, sounded themes that continue to reverberate in our social, cultural, and legislative perception of computers: the awesome, virtually uncontrollable power of computers; the clear division between those who have technological expertise and those who do not; the positioning of the young, particularly teenaged males, as foremost among the former, and the corresponding placement of older persons (i.e., anyone who has not grown up with computers as a fact of daily life, including, presumably, most legislators) among the latter; and the dangerously irresponsible behavior displayed by computer-savvy youth. Those perceptions permeate not only the re-

---

plained that "Air Tasking Orders" list "targets that the United States Air Force will attack in the event of hostilities." *Id.*

[84] 18 U.S.C. § 793(e) (1995).

[85] Congress enacted the predecessor to the existing section (a)(1) in 1984 as part of a more limited Computer Fraud and Abuse Act; the previous (a)(1), however, is identical in all pertinent respects to the present provision.

[86] Pub. L. No. 98-473, 98 Stat. 2190.

[87] Activation of the missiles, and the destruction of the human race, were narrowly averted—again by dint of the young hacker's prowess—in the dramatic climax.

sponse to computers and computer culture in the popular media, but in our legislatures as well. The House Report supporting the passage of the 1984 CFAA specifically referred to testimony describing "War Games" as a "realistic representation of the automatic dialing and access capabilities of the personal computer,"[88] and thus, apparently,[89] of the threat to computer security presented by those capabilities.[90]

Paragraph (a)(1) of § 1030 prohibits conduct already defined as criminal under other federal statutes, and thus, as a legislative matter, is simply unnecessary. That statute does, however, respond quite neatly to the specter of a hacker who accesses a military computer and obtains information that could, and almost does, cause a nuclear war.[91]

---

[88] H.R. REP. NO. 98-894 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3696.

[89] That testimony referred explicitly to "automatic dialing and access capabilities," i.e., the ability of a computer to dial a very long series of phone numbers in order to locate one that gave access to a computer, a comparatively simple and, in itself, utterly harmless task. The testimony cited in the House Report did not provide support for the idea that the film offered a "realistic representation" of the possibility of using a computer to access an Air Defense Command computer, and to then "convince" that computer to launch thermonuclear weapons.

[90] The New York Times, in a decidedly unauthoritative assessment of the technological plausibility of popular computer-centered films, concluded that the events depicted in "War Games" were in fact "probably" impossible. *See* Victor Chen, *Your Home Computer Would Scoff at These Plots*, N.Y. TIMES, May 28, 1995, § 2 at 11.

[91] The reference here to this motion picture is not as incidental or as frivolous as may first appear. It may be difficult to identify any other criminal statute supported on the floor of Congress by, inter alia, a specific citation to an utterly fictional "crime." Nor was the Judiciary Committee's report in 1984 the only occasion on which "War Games" has been used as a frame of reference for actual conduct. When Kevin Poulsen was arrested in late 1983 after a series of "electronic break-ins" at defense-related facilities, his arrest was reported under a headline announcing, "UCLA War Games Arrest." Jonathan Littman, *The Last Hacker*, L.A. TIMES, Sept. 12, 1993, (Magazine) at 18. The British hacker known as "Datastream" arrested in 1994 was described by a Scotland Yard detective as being "just like the character in War Games." Hopkins, *supra* note 81. When the U.S. space agency, NASA, announced its move to a new Mission Control facility, the head of its Systems Division explained the need to spend $2.8 million in computer security by saying, "You've seen the movie War Games, right? Let's say someone decides to play 'Space Shuttle.'" Dan Feldstein, *NASA Wants Top-Flight Computer Security*, HOUSTON POST, Dec. 7, 1994, at A19 (quoting Systems Division Chief John Muratore). When officials at the North American Aerospace Defense Command (NORAD) denied in 1995 that the hacker Kevin Mitnick had penetrated its computer system, it was noted that "[e]ver since the 1980s movie War Games suggested that their computers could be accessed and sabotaged, NORAD has dispelled periodic rumors that the latest computer genius has broken into its system." Dick Foster, *Computers Are Secure, NORAD Says*, ROCKY MOUNTAIN NEWS, Feb. 18, 1995, at 33A.

In a 1985 incident, seven teenagers were charged with theft by computer under New Jersey law; they had, police said, exchanged stolen credit card numbers, traded "secret" phone numbers, and bypassed long-distance telephone charges. The most startling allegation, however, was Middlesex County Prosecutor Alan Rockoff's statement that they had been "changing the positions of satellites up in the blue heavens," a statement that led to the description of their exploits as "the latest real-life version of War Games." In

The 1984 Committee reported that section (a)(2)[92] was designed to punish:

> offenses that may be committed with respect to the type of information protected by the Right to Financial Privacy Act [12 U.S.C. § 3401 et seq.] or the Fair Credit Reporting Act [15 U.S.C. § 1681 et seq.]. . . . The substantive information that would be protected by this provision is information that is within the scope of [those two statutes].[93]

Congress had already criminalized the execution, or attempt to execute, any scheme to defraud a financial institution or to obtain "any . . . of the moneys . . . or other property owned by, or under the custody or control of, a financial institution by means of false or fraudulent pretenses, representations, or promises."[94] The Committee had no comment as to why, if such information was already protected under existing law, and if even the attempt to obtain "any property" owned by or under the custody of a financial institution was already defined as criminal, the provisions of § 1030(a)(2) were necessary at all.

Whether the information is obtained by unauthorized use of a computer, or a copier, or by any other kind of "false or fraudulent representation," amounts to no more than a detail. If Congress intended simply to prohibit unauthorized persons from obtaining this financial information, that aim had been thoroughly accomplished already by the language of 18 U.S.C. § 1344, the bank fraud statute. Any question as to whether the "information" protected by § 1030(a)(2) constituted the "property" protected by § 1344 (a dubious question, given the "any property" language of the bank fraud statute) easily could have been resolved by amending the language of § 1344 to make specific reference to such information. The use of a computer is not the evil that needed legislative attention; that evil was, instead, the gaining of unauthorized access to financial data no matter how accomplished—a matter that Congress had already addressed.

No prosecutions have been reported under this provision, even though, as with (a)(1), potentially appropriate circumstances have arisen. Intrusions into automatic teller banking machines could, ostensibly, be

---

fact, they had not altered the path of any satellite; the computers that control those satellites were, and are, not accessible by outside phone lines. *See* Philip Elmer-DeWitt, *The Great Satellite Caper*, TIME, Aug. 29, 1985, at 65.

[92] Designated at that time as (a)(3).

[93] H.R. REP. NO. 98-894 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3707.

[94] 18 U.S.C. § 1344(a)(2) (1989). By a 1989 amendment, Congress imposed penalties under this statute of up to $1 million or imprisonment of up to 30 years, or both. *See id.*

prosecuted under this section. Although such incidents have occurred, they have not been pursued under (a)(2).

In April and May 1993, in what was reported as "the first incident of its type,"[95] a "phony" ATM was installed at a shopping mall in Connecticut. When customers attempted to access the machine with their ATM cards, it displayed a message indicating that it was not in working order. In fact, the machine recorded the names and access numbers from the cards. The perpetrators then used that information to produce fraudulent access cards and withdraw over $100,000 from customer accounts.[96] The incident resulted in convictions for bank fraud under 18 U.S.C. § 1344 and for the production of counterfeit access devices (the fake ATM cards) under 18 U.S.C. § 1029.[97] Even though the defendants used a computer (both the fraudulent ATM, and the legitimate ATMs from which they obtained money, were "computers" within the meaning of § 1030), and even though they obtained access to protected "information" by means of unauthorized use of a computer, they were not prosecuted under § 1030(a)(2). The bank fraud and access device statutes, neither of which focuses exclusively on the use of computers, were adequate to support convictions and lengthy sentences.[98] Although the defendants used sophisticated electronic technology to commit this crime, it was simply a new method of committing a very old crime.[99]

Similarly, the Ninth Circuit upheld a conviction for bank fraud under 18 U.S.C. § 1344, where the defendant used an ATM card to access the accounts of bank customers and withdraw money, and then "manipulated data" by means of a computer program to conceal his scheme.[100] Even though the defendant used computers (both the ATM that he accessed and the computer he used to conceal the transactions were computers under § 1030), and obtained financial "information"

---

[95] Kirk Johnson, *One Less Thing to Believe In: Fraud at Fake Cash Machine*, N.Y. TIMES, May 13, 1993, at A1.

[96] *See 2 Sentenced in $100,000 Bank Machine Fraud*, N.Y. TIMES, Dec. 21, 1993, at B5.

[97] *See* United States v. Greenfield, 44 F.3d 1141, 1144 (2d Cir. 1995).

[98] *See id.*; *see also* Mark Pazniokas, *Prison Term Sustained in ATM Scam*, HARTFORD COURANT, Apr. 1, 1995, at B5.

[99] As is typical of many computer-related crimes, the incident was accompanied by some overheated public statements. The chairman of a local computer trade association referred to the perpetrators as "terrorists;" prosecutors called it "the new wave of criminal fraud;" the Assistant U.S. Attorney who prosecuted the case, Ronald Apter, was quoted as saying, "[n]early every ATM user in the country has lost some faith in the integrity and the impregnability of the automated banking system." John Larrabee, *ATM Fraud Nets Prison*, USA TODAY, Dec. 21, 1993, at 3A. It requires no citation to point out that money has been stolen from banks, in a wide variety of ingenious modes, for a very long time.

[100] *See* United States v. Bonallo, 858 F.2d 1427 (9th Cir. 1988).

through unauthorized use of those computers, he was successfully prosecuted under the bank fraud statute, rather than the technology-specific CFAA. The prosecution in *Bonallo* was brought in 1985, only shortly after the enactment of the CFAA. Although one might hazard the guess that the new statutory weapon would have been particularly appealing to the prosecution, the government relied on the older, non-technological statute to reach conduct which the new CFAA seemed to address. Again, the computer-specific CFAA was unnecessary.[101]

Paragraph (a)(3), in part, prohibits unauthorized access to government computers. That conduct certainly may warrant criminal prosecution. Where the act involves some other criminal activity, for example, theft, or where the information is put to some other criminal purpose, such as fraud or espionage, existing statutes provide ample basis for prosecution. Congress's concern in enacting the first portion of (a)(3), however, was with the act of unauthorized access itself, and with the apprehension that non-computer-specific statutes would not reach such access.[102] That apprehension was unfounded.

If such access is accomplished by means of any "false, fictitious, or fraudulent statements," it is prohibited by 18 U.S.C. § 1001; if accomplished by the false or fraudulent use of a federal employee's access code or password, the act is a crime under 18 U.S.C. § 912. If such access is accomplished by use of a computer and modem, and therefore by use of telephone wires, with fraudulent intent, it is prohibited under 18 U.S.C. § 1343. It is difficult to conceive of any unauthorized accessing of government information, whether by computer or by other means, that would not fall within the ambit of one or more of these statutes.

Reportedly, the first indictment ever handed down under § 1030 arose under the "trespass" provision of the 1984 statute.[103] In *United States v. Fadriquela*,[104] the defendant was charged with unauthorized access of a computer at a Department of Agriculture Forest Service facility, and also with wire fraud under § 1343 and making false statements to a

---

[101] In another similar incident, in February, 1995, two people were arrested in Oregon after they apparently broke into a van, stole an ATM access card, and proceeded to withdraw over $300,000 from the victim's bank account by using the stolen access card. *Woman Missing Bank Card Finds She Is Overdrawn $346,770*, N.Y. TIMES, Feb. 12, 1995, at 36. A federal grand jury indicted them, not for violations of (a)(2), but for unauthorized use of an access device under 18 U.S.C. § 1029. Charges of burglary or larceny under state law, or bank fraud under § 1344, could have been equally effective in prosecuting this conduct.

[102] *See supra* note 64 and accompanying text.

[103] *See* Baker, *supra* note 37, at 65.

[104] No. 85-CR-40, U.S. Dist. Ct. (D. Colo. 1985) (unpublished opinion).

federal agency under § 1001. A computer "hobbyist,"[105] the defendant had entered the Forest Service computer using an access code he had obtained from a hacker bulletin board.[106] He obtained no data, damaged no data, and "seemed more interested in experimenting with the system than in destroying any data," according to the Forest Service assistant director of information systems.[107]

Fadriquela moved to dismiss the indictment, challenging the constitutionality of § 1030, and in particular the prohibition against "affecting" a government computer.[108] However, he pleaded guilty to misdemeanor counts of wire fraud, and abandoned the constitutional challenge. To the extent that Fadriquela's conduct was properly regarded as criminal, the provisions of § 1343 were adequate to obtain a conviction. The then-current version of § 1030 was not only unnecessary, but might have been found unconstitutional.

Paragraph (a)(3) also prohibits intentional unauthorized access of a computer used "not exclusively" by the government, when such access "adversely affects the use of[109] the Government's operation of such computer." Precisely why the unauthorized access of a shared computer is deemed a crime only when it "adversely affects" the government's operations, whereas simple unauthorized access is criminal when the computer is used solely by the government, is a question unanswered by the legislative history. However, the statute draws that distinction, and must reflect some legislative determination. Prior to the 1994 amendments, this section referred only to "affecting" the government's use of a shared computer. The amended language refers to access that "adversely affects" the government's use. The effect of that language, and its application to specific factual situations, may not be much clearer than that of the language it replaced.

---

[105] *See* Mitch Betts, *Hacker Sentenced for Accessing U.S. Agency Computers*, COMPUTERWORLD, June 24, 1985, at 26.

[106] *See id.*

[107] Paul Korzeniowski, *Agencies' Hacker Troubles Blamed on Bulletin Board*, COMPUTERWORLD, July 8, 1985, at 1. Fadriquela did no damage; indeed, his conduct resulted in the strengthening of the security of the computer system. "We changed all our passwords. . . . The break-in has turned out to be a learning experience for us." *Id.* (quoting L. Vancil, assistant director of information systems at the Lake Wood, Colo., Forest Service facility). "There is a way to get in [the service's] system that they didn't even know existed—and they have since taken corrective measures." Betts, *supra* note 105, at 26 (quoting Assistant U.S. Attorney Cathy Goodwin). Under those circumstances, perhaps this case was not the most appropriate for establishing precedent under § 1030. " . . . [W]e wanted to get some convictions under the new law." *Id.*

[108] *See* Mitch Betts, *U.S. Attorneys Push to Clarify Vague '84 DP Crime Law*, COMPUTERWORLD, July 1, 1985, at 22.

[109] So in the original.

No appellate decisions have been reported under paragraph (a)(3). The only reported decision of any sort is *Sawyer v. Department of the Air Force*,[110] which involved a computer programmer fired from his Air Force job because he had accessed a computer without authorization, altered contract records, and then submitted fraudulent invoices for which he received over $17,000.[111] However, the decision sets forth virtually no additional factual background or legal analysis, thus providing little guidance or insight about the statute. Moreover, of course, the decision was administrative, not criminal. A reading of the cursory opinion, however, raises the question why, if Sawyer had "improperly" received payments based on "fraudulent invoices" (apparently not involving any accessing or use of a computer), he was discharged under a computer-specific statutory provision that did not even refer to fraud.

Section (a)(4) of the statute prohibits nothing more than garden-variety fraud that happens to involve access to a government computer. Conduct punishable under (a)(4) appears to be as easily punishable under the general fraud statute,[112] or under the federal mail fraud or wire fraud statutes[113] or as common-law fraud. Indeed, the language of (a)(4) specifically excepts from its scope the only kind of fraud that might arguably go beyond the general fraud statute: fraudulent use of the computer itself.[114] The use of a computer is not "anything of value," the obtaining of which would support a prosecution under (a)(4).

Paragraph (a)(5) punishes, in part, unauthorized transmission of information that "modifies or impairs" certain medical data. The prospect of the unauthorized use of a computer to alter medical treatment has been raised as a particularly terrifying type of crime made possible by computer technology. The Senate Judiciary Committee, reporting the 1986 amendments to the full chamber,[115] referred to a 1983 incident in which

> a group of adolescents known as the '414 Gang' broke into the computer system at Memorial Sloan-Kettering Cancer Center in New York [and] gained access to the radiation treatment records of 6,000

---

[110] 31 M.S.P.R. 193 (1986).

[111] The Merit Systems Protection Board found "unpersuasive" Sawyer's claim that he sought merely to "point out deficiencies" in a computer accounting system. The statute requires proof only of intentional access without authorization, so this claim would have been irrelevant in any event.

[112] *See* 18 U.S.C. § 1001 (1989).

[113] *See infra* note 210.

[114] The conduct is punishable "unless the object of the fraud and the thing obtained consists only of the use of the computer." 18 U.S.C. § 1030(a)(4) (1995). The House Report on this provision specifically recommended that mere "'time stealing' . . . should be handled privately or at the State or local level." H.R. REP. NO. 98-894 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3708.

[115] S. REP. NO. 99-432, *reprinted in* 1986 U.S.C.C.A.N. 2480.

> past and present cancer patients and had at their fingertips the ability to alter the radiation treatment levels that each patient received.

In fact, the group neither effected nor apparently even attempted any such alteration. Nonetheless, the Committee relied on the "potential" danger that the situation presented to demonstrate the need for legislation to combat such behavior.[116]

No prosecutions have been commenced to date under the "medical treatment" provision of (a)(5). Indeed, research for this article turned up no reliable reports[117] of any incidents in the United States[118] in which a hacker altered medical data. Lethally erroneous prescription and administration of medicines and medical procedures have, of course, occurred without the involvement of computers.[119] A variety of medical errors has resulted in criminal as well as civil liability.[120] Because

---

[116] The same report refers to the Sloan-Kettering case as "but one example of computer crimes directed at altering medical treatment records." No other example is put forward. *See id.*

[117] In May 1995, newspapers reported that "at least one case of murder by computer has been recorded," as a result of a hacker's alteration of a patient's medication information. The information was attributed to Professor David L. Carter of Michigan State University, who had presented a paper on computer crime to a British law enforcement conference. *See* Ray Moseley, *Organized Crime Going High-Tech, Worldwide in Scope*, SUNDAY GAZETTE MAIL, May 28, 1995, at 11A. In a telephone interview, however, Professor Carter stated that he knew of no such "murder by computer" incident and had not related any such incident to the reporter who interviewed him. He had instead referred to an unsuccessful attempt to tamper with drug dosage information. Telephone Interview with David L. Carter, Professor, Michigan State University (June 26, 1995).

[118] Under Great Britain's Computer Misuse Act of 1990, a nurse pleaded guilty in June 1993 to "unauthorized modification of computer material," for using a computer to prescribe potentially dangerous drugs to a patient. The drugs were not administered; a "sharp-eyed ward sister" noticed the change in prescription. The nurse gained access to the computer system by using the "pin number" of a hospital doctor; he had memorized the doctor's number while observing the doctor's awkward attempts to access the system. *Nurse-Hacker Alters Hospital Prescriptions*, COMPUTER AUDIT UPDATE, Feb. 1994.

[119] In December 1994, in highly-publicized incidents, two patients at the Dana Farber Cancer Institute died after receiving an erroneous dosage of a highly toxic cancer drug four times its correct level. *See* Richard A. Knox & Daniel Golden, *Drug Dosage Was Questioned*, BOSTON GLOBE, June 19, 1995, at 1. At least 13 deaths were reported as the result of the mistaken injection of the cancer drug Vincristine, when medical personnel confused it with another drug. *See* Richard A. Knox, *Response Is Slow to Deadly Mixups*, BOSTON GLOBE, June 26, 1995, at 29. That same article referred to recurring errors in the administration of cancer drugs as a result of disastrous confusion between "look-alike and sound-alike drugs," of illegible handwriting, and of prescriptions that mistake daily doses with multi-day doses. *See id.* Knox also referred to a 1991 Harvard University study that found that 250,000 Americans are injured by medication errors each year. *See id.* These terrifying errors were not the result of unauthorized access into computerized medical databanks.

[120] In New York v. Einaugler, 618 N.Y.S.2d 414 (App. Div. 1994), *review denied*, 647 N.E.2d 459 (N.Y. 1995), a doctor was convicted of recklessly engaging in conduct causing a substantial risk of serious injury, under N.Y. PENAL LAW § 120.20 (McKinney

criminal liability can be, and has been, imposed for such conduct under criminal statutes of general application, it is not apparent why conduct involving the unauthorized use of a computer in a medical setting could not be prosecuted under those same statutes, and why, therefore, a computer-specific statute is needed to address that possibility.

Paragraph (a)(6) prohibits trafficking in passwords or other means by which one may access a computer unlawfully. Title 18 U.S.C. § 1029 prohibits, inter alia, trafficking in "access devices." That term is defined broadly to include "any . . . means of account access."[121] Thus, the language of § 1029 encompasses the narrower language of § 1030(a)(6), so that any act prohibited under (a)(6) would also violate § 1029. Both provisions identify the same mens rea: under each statute, conduct is prohibited when it is done knowingly and with intent to defraud. Accordingly, the proscriptions of (a)(6) appear to be simply redundant and therefore unnecessary. Because no court has yet been called upon to examine the distinctions, or lack thereof, between these two statutes, the view offered here must await judicial confirmation or rejection.

Clearly crimes can be accomplished by means of a computer, and where a sufficient federal interest exists, such crimes warrant federal prosecution. However, the federal statute aimed most specifically at the criminal use of a computer, § 1030, has not yet proved successful in supporting prosecutions that could not have been instituted under other federal statutes. Computer-related crimes have been prosecuted successfully under other, non-computer-specific statutes, both before and after the passage of § 1030. The provisions of § 1030 are largely duplicative of existing statutes. The legislative conclusion expressed by Congress in enacting § 1030, that a computer-specific statute is the only effective way to address such conduct, was not supported by sound evidence presented either at the time of enactment or produced thereafter.

2. Overbreadth: It's the Crime, Not the Computer

Legislation premised on the notion that "computers are different" is likely to be constitutionally overbroad: such legislation reflects and amplifies the conclusion that conduct not otherwise criminal somehow becomes criminal when it is accomplished by means of a computer. That

---

1995), when he fed a patient through a dialysis catheter that he mistakenly thought was a feeding tube.

In April 1995, reckless homicide charges were brought under Wisconsin law against a medical laboratory for misreading the pap smears of two patients who subsequently died of breast cancer. *See* Gina Kolata, *Medical Laboratory Faces Charges in Cancer Deaths*, N.Y. TIMES, Apr. 13, 1995, at A16.

[121] *See infra* note 216 and accompanying text.

approach proceeds from a focus on the computer itself, rather than on harm; on the means rather than the result. The consequence of a computer-specific legislative approach is to invite prosecutorial attention to technology rather than to the culpability of conduct.

The CFAA invites that misdirection of prosecutorial focus; however, because so many of its provisions do little more than duplicate existing criminal statutes, overbreadth is not the major problem with that legislation. At least one provision of the CFAA, however, is clearly overbroad because it prohibits conduct that is not, and probably was not intended to be, criminal. Paragraph (a)(5), as amended in 1994, prohibits, inter alia, the transmission of a "program, information, code or command" to a computer or computer system if the person causing the transmission intends or recklessly disregards the substantial risk that the transmission will damage a computer or prevent the use of that computer. It is not difficult to understand the motivation for this provision: certainly, the possibility of a virus that incapacitates vital government computers, or telephone service, or air traffic control functions, or even large numbers of privately used computers, seems to warrant legislative action. The language of the new provision, however, is overly inclusive.

A computer security professional would be faced with the choice of not testing anti-virus technology or else running the risk of prosecution. Computer science students who write a virus programs as an academic or research exercise could find themselves subject to criminal liability under (a)(5) if they transmit that program to a classmate or a teacher, or if they simply test the program to see if it works. These individuals, by writing and testing virus or anti-virus programs, could be said at least to have disregarded the substantial risk of damaging a computer, and would therefore be engaging in culpable behavior. Although prosecutors might employ their discretion and not pursue charges in such cases, reliance on such discretion is hardly a justification for ignoring fundamental flaws in the statute.[122]

Another section of the CFAA, (a)(6), also lends itself to overbroad interpretation. That section prohibits "trafficking in any password or similar information through which a computer system may be accessed without authorization." Prosecutors sought and obtained indictments under that provision against a defendant[123] who obtained proprietary software, altered it so as to facilitate unauthorized access to computer systems, and then distributed the altered software by making it available through computer bulletin boards. Although versions of the software

---

[122] Prosecutorial discretion has been misused in more than one computer-related prosecution. *See supra* note 29 *et seq.*; *infra* notes 139 *et seq.*, 171 *et seq.*

[123] *See* United States v. Rose (N.D. Ill. 1990) (unpublished opinion).

were widely available through bulletin boards, there was no evidence that the defendant or anyone else had used the altered version to access any computer,[124] and defendant neither made nor sought money for his work, he was charged under § 1030(a)(6).

Rose's defense included an attack on the constitutionality of (a)(6) on the grounds that it could be read to prohibit any discussion of computer security problems and possible solutions; therefore it was overbroad, vague, and violative of First Amendment guarantees. Because Rose's conduct was not even alleged to have included monetary gain, a denial of his motion to dismiss would have effectively rendered such evidence unnecessary to establish "trafficking." If no evidence of sale is necessary to establish trafficking, then simply discussing ways in which a computer "may be accessed" without authorization, regardless of the motive for that discussion, would amount to a federal crime. This intriguing issue was not addressed by the court because shortly after the motion was filed Rose pleaded guilty to one count of wire fraud under § 1343. Thus, at least some of the provisions of the CFAA present problems of overbreadth.

However, a much more striking illustration of an overbroad computer-specific statute is the Communications Decency Act (CDA).[125] That statute prohibits the use of "a telecommunications device" to make available, inter alia, "indecent" material to minors,[126] and the use of "an interactive computer service" to make available "patently offensive" material to minors.[127]

A broad coalition of organizations brought suit on the day the bill was signed into law,[128] seeking an injunction against enforcement of the CDA. In a powerful and lengthy opinion, a three-judge panel[129] upheld

---

[124] *See* Mark Potts, *'Hacker' Pleads Guilty to AT&T Case*, WASH. POST, Mar. 23, 1991, at A1. The Maryland prosecutor, U.S. Attorney Breckinridge Willcox, stated that, "it may be very difficult, if not impossible, to determine what, if any, damage was done." *Man Indicted on Computer Hacking Charges*, UPI WIRE, May 16, 1990.

[125] *See* Pub. L. No. 104-104, § 502, 110 Stat. 56, 133-35 (amending Title V of the Telecommunications Act of 1996, 47 U.S.C. § 223); *see also* ACLU v. Reno, 929 F. Supp. 824, 827 (E.D. Pa. 1996).

[126] *See* 47 U.S.C. § 223(a)(1)(B) (1989).

[127] *See* 47 U.S.C. § 223 (d)(1). The court noted that the statute failed to define the term "telecommunications device." *See ACLU v. Reno*, 929 F. Supp. at 828, n.5. The court also noted the unresolved "tension between the scope of 'telecommunications device' and the scope of 'interactive computer service'. . . ." *Id.* Such definitional problems are typical of statutes written in technology-specific language. *See infra* Part III.B.3, notes 199-206.

[128] February 8, 1996. *See ACLU v. Reno*, 929 F. Supp. at 827.

[129] The panel, consisting of two judges of the United States District Court for the Eastern District of Pennsylvania and one from the Third Circuit, was convened pursuant to the expedited review provisions of the CDA. *See* § 561(a); *ACLU v. Reno*, 929 F. Supp.

the granting of an injunction, holding the statute unconstitutionally vague and overbroad.[130] The court held that, while "obscene" material and "child pornography" were already subject to criminal penalties,[131] "indecent" or "patently offensive" material is protected by the First Amendment.[132]

The court cited numerous examples of "offensive" or sexually-explicit communications that would be subject to criminal penalty under the CDA, even if they are not obscene and even if they provide valuable artistic or informational content, i.e., precisely the sort of communications that cannot constitutionally be prohibited.[133] The use of a computer (a "telecommunications device") to transmit such material cannot make such conduct criminal when it is constitutionally protected in other contexts.[134]

The *ACLU* court held that the democratic conversation[135] fostered by the Internet could not be singled out for criminal prohibition when such conversation was protected in other situations.[136] Constitutional guarantees do not disappear simply because a computer is involved. Congress's short-sighted focus on technology, and on "Internet porn," rather than on established constitutional principles, led it to enact legislation that was overbroad and "profoundly repugnant" to the First Amendment.[137]

Even when a prosecution is based on a non-computer-specific statute, a prosecutorial focus on the computer rather than on the culpability

---

at 827.

[130] *See ACLU V. Reno*, 929 F. Supp. at 856, 858-59, 863. "Any content-based regulation of the Internet, no matter how benign the purpose, could burn the global village to roast the pig." *Id.* at 882.

[131] *See id.* at 829, 857, 865.

[132] *See id.* at 851, 871 n.10.

[133] *See id.* 853. The CDA "would effect a complete ban even for adults of some expression, albeit 'indecent,' to which they are constitutionally entitled . . . ." *Id.* at 854. The statute would thus unconstitutionally force "many speakers who display arguably indecent content on the Internet [to] choose between silence and the risk of prosecution." *Id.* at 849.

[134] "[O]ur fundamental constitutional principles can accommodate any technological achievements, even those which presently seem to many to be in the nature of a miracle such as the Internet." *Id.* at 865 n.9 (separate opinion of Buckwalter, J.).

[135] *See ACLU v. Reno*, 929 F. Supp. at 881.

[136] "[G]overnment-imposed, content-based speech regulations are generally inconsistent with '[o]ur political system and cultural life'. . . ." *Id.* (citing Turner Broadcasting System, Inc. v. FCC, 114 S. Ct. 2445, 2472 (1994)). "There is no question that a Village Green Decency Act, the fruit of a Senator's overhearing of a ribald conversation between two adolescent boys on a park bench, would be unconstitutional." *Id.* at 882 (separate opinion of Buckwalter, J.).

[137] *See id.* at 881 (separate opinion of Buckwalter, J.).

of the conduct can lead to the same faulty conclusion: that the use of a computer itself amounts to a crime.

In *United States v. LaMacchia*,[138] the court dismissed an indictment brought under § 1343, the wire fraud statute, against the operator of a computer bulletin board on which users had made available "pirated" software, software manufactured by private companies intended for sale to consumers. The defendant, a student at the Massachusetts Institute of Technology, was not alleged to have stolen, unlawfully obtained, or gained unauthorized access to any of the software; instead, the prosecution was based on his operation of a bulletin board that other persons used to make the software available. Most crucial to the court's decision, LaMacchia charged nothing for the service, and was not even alleged to have "sought or derived any personal benefit from this scheme."[139]

LaMacchia was charged with conspiring to commit wire fraud, i.e., conspiring with "persons unknown" to devise a scheme to defraud.[140] The essence of the charge was that LaMacchia and his bulletin board users had defrauded the software manufacturers of revenues that the sales of these programs would have generated.[141] Because the amount of pirated software is estimated by the software industry at an astonishing dollar value,[142] the case was regarded as a test of the industry's ability to stop unauthorized copying and distribution. Because LaMacchia did not himself obtain the software, or place it on the bulletin board, or distribute it to users—because he was merely the operator of the bulletin board system (the "sysop")—the case was regarded as a test of the liability of sysops for materials posted by other persons.[143] And because the indictment was dismissed, the case was taken to reflect the inadequacy of § 1343, and indeed of the law generally, to prosecute computer crimes.[144]

---

[138] 871 F. Supp. 535 (D. Mass. 1994).

[139] *Id.* at 537.

[140] *See id.* at 540.

[141] *See id.* at 536.

[142] In 1992, the Software Publishers Association reported in testimony before Congress that software manufacturers were losing $2.4 billion annually as the result of piracy. *See id.* at 540 n.5. In 1993, according to that organization's position statement, an estimated $7.5 billion was lost worldwide in sales of business application software alone. *See Software Publishers Association Position Statement on the* LaMacchia *Decision, reprinted in* PR NEWSWIRE, Jan. 5, 1995.

[143] Massachusetts Institute of Technology (MIT) owned the computer on which the bulletin board operated. MIT was not charged in connection with the case.

[144] *See, e.g.*, Jules Crittenden, *Ruling Clears Way for Computer Bandits*, BOSTON HERALD, Dec. 30, 1994, at 1: "There's no copyright law in cyberspace and computer bandits are free to walk off with all the software they can carry until Congress does something about it, a federal judge ruled yesterday . . . . The . . . decision . . . let one MIT cyberhombre off the hook and could start a software stampede . . . . 'You have Billy the Kid out there with his fancy modem and his computer. He's the new gun-

The decision, although significant, reflects somewhat more modest conclusions about the state of the law.

The problem with the indictment was quite simple: the conduct alleged was not prohibited by the statute. Section 1343 punishes schemes to defraud or to obtain money or property by fraudulent means, and the transmission of "words, pictures, etc." for the purpose of furthering such schemes. The indictment, however, did not allege that LaMacchia had made any misrepresentation, or that he intended to defraud anyone, or that he transmitted anything in order to further a fraud. The indictment did not allege that he had devised a scheme to obtain money or property. Instead, he merely made available, without charge, a communications conduit that others used for their own purposes. Thus, based on the plain language of § 1343, the indictment failed to allege conduct prohibited by that statute. The fact that computer technology was involved did not alter that dispositive fact.

The indictment relied upon § 1343, in effect, as a means of imposing criminal penalties for copyright infringement.[145] The indictment specified the object of the alleged scheme as "the facilitation . . . of the illegal copying and distribution of copyrighted software[146] without payment of licensing fees and royalties to software manufacturers and vendors."[147] But LaMacchia could not have been indicted directly for copyright infringement under 17 U.S.C. § 506, because that statute requires proof that the infringement was pursued "willfully and for purpose of commercial advantage or private financial gain."[148]

LaMacchia, in the tradition of the "hacker ethic," had made his bulletin board service available, not for profit or gain, but to facilitate the exchange of software. Because LaMacchia could not be pursued directly for criminal copyright violation, prosecutors opted instead to rely upon the wire fraud statute. The attraction of § 1343, the *LaMacchia* court noted, was that it required no proof of intent to profit from the scheme.[149] The language of that statute, however, ill described LaMacchia's conduct.

---

slinger,' said Robert Gwin, legal director of the Boston Computer Society." In fact, the case did not address liability for obtaining copyrighted software; LaMacchia was not even alleged to have obtained, or "walked off with," anything. Billy the Kid, according to frontier legend, acted for the purpose of personal gain. LaMacchia, as the court explicitly held, was not even alleged to have done so. *See LaMacchia*, 871 F. Supp. at 537.

[145] *See LaMacchia*, 871 F. Supp. at 537.

[146] Computer programs are subject to copyright protection under the 1992 amendments to 17 U.S.C. § 101. *See id.* at 540 n.6.

[147] *Id.* at 536.

[148] *Id.* at 539 (tracing 17 U.S.C. § 506 (a)). Criminal penalties for copyright infringement are set forth in 18 U.S.C. § 2319 (1995).

[149] *See id.* at 541-42.

The *LaMacchia* court relied heavily on *Dowling v. United States*,[150] where the Supreme Court reversed a conviction for interstate transportation of stolen property under 18 U.S.C. § 2314, holding that criminal statute inappropriate as a copyright-enforcement tool.[151] In *Dowling*, the defendant had engaged in an elaborate scheme to sell unauthorized copies of copyrighted recordings; part of that scheme involved the use of the mails to advertise the pirated records. The *Dowling* court found that although the defendant had criminally infringed on the copyrights, such "interference with copyright does not easily equate with theft, conversion, or fraud."[152]

Congress devoted "a good deal of care" to defining the conduct that would comprise criminal copyright infringement; and those older crimes did not fit that careful definition. An "expansive reading" of those older statutes, equating theft or fraud with criminal copyright violations, "would have the unsettling effect of criminalizing a broad range of conduct involving copyright and other intellectual property that had historically been regulated by the civil laws."[153]

Copyrights are protected primarily by civil, not criminal, laws; and the narrow range of conduct that amounts to criminal copyright infringement is defined specifically by the Copyright Act, not by the "blunderbuss solution"[154] of equating other criminal conduct with such infringement. "The only defense against [software] piracy is the copyright law;"[155] permitting copyright prosecutions to proceed under the wire fraud statute would "produce the same pernicious result . . . warned of in *Dowling*."[156]

---

[150] 473 U.S. 207 (1985).

[151] *See infra* note 224 and accompanying text (discussing *Dowling*). Although *Dowling* applied directly only to the use of § 2314, the *Dowling* Court expanded upon, and the *LaMacchia* court focused upon, the relationship of the mail fraud statute to copyright enforcement.

The mail fraud statute, 18 U.S.C. § 1341, and the wire fraud statute, 18 U.S.C. § 1343, are virtually identical: "what can be prosecuted . . . under the mail fraud statute is equally susceptible to punishment under § 1343, so long as the jurisdictional element is met." *LaMacchia*, 871 F. Supp. at 541.

[152] *Dowling*, 473 U.S. at 217.

[153] *LaMacchia*, 871 F. Supp. at 538 (citing *Dowling*, 473 U.S. at 228, and referring to reasoning therein).

[154] *Dowling*, 473 U.S. at 226.

[155] *LaMacchia*, 871 F. Supp. at 540 n.7 (quoting S. REP. No. 268, 102d Cong. (1992)).

[156] *Id.* at 544. Dowling did not contest his conviction for copyright violations. The Court upheld his conviction for mail fraud for reasons specific to that case: the materials he unlawfully copied were subject to a statutory reporting requirement. Dowling was required to notify the copyright owners of his intention to distribute. He committed fraud by intentionally failing to so notify them. No such requirement applied to the software at

Copyright violations, whether accomplished with a computer or other means, amount to criminal conduct only when motivated by commercial advantage or financial gain. This statutory edict is not the result of a mere oversight; the *LaMacchia* court detailed the lengthy history of the copyright statute to demonstrate repeated congressional attention to this precise issue.[157] The court cited the congressional testimony of the Vice President and General Counsel of the Computer & Communications Industry of America on the 1992 amendments to the Copyright Act:

> There are millions of people with personal computers to make copies. That is exactly one of the reasons I think you want to be very careful. You do not want to be accidentally taking a large percentage of the American people, either small business or citizens, into the gray area of the criminal law.[158]

To hold LaMacchia criminally responsible for the unauthorized copying, or even distribution, of copyrighted software would be to criminalize the conduct of "the myriad of home computer users who succumb to the temptation to copy even a single computer software program for private use. It is not clear that making criminals of a large number of consumers of computer software is a result that even the software industry would consider desirable."[159] Indeed, because LaMacchia did not copy any software himself, his conduct was far removed from such culpability.

The *LaMacchia* court described the case as presenting "the issue of whether new wine can be poured into an old bottle."[160] That characterization, and similar language used by news accounts and commentators,[161] suggested that the case raised some fundamentally new legal issues. While the technology involved was certainly comparatively new,[162] the

---

issue in *LaMacchia*, and thus there were no analogous grounds for imposing liability for fraud. *See id.* at 542. There were, in fact, no grounds at all for imposing such criminal liability.

[157] The Court pursued that history through 1992, when § 506 was most recently amended, citing the remarks of the sponsor of the 1992 amendments, Senator Hatch, that "the copying must be undertaken to make money [in order to warrant criminal penalties], and even incidental financial benefits that might accrue as a result of the copying should not contravene the law where the achievement of those benefits [was] not the motivation behind the copying." *Id.* at 540 n.8.

[158] *Id.* at 544-45 n.18.

[159] *Id.* at 544. "The exchange of software is extremely common among the millions of Internet users." Peter H. Lewis, *Student Accused of Running Network for Pirated Software*, N.Y. TIMES, Apr. 9, 1994, at 1.

[160] *LaMacchia*, 871 F. Supp. at 536.

[161] *See, e.g.*, Peter Lewis, *Judge Rejects Computer Crime Indictment*, N.Y. TIMES, Dec. 31, 1994, at 10 (describing the dismissal as the court's "declining to prosecute a computer-age crime with telegraph-era law.").

[162] *LaMacchia* was reportedly the first prosecution of a "sysop" of a bulletin board on

legal issues, to a large extent, were not. The copyright statute did not apply, not because of the technology LaMacchia utilized, but because he sought no financial gain. The wire fraud statute was not violated, not because of the technology involved, but because LaMacchia devised no scheme to defraud or to obtain anything of value. The fact that a computer was involved did not criminalize conduct that was not a crime under the language of the statute. The court's holding rested squarely on that quite traditional, and quite appropriate, analysis.

Nevertheless, the technology did raise, and will continue to raise, questions as to the role of the law in such cases.[163] In *LaMacchia*, as in virtually every computer-related case, the search continues for an appropriate analogy with which to frame such cases; because the law operates by analogizing new cases to earlier situations, the choice of an appropriate framework is particularly important. LaMacchia's bulletin board might be viewed as a kind of "safe house" where unauthorized or even stolen goods were fairly openly exchanged, little different from a place where shoplifters might congregate to swap their loot.[164] The bulletin board might thus be viewed as encouraging or facilitating the unauthorized distribution of software. But bulletin boards can also be compared to libraries, where copyrighted materials are freely available to anyone. The public is encouraged to make use of these materials, even though they are also sold for a profit at nearby bookstores, in part because of the social value of literacy and easy availability of information. Using that conceptual framework, software should also be freely available to the public (particularly, perhaps, to people of limited means) even though it is also sold commercially; the value of computer literacy and the availability of electronic information might be a comparable social good.

---

which proprietary software was available free of charge, and was reported to "represent an apparent escalation of the federal government's crackdown" on such bulletin boards. *See* Barbara Carton, *Man Charged in Software Piracy*, BOSTON GLOBE, Sept. 1, 1994, at 41; Michael Dresser & Nelson Schwartz, *MIT Student Indicted on Piracy Charges*, BALTIMORE SUN, Apr. 9, 1994, at 1A.

[163] The court described LaMacchia's conduct as "heedlessly irresponsible" at best, and "at worst as nihilistic, self-indulgent, and lacking in any fundamental sense of values," and called upon Congress to amend the copyright statute to impose criminal penalties for "multiple, willful infringements . . . even absent a commercial motive." *LaMacchia*, 871 F. Supp. at 545.

[164] "To federal prosecutors, what David LaMacchia did was the electronic equivalent of walking into Egghead Software and leaving with boxes of computer programs hidden under his coat." Ronald Rosenberg, *Technology Tests Limits of Law in Computer Case*, BOSTON GLOBE, Apr. 9, 1994, at 1. "Just like you wouldn't think of walking into a candy store and walking out with a candy bar without paying for it. . . . [P]eople who use software should understand that a lot of hard work goes into creating software and the people who produce that software are entitled to be paid for their efforts." *Nightline* (ABC television broadcast, May 2, 1994) (comments of Ken Wasch, Software Publishers Association).

Professor Laurence Tribe compared the bulletin board to a "common carrier" such as the telephone system: "It's like saying, really, that the telephone company will now be guilty if people conduct criminal conversations over the telephone. It's really an extreme stretch."[165] LaMacchia's attorneys compared the bulletin board to a library where patrons duplicate pages of copyrighted books: "Nobody suggests that the copy machine manufacturer, or the librarian, or the board of trustees of the library should be held criminally liable for any copyright violation,"[166] and to a non-computerized bulletin board in a public place such as a laundromat: "If someone buys a lemon of a car advertised on a bulletin board, can the owner of the bulletin board be indicted for what someone else uses it for? David LaMacchia maintained a bulletin board. Get rid of the word 'computer.'"[167] Imposing liability on LaMacchia would be "like the Boston Globe being held accountable for all its classified ads."[168]

These competing descriptions of an appropriate parallel for computer-related activities lead to very different conclusions about liability, both criminal and civil, and therefore to different visions of the consequences for on-line communications.[169] The choice of an appropriate and workable analogy for assessing legal rights and responsibilities in the on-line environment is a crucial and, for the foreseeable future, very open question.[170]

---

[165] *Nightline* (ABC television broadcast, May 2, 1994) (comments of Laurence Tribe, Ralph S. Tyler, Jr. Professor of Constitutional Law, Harvard Law School).

[166] Marianne Lavelle, *U.S. Sees Computer Crime as Threat*, NAT'L L.J., July 25, 1994, at A21 (quoting Harvey A. Silverglate, attorney).

[167] Barbara Rabinovitz, *A Case From Cyberspace*, MASS. LAW. WKLY, Aug. 22, 1994, at 29.

[168] Rosenberg, *supra* note 164, at 1 (quoting David Duncan, LaMacchia's attorney).

[169] "Consider the possibilities (if liability were imposed on the operator of a bulletin board). A user becomes disgruntled with a sysop so he uploads a dozen copyrighted programs to that bulletin board. Then he calls the Software Publishers Association's toll-free tip line. Is this sysop guilty?" *SPA Says 1st BBS Sysop Indicted*, NEWSBYTES NEWS NETWORK, Sept. 1, 1994. "Congress isn't going to want to hold the operators of computer bulletin boards criminally liable for everything anybody does with the system, because nobody would then operate these systems, and the communications highway, the information highway, would grind to a halt." *Nightline* (ABC television broadcast, May 2, 1994) (comments of Harvey Silverglate, attorney). "Owners of intellectual property rights will not be willing to put their interests at risk if appropriate systems . . . are not in place to permit them to set and enforce the terms and conditions under which their works are made available (on line)." Intellectual Property and the National Information Infrastructure (Preliminary Draft of THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY) (the "GREEN PAPER") July 1994, at 6.

[170] The decision in *LaMacchia* did not mandate an "open season" on the distribution of copyrighted software. In *Kenadek*, unpublished decision, defendant pled guilty to a charge of criminal copyright infringement, for conduct similar to that of LaMacchia, with

Like *LaMacchia*, *United States v. Baker*[171] involved the prosecution of computer-related conduct under a non-computer-specific statute. As in *LaMacchia*, even though the statute in *Baker* did not focus specifically on the use of computers, the prosecutor did. And in both cases, the indictments were dismissed because the conduct alleged did not amount to a

---

the crucial distinction that he charged a fee for the use of his bulletin board. That conduct fell squarely within the prohibition of 17 U.S.C. § 506 against infringements for the purpose of financial gain, and was thus properly punishable as a crime. *LaMacchia* did not address the potential liability of the persons who obtained the software in the first place; conceivably, that conduct might engender criminal liability. Probably more central to the resolution of this case and others like it, however, is that copyrights are, and historically have been, protected primarily by civil enforcement actions: nothing in *LaMacchia* diminishes the right of a copyright holder to seek damages for the unauthorized distribution of licensed software. The Software Publishers Association brought a civil suit against Kenadek, in addition to pressing criminal charges against him.

Two notable decisions have been reported regarding the civil liability of commercially-operated on-line services. In *Cubby v. CompuServe*, 776 F. Supp. 135 (S.D.N.Y. 1991), summary judgment was granted in favor of the defendant, a popular on-line information and communication service. *See id.* at 137. The defendant there, the court ruled, was a distributor, not a publisher, and therefore could not be held liable for the allegedly libelous statements made by an individual subscriber absent evidence that CompuServe knew or had reason to know of the defamatory statement; the court analogized CompuServe's legal status to that of a bookstore or newsstand vendor, which cannot be held liable for every potentially libelous word contained in every book on its shelves absent a showing of awareness of the offending material. *See id.* at 139.

In *Stratton-Oakmont Inc. v. Prodigy Services Corp.*, 1995 WL 323710, 63 U.S.L.W. 2765 (N.Y. Sup. Ct.)(Ain, J.)(Order granting partial summary judgment, May 24, 1995), the defendant was held amenable to suit for an allegedly libelous statement made by an individual on-line subscriber. The court there found that Prodigy should be held to the liability standard applied to publishers rather than to the lower standard applied to mere distributors, in large part because Prodigy had at one time held itself out as performing a screening or editing function, and had in fact implemented editorial control over the material posted by individual subscribers. Having exercised such control, the court reasoned, Prodigy could not then avoid liability by claiming it had no control.

Recent decisions addressing the civil liability of bulletin-board operators include *Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1552, 1562-63 (M.D. Fla. 1993) (awarding partial summary judgment, and damages, against operator of for-profit bulletin board on which users had posted unsolicited copies of images from plaintiff's magazine, even though the "sysop" had no knowledge that the images had been made available) and *Sega Enterprises, Ltd. v. MAPHIA*, 857 F. Supp. 679, 682 (N.D. Cal. 1994) (preliminary injunction issued against operator of bulletin board, who advertised and sold by means of the bulletin board certain devices, the "only substantial use" of which was to copy plaintiff's video games; defendant charged a fee for the use of the bulletin board, and knowingly facilitated the unauthorized copying of copyrighted games).

For an overview of issues regarding liability of sysops and systems administrators, see generally LANCE ROSE & JONATHAN WALLACE, SYSLAW (2d ed. 1992); although useful, the material presented there has been overtaken in some significant respects by subsequent legislation, case law, and other events—an inevitable hazard to which virtually all commentary on computer law, including this article, is subject. The same authors present more recent material, although largely peripheral to the subject of this article, in NETLAW (1995).

[171] 890 F. Supp. 1375 (E.D. Mich. 1995) (Cohn, J.).

crime, and the defendant's use of a computer did not make his conduct criminal. Both cases were pursued because the prosecution focused on the use of a computer rather than on the culpability of the defendant's conduct. Although these cases were brought under statutes of general applicability, the prosecutions were flawed for the same reason that computer-specific statutes are flawed: they proceeded from the premise that the technology itself engendered a criminal dimension to conduct otherwise innocent.

The prosecution in *Baker* was based on the electronic mailing (e-mailing) of statements alleged to be threats. The *Baker* court relied on traditional grounds for the dismissal (the conduct did not amount to the crime alleged), but, in unusually strong language, the court criticized the prosecution for even commencing the action. In the court's view, the decision to prosecute resulted from a focus on the technology rather than on the (absence of) culpability of the conduct.

The defendant in *Baker*, a student at the University of Michigan, had posted a lurid story depicting graphic sexual violence[172] to a newsgroup.[173] The defendant had then exchanged a series of private[174] e-mail messages with another user of that newsgroup, identified as "Arthur Gonda," which centered on similarly graphic, sexually violent fantasies. The original story depicted the fictional rape of a character to whom Baker gave the name of a female classmate.[175] A Michigan alumnus who happened to be browsing the newsgroup read Baker's story, recognized the name of the classmate, and notified authorities at the university.[176]

Discovery of Baker's fiction led to a great deal of publicity, both locally and nationally,[177] and to a police investigation that turned up[178] the private e-mail messages between Baker and "Gonda" and resulted in an indictment under 18 U.S.C. § 875(c), alleging the transmission in interstate commerce of a "communication containing any threat to kid-

---

[172] The defendant attached the following statement to the beginning of the story: "The following story contains lots of sick stuff. You have been warned." United States v. Baker, Indictment No. 95-80106, Feb. 14, 1995, Exhibit 1.

[173] A newsgroup is an electronic forum, or message center, typically devoted to conversations in a specific subject area. Baker posted his original story to a newsgroup entitled "alt.sex.stories." *See Baker*, 890 F. Supp. at 1379, 1386.

[174] The posting in the newsgroup was "publicly" available to anyone with the technology to access that newsgroup; the e-mail messages between the defendant and Gonda were accessible only to the conversants. *See id.* at 1379.

[175] *See id.*

[176] *See* Peter H. Lewis, *Writer Arrested After Sending Violent Fiction Over Internet*, N.Y. TIMES, Feb. 11, 1995, at A10.

[177] *See Baker*, 890 F. Supp. at 1379 & n.3.

[178] Baker consented to the search of the messages stored on his computer. *See id.* at 1379 n.4.

nap . . . or injure (any) person."[179] The indictment, based on "unspecified communications . . . presumably includ[ing]" Baker's original story,[180] alleged that they amounted to threats.

Baker's story, offensive and even disturbing as it may have been, was a fictional account of a fictional event. It amounted to a fantasy that included the name of a real person; it was not a threat to carry out the fantasized acts, or indeed to do anything at all, to the woman whose name was used. The prosecution, eventually recognizing that the story did not amount to a threat, dropped the charge based upon the story altogether.[181]

A superseding indictment was based solely on the e-mail messages between Baker and Gonda.[182] But those messages too, the court held, did not amount to threats and could not support an indictment under § 875. The decision centered on the First Amendment limitations on prosecutions of "threats."[183] A statement is prosecutable as a threat under § 875, the court held, only when it is "so unequivocal, unconditional, immediate and specific as to the person threatened as to convey a gravity of purpose and imminent prospect of execution."[184] Moreover, a statement that "would not be interpreted by any foreseeable recipient as expressing a serious intention to injure or kidnap simply is not a threat under the statute."[185]

Baker's e-mail messages did not cross that threshold, and were therefore constitutionally protected. Most of the messages could not be described as targeting an ascertainable class of persons.[186] Because they were all private messages addressed to Gonda, Gonda was the only

---

[179] The indictment named both Baker and "Gonda" as defendants. Gonda was never located; the court noted that the name was assumed to be an electronic alias. "Gonda's identity is entirely unknown; 'he' could be a ten-year-old girl, an eighty-year-old man, or a committee in a retirement community playing the role of Gonda gathered around a computer." *Id.* at 1386.

[180] *Id.* at 1380.

[181] *See id.* n.6.

[182] *See Baker*, 890 F. Supp. at 1380.

[183] "Because prosecution under 18 U.S.C. § 875(c) involves punishment of pure speech, it necessarily implicates and is limited by the First Amendment." *Id.* at 1381.

[184] *Id.* at 1382 (citing United States v. Kelner, 534 F.2d 1020 (2d Cir. 1975)). The court also relied extensively on virtually identical language from *Watts v. United States*, 394 U.S. 705 (1969).

[185] *Baker*, 890 F. Supp. at 1384.

[186] One message expressed Baker's desire to "do it to . . . a 13 or 14 [year old]." *Id.* at 1387. The bill of particulars, with regard to the count based on that message, somewhat astonishingly identified as targets of that statement "13 and 14-year-old girls who reside in . . . Baker's neighborhood in Ann Arbor, Michigan, and . . . in Baker's (hometown) neighborhood in Boardman, Ohio." *Id.* at 1387-88.

"foreseeable recipient."[187] Given the utter lack of evidence as to Gonda's identity, no conclusion could be reached as to whether that "person" would regard the messages as expressing a serious intention to act; and no evidence was adduced to suggest that conclusion.[188] More simply, and more important, none of the messages actually threatened to take any action. They were, as the court made clear, nothing more than shared fantasies, containing no indication whatsoever of any intention to undertake any act at any time, let alone to kidnap or injure any identifiable person or persons. At no time did the messages indicate the "imminent prospect of execution" of any such act.[189]

As a matter of constitutional and statutory analysis, the decision expressed a quite straightforward, unsurprising application of the law. The decision rested on well-established, traditional grounds: the communications simply did not amount to threats, and could not support a prosecution premised on allegations that they did. The fact that a computer was involved did not criminalize conduct that would not have been criminal had it been accomplished by other means; the legal protections afforded speech by the First Amendment do not vanish in the presence of a computer.[190] To a large extent, *Baker* did not implicate any legal doctrine specific to the use of technology, and is thus not a "computer-crime" case at all.[191]

However, the court made very clear its view that the use of computer technology had been central to the decision to prosecute Baker. The opinion went beyond merely dismissing the indictment. The court found that the indictment was based upon poor judgment and reflected an indifference to the clear requirements of the law. Attention to the law, as the court demonstrated in its review of "threat" cases, would have compelled the conclusion that the e-mail messages clearly fell outside the prosecutorial ambit. The statute punishes only transmitting threats to injure or kidnap,[192] and there was no evidence that Baker had engaged in that conduct.

---

[187] The classmate whose name was used in the story became aware of the material only because of the actions of the alumnus and of the University of Michigan. *See* Lewis, *supra* note 176, at A10.

[188] *See Baker*, 890 F. Supp. at 1386.

[189] *See id.* at 1386-90 (addressing each count individually).

[190] The Washington Post editorialized that "a lot of what happens on the Internet may be best covered by existing laws, at least on the criminal side." *Real and Virtual Crimes*, WASH. POST, Feb. 17, 1995, at A24.

[191] The Electronic Frontier Foundation declined to enter the case as amicus, precisely because it viewed the case as a "traditional"—i.e., not technology-specific—prosecution.

[192] *See generally Baker*, 890 F. Supp. at 1380-91 (discussing 18 U.S.C. § 875(c) (1995)).

The court described the dismissal as "inevitable" and found the decision to prosecute a perplexing one:

> The government's enthusiastic beginning petered out to a salvage effort once it recognized that the communication which so much alarmed the University of Michigan officials was only a rather savage and tasteless piece of fiction. Why the government became involved in the matter is not really explained in the record.[193]

The *Baker* court concluded with the admonition that "about the best thing the government's got going for it at this moment is the sincerity of purpose exhibited by (the prosecutor). I am not sure that sincerity of purpose is either synonymous with a good case under the law, or even the exercise of good judgment."[194]

That remarkable language suggested the court's view that the prosecution stemmed precisely from the involvement of the computer. The court's opinion, and the factual context of the case, indicate compellingly that the defendant's use of a computer was central to the decision to prosecute. The court specifically noted that the prosecution was based upon Baker's transmission of words

> by means of the Internet, a relatively new communications medium that is itself currently the subject of much media attention. . . . While new technology such as the Internet may complicate analysis and may sometimes require new or modified laws, it does not in this instance qualitatively change the analysis under the statute or under the First Amendment.[195]

The court noted that all of the messages upon which the indictment was based were private, and that "it is only as a result of this prosecution and the ensuing publicity that the content of the messages have been publicly aired."[196] As to the treatment of Baker, the court went out of its way to note that Baker had been held in custody for twenty-nine days, a circumstance the court found "disturbing" and "inexplicable."[197] Taken together with the court's comments about the "judgment" of the prosecution, the publicity surrounding the case, and the prominent role of

---

[193] *Id.* at 1390.

[194] *Id.* at 1391.

[195] *Id.* at 1390.

[196] *Id.* at 1386.

[197] *See Baker*, 890 F. Supp. at 1379 n.5. The court noted that psychiatric evaluations conducted during investigation of this case concluded that Baker "presented no clear and present danger . . . to anyone" and "displayed no risk factors for potential violence." *Id.* The court found that "why Baker was . . . taken into custody . . . is inexplicable," and termed the prosecution's justification "farfetched." *Id.*

technology,[198] the court made clear that it viewed this detention as a direct result of the decision to prosecute *Baker* as an "Internet porn" case.

Baker's conduct was not criminal, and his use of electronic technology did not make it so. Yet he was charged, and in effect punished, because of the prosecution's focus on his use of a computer. That focus on technology led to the prosecution of conduct that was not criminal. Criminal statutes that focus on technology rather than on conduct invite similar results.

3. Definitional Problems with the Computer-Specific Approach

The adoption of the computer-specific legislative approach entails a constant struggle to provide a workable and effective definition of the targeted technology.[199] To the extent that statutes are defined in terms of specific technology, continuing advances in technology and the ingenuity of those determined to use that technology to criminal ends will constantly threaten to render those statutes obsolete.

The statutory definition of the crucial term "computer" illustrates this point. Without a workable definition of that term, any computer-specific statute will prove utterly ineffective. The legislative effort to provide such a definition dates back to the earliest proposed statutes, and promises to continue as long as statutes employ such language. The 1984 House Report on the CFAA[200] candidly admits that

> [t]he whole issue of defining the word 'computer' has plagued the consideration of computer crime legislation since its early days. . . . Initially, it was the Subcommittee on Crime's opinion that the dictionary definition was as good as one available considering the volatile state of technology in this area. The Committee decided, however, that a specific definition was desirable in order to avoid attacks upon the statute on the grounds of vagueness."[201]

The initial federal attempt at defining a "computer" in the proposed 1979 legislation[202] proved sufficiently unsatisfying that it was modified in the 1984 Act:

---

[198] *See id.* at 1390.

[199] *See supra* note 127 (addressing the confusing and inconsistent technological language set forth in the Communications Decency Act).

[200] The very title of the statute is something of a misnomer; most of its provisions do not directly address fraud. Moreover, despite its original 1984 title, 18 U.S.C. § 1030 never addressed "access devices."

[201] H.R. REP. NO. 98-894 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3709.

[202] The proposed 1979 statute defined a computer as "an electronic device which performs logical, arithmetic, and memory functions by the manipulations of electronic or magnetic impulses, and includes all output, processing, storage, software, or communica-

> "[C]omputer" means an electronic, magnetic, optical, electrochemical or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand-held calculator, or other similar device.[203]

This definition may represent, in most instances, a quite effective and workable definition. Nevertheless, problems in its application are all too easy to envision. A calculator appears to satisfy all aspects of the definition, and yet is explicitly excluded from the scope of the statute. The rationale for its exclusion may be hypothesized; but without some specific statutory guidance, that unexplained exclusion invites unnecessary confusion and litigation. If the exclusion is based solely on its size (as suggested by the "portable hand-held" description), then surely an argument might be presented about the exclusion of some other small device. If a laptop computer would not so challenge the definition, consider a possible next-generation "computer" that might be entirely "hand-held." Consider the possibility of a wrist-watch with extensive computing or telecommunications capability. Consider a product marketed as a calculator, but which also has telecommunications capabilities. A camera may be described as an optical data-processing device possessing storage functions, and thus appears to fall within this definition; yet it makes little sense to ascribe to Congress the intent to include a camera as a vehicle for committing computer fraud or abuse. Would a "data storage facility" include a building containing a telephone company switching station or indeed a telephone company office building, thus defining the structure itself as a "computer"? One need not accept the cogency of all of these examples to acknowledge the perplexing difficulty of providing a definition that is neither over- nor under-inclusive. Inevitable changes in technology will present unforeseeable problems with any definition of a "computer." The solution to this definitional problem does not lie in statutory language prescient enough to anticipate technology not yet invented. The solution instead is to focus on the prohibited result, for example theft or unauthorized alteration of data, and not on the particular means used to achieve that result.

Similarly, definitional problems complicate the effort to combat computer "viruses" by means of technology-specific statutes. The specter of harmful viruses—programs capable of being transmitted from one computer to another, attaching themselves to the operating system of

---

tion facilities which are connected or related to such a device in a system or network." S. 240, 96th Cong. (1977); *see also* Tompkins & Mar, *supra* note 32, at 463 n.17.

[203] 18 U.S.C. § 1030(e)(1) (1995).

those computers, and then causing damage, including deletion or alteration of data or even the "crashing" of computers or computer systems—was brought to public attention probably most forcefully by the Internet "virus" or ""worm" released by Robert Morris in 1988.[204] Particularly in the few years following that highly-publicized (but ultimately quite harmless, and possibly in the long run even beneficial) event, computer users and the public were presented regularly with threats of new, hazardous, or potentially catastrophic viruses.[205]

Largely in response to reports and rumors of such viruses that surfaced repeatedly in the late 1980s and early 1990s, Congress amended the CFAA in 1994 to prohibit the transmission of a "program, information, code or command" with intent to cause damage to a computer. The focus of that statute is on the thing transmitted, rather than the causation of harm. While that language appears to include all forms of what we now know as "viruses," the relentless pace of technological change may very well make possible some pernicious worm or virus that does not easily fall under that definition.

By defining the crime in terms of technology, however, Congress has tied its legislative hopes to that existing technology. In effect, Congress simply hoped that the technology will not dramatically change. Had Congress chosen instead to focus on harm caused by conduct, however, the statute would not be limited to the current state of knowledge. Harm is still harm, no matter the sophistication of the machine that facilitates it.

Definitional problems arise also regarding the crucial term "access," which appears in five of the six sections of the CFAA, and

---

[204] *See supra* note 48 and accompanying text.

[205] *See, e.g.*, Baker, *supra* note 37, at 61. The threat of viruses has proven to be much better as the subject of newspaper and television stories than as an accurate description of real events. In fact, despite the media attention given to this threat, there has been no incident in which a virus has caused any appreciable damage. No virus, or worm, has ever spread as widely as Morris's worm; and that incident caused no damage at all other than the "down time" of certain computers and the time invested by programmers in successfully combating the worm. Thus, there is no body of historical evidence indicating that viruses have presented a substantial threat to the welfare of the nation.

Indeed, the transmission of viruses may not represent a serious threat in the future; more mundane and familiar types of criminal behavior now appear to be the most troublesome source of disruption. "The most dangerous viruses don't spread too far. They tend to blow up, people notice them and devise an anti-virus." Bill Kenny, programmer at Digital Dispatch. "Computer viruses still are a serious problem, but our large company clients now view them as under control. In other words, they see them more as expensive nuisances." Michael Major, *Taking the Byte Out Crime: Computer Crime Statistics Vary as Much as the Types of Offenses Committed*, MIDRANGE SYS. MAG., Mar. 23, 1993, at 25 (quoting Donn Parker, computer security consultant).

which can fairly be described as the operative act prohibited by the statute. Paradoxically, at least some members of Congress are aware of the difficulties inherent in prohibiting "access." When section (a)(5) was amended in 1994, the sponsor of the amendment, Senator Leahy, addressed this issue directly:

> Under the [1986] statute, prosecution of computer abuse crimes must be predicated upon the violator's gaining "unauthorized access" to the affected "federal interest computers." However, computer abusers have developed an arsenal of new techniques which result in the replication and transmission of destructive programs or codes that inflict damage upon remote computers to which the violator never gained "access" in the commonly understood sense of that term. The new subsection of the CFAA created by this bill places the focus on harmful intent and resultant harm, rather than on the technical concept of computer "access."[206]

This statement focuses squarely on the problems caused by defining computer-related crime in terms of technology, even in language as relatively non-specific as "access." As Senator Leahy recognized, the technology changes and will continue to change. The solution is not to replace "access" with a more up-to-the-minute term of art; the solution is to focus on the harmful result and not on particular means of inflicting that harm. Despite this recognition in the legislative history and in the amended (a)(5), the remaining provisions of the CFAA are still couched in terms of "access."

Somewhat similarly, the focus of the earlier version of (a)(5) on access to "information" has been replaced by an emphasis on intentional, or reckless, transmission of programs or commands that cause damage. Although not explicitly stated by Senator Leahy, this change also could be described as "focus[ing] on harmful intent and resultant harm," rather than on the somewhat more "technical" concept of "information."

To the extent that harm is a simpler, more general and more legally familiar term, courts and prosecutors are likely to find it easier to work with than the more technical "information." Precedent will help to supply answers in potentially grey areas and forestall unnecessary argument in many situations. "Information," on the other hand, may invite litigation and require courts to grapple uncomfortably with the language of technology. Likewise, "transmission" may prove to be more easily and generally applied than "access."

As noted by Senator Leahy, changes in technology have already blurred the meaning of "access." The question of whether a defendant has sent (transmitted) a program from his computer, however, is much

---

[206] 140 CONG. REC. S12,312 (daily ed. Aug. 23, 1994) (statement of Sen. Leahy).

less likely to raise troublesome technical issues. More important, the focus on result—damage or loss—is far preferable to a concentration on a particular, difficult-to-define set of actions taken by a defendant on his keyboard. Courts have been able to apply the malleable concept of damage to a very broad range of situations; determining whether damage has been caused requires no technological expertise. If a crime is defined in terms of specific computer operations, in contrast, prosecutions will have to focus on technology even as that technology rapidly evolves. To the extent that the amended section is defined in terms of harm or damage, it is likely to prove more effective than its predecessor.

4. Imprecision: The "Uneasy Fit" of Computer-Specific Statutes

Much of the rationale supporting the enactment of computer-specific statutes stems from the idea that traditional crimes such as larceny or trespass do not easily apply in the computer setting. The House Report accompanying the original 1984 legislation asserted that, "[d]ifficulties in coping with computer abuse arise because much of the property involved does not fit well into categories of property subject to abuse or theft . . . ."[207] These difficulties led the Report to conclude that "traditional theft/larceny statutes" would not be effective in combating "computer assisted crimes." Congress accepted that conclusion, refusing to rely on those statutes of general application, because it determined that they would not "fit well" with computer-related criminal conduct; new, computer-specific statutes were necessary to counter this "new" wave of criminal conduct.

Curiously, however, Congress responded to this problem by enacting a fraud statute as the major weapon against computer crime. Fraud was and is already prohibited by a variety of federal statutes; a specific computer fraud statute appears to be superfluous. Fraud is a traditional crime, and a fraud statute scarcely constitutes an innovative means of response to the prospect of new, unprecedented crimes that cannot be adequately prosecuted under traditional statutes. Thus, Congress's response seems at odds with its own reasoning.

Moreover, fraud is an imprecise, and largely inaccurate, description of the conduct Congress sought to prohibit with § 1030. That conduct is much more appropriately described as unauthorized access, or unauthorized manipulation of data, or simply theft, than as fraud. For instance, to describe Morris's conduct as "fraud" requires the invention of an unwieldy legal fiction: that he intentionally misrepresented himself to a se-

---

[207] H.R. REP. NO. 98-894 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3695.

ries of computers by using a password or access code that was not his. In fact, he did not represent himself directly to any remote computer at all; the worm, or virus, moved to new machines without any further action on Morris's part. He did not intend to gain anything, a necessary element of the crime of fraud. Morris's conduct might have been criminal, but it does not easily fall within the definition of fraud.

Because almost all computer-crime prosecutions involve allegations of unauthorized access, the traditional crime of fraud frequently will not "fit well" with the defendant's conduct in such cases; if that lack of fit was the reason for Congress's refusal to rely on traditional crimes such as larceny or trespass, Congress should have similarly rejected the use of fraud.

IV. AN ALTERNATIVE APPROACH

The conduct most often at the heart of "computer crime" cases, and the conduct to which computer crime legislation should be addressed, is unauthorized access of, misuse of, or damage to, information. It is the protection of information—whether that information is "owned" by the government, a bank, a hospital, or a private individual—that is, or should be, the aim of legislation in this area. Statutes that seek appropriately to protect information, and to punish unauthorized theft, alteration, or deletion of properly restricted information, perform an important role in modern criminal justice. That role has been, and continues to be, fulfilled quite adequately by existing "traditional" criminal statutes. The difficulties envisaged by Congress in a reliance on such statutes are largely illusory; to the extent that such problems do exist, they can be cured easily by straightforward definitional clarification. Such statutes are likely to be more effective vehicles for the prosecution of computer-related crimes. Statutes that focus instead on the technical means by which a prohibited result may be achieved tend to be unnecessary, imprecise, and quickly outstripped by changing technology.

A. Prosecutions Under Other Statutes

Underlying the enactment of computer-specific statutes is the view that statutes of general application are inadequate to prosecute computer crimes. This view has been expressed in the proceedings of Congress since at least 1979. Commentators have urged the same point, arguing that statutes drafted without specific regard to technology can be applied to computer crimes only by stretching those statutes to, and sometimes beyond, their limits.[208]

---

[208] *See* Roddy, *supra* note 32, at 352-57, 365; Susan Hubbell Nycum, *The Criminal*

In fact, the cases do not support that conclusion. Computer crimes have been prosecuted successfully under non-computer-specific statutes, both before and after the enactment of technology-specific statutes.

The wire-fraud statute, 18 U.S.C. § 1343, has produced more convictions for computer-related crimes than § 1030 or any other computer-specific statute.[209] Section 1343 authorizes punishment of:

> [w]hoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio or television communication in interstate or foreign commerce, any writings, signs, signals, pictures or sounds for the purpose of executing such scheme or artifice.

The sweep of this statute is very broad indeed. Its application to computer-related conduct proceeds, of course, from the term "wire." Because communication between remote computers entails the use of telephone lines, no court has questioned the inclusion of such computer communications within the scope of the statute.

The wire-fraud statute has been successfully used to prosecute the unauthorized accessing of computer systems by modem and phone lines.[210] To the extent that such conduct comprises the essence of most "computer crimes," § 1343 has proven an effective tool for prosecuting those crimes. If the element of fraud presented a troublesome element in such prosecutions, Congress has carried that element forward to § 1030.[211] Thus, the computer-specific § 1030 represents no significant improvement over the broader § 1343.

In 18 U.S.C. § 1029, Congress prohibited "fraud and related activity in connection with access devices." As originally enacted in 1984, and until its amendment in 1994, its provisions prohibited the knowing production, use, or trafficking of counterfeit or unauthorized access devices with the intent to defraud.[212] The crucial term "access device" is defined as "any card, plate, code, account number, or other means of ac-

---

Law Aspects of Computer Abuse, 5 RUTGERS J. COMPUTERS & L. 271 (1975).

[209] *See* James Tramontana, Note, *Computer Viruses: Is There A Legal Antibiotic?*, 16 RUTGERS COMPUTER & TECH. L.J. 253, 263 (1990).

[210] *See, e.g.*, United States v. Seidlitz, 589 F.2d 152 (4th Cir. 1978) (resulting in a conviction under the wire-fraud statute prior to the enactment of § 1030).

[211] See discussion of the "uneasy fit" of fraud to computer crimes, *supra* Part III.B.4.

[212] *See* 18 U.S.C. § 1029(a)(1) (1995). The statute also prohibited trafficking in or using access devices and thereby obtaining "anything of value aggregating $1000 or more," the knowing possession of multiple such devices with the intent to defraud, and the knowing production or possession of device-making equipment with the intent to defraud. *Id.*

count access that can be used . . . to obtain . . . any . . . thing of value or that can be used to initiate a transfer of funds."[213]

The statute has been applied by the courts to protect a wide variety of the increasing number of assets and services that can or must be accessed through digital gateways. Congress's overriding concern, however, was credit card fraud; the statute was enacted in 1984 under the title "Credit Card Fraud Act."[214] Specifically, the legislature intended to punish "the actual counterfeiting or altering" of credit cards, the "stealing and use of account numbers," the "possession of fraudulent cards or other similar payment devices," and the "use or sale of any device or mechanism which could be used in the place of a legitimate payment device (such as sales slips or credit slips)."[215]

The legislative history demonstrates that Congress intended to prohibit credit card fraud, but realized that such fraud could be effected in a variety of ways. Congress could have responded to this drafting problem by enacting a statute limited to credit cards and credit card fraud, and that specifically referred to each of the particular problems identified above. The result might well have been a fairly narrow statute, with no application to situations not directly involving credit cards, and that would have been subject to litigation regarding the definition of "credit card." Situations that Congress intended to address might well have fallen outside the scope of such limited language.

The approach taken originally, however, was to draft the statute in language broad enough to cover the range of fraudulent activity Congress intended to prohibit and broad enough to include a wide variety of known and not-yet-known methods devised to facilitate the fraudulent use of credit cards. The result was the statutory focus on "access devices."

Because of the breadth of that language, the statute has been applied successfully in a variety of cases involving misuse of access devices, including long-distance telephone service access codes,[216] automatic teller machines and ATM cards,[217] and cellular telephone access numbers,[218] as well as credit cards.[219] The provisions of § 1029 might literally be applied to conduct involving very low technology indeed, such as writing down or simply memorizing a credit card number in order to access that account fraudulently. However, mindful of the legislative focus on de-

---

213 § 1029(e)(1).

214 Pub. L. No. 98-473, 98 Stat. 2183.

215 H.R. REP. NO. 98-894 (1984), *reprinted in* 1984 U.S.C.A.A.N. 3689, 3691.

216 *See, e.g.*, United States v. Brewer, 835 F.2d 550 (5th Cir. 1987).

217 *See, e.g.*, United States v. Greenfield, 44 F.3d 1141 (2d Cir. 1995).

218 *See, e.g.*, United States v. Bailey, 41 F.3d 413 (9th Cir. 1994).

219 *See, e.g.*, United States v. Lee, 815 F.2d 971 (4th Cir. 1987).

vices that afford electronic means of gaining unlawful access, courts have restricted its scope accordingly.[220] But even as restricted to technologically sophisticated devices, the statute has proven to be of considerably broader application than it would have been had Congress focused on the specific means (credit cards) rather than on the result (production or use of counterfeit "access devices"). The utility of the statute serves as an instructive example of legislation not defined in terms of specific technology or specific technological means, but in terms of the prohibited result.[221]

Title 18 U.S.C. § 2314, which prohibits the interstate transportation of stolen property (ITSP),[222] predates computer technology and was not

---

[220] The court in *Bailey*, while reversing the district court, cited with apparent approval the lower court's comment that, "[w]hat legislative history there is [regarding § 1029] indicates that the purpose of this legislation was to prevent access to accounts . . . . If you follow the [prosecution's] line of reasoning then even a crowbar could be an access device because you could use it to pry open an ATM machine." *Bailey*, 41 F.3d at 416.

[221] The original provisions remain in effect. However, in 1994, a number of additional substantive provisions were added. Congress amended the statute to prohibit, inter alia, the use, production, trafficking in or possession of a "telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services," with the intent to defraud. Ironically, these added provisions suffer from the same problems identified in § 1030. The amendments are unnecessary. They prohibit conduct that is already prohibited, either under the earlier provisions of § 1029, or under other existing statutes. Fraudulently "effect[ing] transactions" with an unauthorized "access device" is prohibited under § 1029(a)(1); doing so and thereby gaining "anything of value" is prohibited by (a)(2). The prohibition of (a)(6) against soliciting, with the intent to defraud, for the purpose of offering or selling information about an access device, is simply redundant of the prohibition in (a)(4) against "trafficking" and possessing access devices. The language of (a)(7), prohibiting the "present[ation] for payment," without authorization and with the intent to defraud, of a record of a transaction made by an access device, adds nothing to the much simpler and more direct language of (a)(1) and (a)(2), which prohibit using an unauthorized access device and obtaining anything of value by doing so. The other two added provisions, (a)(5) and (a)(6), prohibit conduct that is already made criminal under the Electronic Communications Privacy Act, 18 U.S.C. § 2511.

Moreover, the language of these provisions represents a retreat from the broader, effective language of the original statute, and instead focuses on specific technology: "telecommunications instruments" and "scanning receivers." Instead of the quite effective focus on results—the unauthorized use of access devices—these added provisions simply enumerate two specific means of achieving that prohibited result. If it is already a crime to use with the intent to defraud any unauthorized access device, no legislative function is served by adding a prohibition against the use with the intent to defraud of a specific unauthorized access device.

[222] Section 2314 applies, in part, to whoever "transports, transmits, or transfers in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of $5,000 or more, knowing the same to have been stolen, converted or taken by fraud." Its companion provision, § 2315, provides for the punishment of whoever "receives, possesses, conceals, stores, barters, sells, or disposes of any goods, wares, or merchandise, securities, or money of the value of $5,000 or more . . . which have crossed a State or United States boundary after being stolen, unlawfully converted, or

enacted to combat computer-related crimes. Nevertheless, several computer-related prosecutions have been brought successfully under that statute, even after the passage of § 1030. On its face, § 2314 describes the conduct at issue in many computer-related cases much more comfortably than the CFAA: the cases usually involve the transmission or "transportation" of unlawfully obtained computer data, rather than an awkward approximation of fraud.[223] Section 2314, however, has proven to be a problematic tool for prosecuting computer-related conduct: several such prosecutions have resulted in dismissal of the computer-related charges based on § 2314. The stumbling block here is the Supreme Court's reading of "property" under that statute in *Dowling v. United States*.[224]

Dowling involved a scheme to manufacture and distribute bootleg[225] phonograph records containing performances of copyrighted musical compositions. The physical objects the defendant sought to distribute—the tangible vinyl disks—were not alleged to have been stolen.[226] Instead, the prosecution under § 2314[227] was based on the view that "the unauthorized use of the musical compositions rendered the phonorecords 'stolen, converted, or taken by fraud' within the meaning of the statute."[228] Thus, regarding the conduct element of § 2314, the government's theory was that the unauthorized use of the musical compositions—i.e., the infringement of the copyrights on those compositions—amounted to unlawful obtaining, and was thus equivalent to theft, conversion, or fraudulent taking. With regard to the element of "goods, wares, or merchandise" under § 2314, the indictment alleged that it was the "performances," contained in reproducible magnetic impulses, which comprised the allegedly stolen "property."[229] The Supreme Court, finding that § 2314 had been applied only to physical objects that had themselves been "stolen, converted or taken or fraud," held that "the statutory language, by requiring that the 'goods, wares, [or] merchandise',

taken, knowing the same to have been stolen, unlawfully converted, or taken."

[223] Proof of interstate transportation, typically over telephone lines, of course serves as a limitation on federal prosecution; but the CFAA has similar jurisdictional thresholds. *See supra* note 73.

[224] 473 U.S. 207 (1985).

[225] "A 'bootleg' phonorecord is one which contains an unauthorized copy of a commercially unreleased performance." *Id.* at 209 n.2.

[226] *See id.* at 214.

[227] Dowling was also convicted of copyright infringement under 17 U.S.C. § 506; that conviction was not contested before the Supreme Court. *See id.* at 209.

[228] *Id.* at 215.

[229] The prosecution did not contend that the transported "goods, wares, or merchandise" were the copyrights themselves. It is not clear how such a claim could have been pursued; and the Court foreclosed that line of reasoning: "[t]he infringer . . . does not assume physical control over the copyright. . . ." *Dowling*, 473 U.S. at 217.

be 'the same' as those 'stolen, converted, or taken by fraud, . . . seems clearly to contemplate a physical identity between the items unlawfully obtained and those eventually transported, and hence some prior physical taking of the subject goods."[230] Because there was no "physical identity" between the intangible copyrights and the tangible records, the conduct alleged was beyond the reach of § 2314. Dowling was properly convicted of copyright infringement, but not of the transportation of "property" that had been "stolen, converted, or taken by fraud."

Thus, *Dowling* could be read to hold § 2314 applicable only to tangible physical property, and not to intangible property such as the magnetic impulses comprising a musical recording.

That reading was applied to exclude charges in an analogous situation involving computer data. In *United States v. Brown*,[231] the defendant was charged under §§ 2314 and 2315 with the transportation and possession of a computer source code[232] taken unlawfully from his former employer. The Tenth Circuit affirmed the dismissal of the charges, holding that computer source code is "not the type of property which is contemplated within the language of the statute, 'goods, wares, or merchandise,'" and therefore could not constitute "property," the theft, conversion, or fraudulent taking of which would be subject to prosecution under § 2314.[233] The computer data comprised intangible intellectual property, while the statute applied only to tangible, physical "goods, wares, or merchandise." The *Brown* court expressly relied on *Dowling* to reach that conclusion: the "essential ingredient of the statute—the involvement of physical 'goods, wares [or] merchandise' that were themselves 'stolen, converted, or taken by fraud'—was missing in *Dowling* and is likewise missing here."[234]

Thus, *Dowling* and *Brown* appear to foreclose the use of § 2314 as a tool for prosecuting the unauthorized taking, or transfer, of computer data, on the grounds that computer data is not "property" within the meaning of that statute. A close reading of *Dowling*, however, leads to a quite different conclusion. *Dowling* can be read merely to exclude § 2314 as a tool for prosecuting copyright infringement.[235] The bulk of the

---

[230] *Id.* at 216.

[231] 925 F.2d 1301 (10th Cir. 1991).

[232] The court explained as follows: "source code, also called assembly language, . . . contains mnemonic abbreviations for each step and can be read by expert programmers. Once a programmer has access to the source code of a program, he is able to determine the construction of the program and write his own version." *Id.* at 1303 n.4.

[233] *See id.* at 1306.

[234] *Id.* at 1307.

[235] *See* Todd H. Flaming, *The National Stolen Property Act and Computer Files: A*

Court's opinion in *Dowling* is devoted specifically to that issue.[236] The Court identified the issue as "whether the statute reached the interstate transportation of 'bootleg' phonorecords, (which were) 'stolen, converted, or taken by fraud' only in the sense that they were manufactured and distributed without the consent of the copyright owners,"[237] thus immediately focusing its attention on the conduct—whether unauthorized use of copyrighted material amounted to theft, conversion or fraudulent taking—rather than on a definition of property.

In identifying the elements of the statute, the Court carefully distinguished between the requirement of transportation of goods, wares, or merchandise (which "Dowling does not contest")[238] and the requirement that the goods be "stolen, converted, or taken by fraud," the element on which Dowling's appeal focused.[239] The Court reiterated that:

> there is no dispute . . . that Dowling's (conduct) . . . constituted infringement of those copyrights. It is less clear, however, that the taking that occurs when an infringer arrogates the use of another's protected work comfortably fits the terms associated with physical removal employed by § 2314. . . . The infringer invades a statutorily defined province guaranteed to the copyright holder alone. But he does not assume physical control over the copyright nor does he wholly deprive its owner of its use.[240]

This language strongly suggests that the problem in *Dowling* was not the type of property involved, but the fact that the property—tangible or intangible—had not been "stolen, converted, or taken by fraud." Dowling had not taken anything, but had instead infringed on the rights of the copyright owner. Seen in that light, *Dowling* would permit prosecution under § 2314 of the theft, or taking, of computer data, so long as the conduct could be shown to be theft or taking, rather than the infringement of copyright.

The *Brown* court clearly did not view *Dowling* from this perspective. In *Brown*, the court repeatedly referred to the intangibility of the "property" as the dispositive factor:

> *Dowling* holds that § 2314 applies only to physical 'goods, wares or merchandise.' Purely intellectual property is not within this category. It can be represented physically, such as through writing on a page,

---

New Form of Property, a New Form of Theft, 1993 U. CHI. L. SCH. ROUNDTABLE 255 (advocating this view).

[236] *See* Dowling v. United States, 473 U.S. 207, 218-27 (1985) (addressing exclusively the subject of copyright infringement, not the definition of "property" or "goods, wares, and merchandise.").

[237] *Id.* at 208.

[238] *Id.* at 214.

[239] *Id.*

[240] *Id.* at 217.

> but the underlying, intellectual property itself, remains intangible. . . . We hold that the computer program itself is an intangible intellectual property, and as such, it alone cannot constitute goods, wares, merchandise, securities or moneys which have been stolen, converted or taken within the meaning of §§ 2314 or 2315.[241]

The dismissal in *Brown* could, perhaps, have been affirmed on the ground that the indictment alleged, and the government's proffered evidence might have shown, a copyright infringement and not a theft, conversion, or taking of the source code. The indictment specifically described the source code, and the program for which it contained instructions, as the "exclusive property" of the employer;[242] the defendant argued that the indictment actually alleged conduct amounting to infringement on intellectual property rights, not theft;[243] and the Tenth Circuit's opinion suggests that the prosecution's case might indeed be so described.[244] Thus, the *Brown* court could have viewed the case as an attempt to punish copyright infringement and, citing language in *Dowling*, found § 2314 an inappropriate vehicle for that purpose. Although that possibility was open to it, *Brown* clearly rests squarely on the notion that § 2314 applies only to physical property, and not to intellectual property such as computer codes.

The court in *United States v. Riggs*,[245] however, took quite a different view of *Dowling* and the scope of § 2314. The case was among the first prosecutions resulting from the "hacker crackdown" of the late 1980s,[246] and is still regarded as significant by the computer community. *Riggs* reflects quite graphically the clash of competing interests in cyberspace, most notably the clash between the telephone industry and hackers.[247]

The indictments against Riggs and co-defendant Niedorf arose from the unauthorized copying and publication of a document owned by Bell-South, one of the regional Bell operating companies,[248] containing infor-

---

[241] United States v. Brown, 925 F.2d 1301, 1307-08 (10th Cir. 1991).

[242] *See id.* at 1303 n.5.

[243] *See id.* at 1303.

[244] According to the court, the prosecution attempted to distinguish *Dowling* primarily on the grounds that the source code here took 15 years to develop, and that the code was "removed from things that the victim thought they had protected." *Id.* at 1305.

[245] 739 F. Supp. 414 (N.D. Ill. 1990).

[246] *See supra* note 20; *see also* Dorothy E. Denning, United States v. Craig Neidorf: *A Debate on Electronic Publishing, Constitutional Rights, and Hacking*, 34 COMMUNICATIONS OF THE ACM 24 (1991); also available on-line at <http://www.eff.org>.

[247] For a fascinating account of the events surrounding the *Riggs* case, see STERLING, *supra* note 23. *See also* Barlow, *supra* note 14; Cutrera, *supra* note 16; Denning, *supra* note 246.

[248] The regional Bell companies were formed in 1984 as the result of federal anti-trust

mation about the operation of its "enhanced 911" system for handling emergency calls. In December 1988, Riggs gained unauthorized access to a BellSouth computer system in Atlanta,[249] downloaded the text of the "E911" document, and sent it by modem to Niedorf in Missouri. Niedorf subsequently published a modified copy of the document in his online newsletter "Phrack," which was available on various hacker bulletin boards around the country. During the law enforcement raids comprising Operation Sun Devil in February 1990—over a year following Riggs's downloading of the document, and eleven months after the publication of the revised copy in Phrack, but only days after the telephone system crash of Martin Luther King Day—Riggs and others, eventually including Niedorf, were arrested, their equipment confiscated, and prosecutions against them commenced.

Riggs and Niedorf were indicted for trafficking in information that would permit unauthorized access to computers under § 1030(a)(6),[250] wire fraud under § 1343, and interstate transportation of stolen property under § 2314. Riggs, who had obtained a copy of the document by means of unauthorized access, pleaded guilty to wire fraud[251] charges.[252]

---

litigation.

[249] The security system was so lax that not even a password was required to gain access. *Cf.* Michael Godwin, *Some 'Property' Problems in a Computer Crime Prosecution*, 16 CARDOZO L. FORUM 24 (1992); BellSouth improved its security measures as a result of Riggs's access. *See* Denning, *supra* note 246, at 29.

[250] The charges under 18 U.S.C. § 1030(a)(6) were dropped in a superseding indictment, apparently because the E911 document did not in fact provide information that would facilitate unauthorized access to any computer; the document merely described the operation of the system. See Denning, *supra* note 246, describing specifically the information contained in the E911 document.

[251] The basis of the fraud counts was that Riggs had made use of an account assigned to a BellSouth employee, and, in that sense, had misrepresented himself to be that employee.

[252] Riggs's sentencing raised other interesting questions. The district court ordered, inter alia, that Riggs was not to "own personally or directly have control over a computer of any type for [his] own personal use during the period of supervised release." *See* United States v. Riggs, 967 F.2d 561, 563 (11th Cir. 1992). On appeal of that sentencing condition, Riggs argued, in an amicus brief filed by the Electronic Frontier Foundation, that that condition amounted to an infringement of his First Amendment rights.

The order did not simply prohibit particular illegal uses of a computer, the brief pointed out, but the use of a computer for any purpose, including the exercise of rights of speech and association. Particularly for a computer-literate person like Riggs, such a prohibition seriously curtailed his ability to communicate. The EFF noted that an analogous (although less restrictive) limitation on the use of mails by a person convicted of mail fraud was struck down, precisely on First Amendment grounds, in *United States v. Holloway*, 740 F.2d 1373 (6th Cir. 1984).

To impose an even harsher prohibition against the use of a computer would thus appear also to be unconstitutional; only if, somehow, computers themselves were dangerous instruments like firearms, could Riggs's sentence be valid. Amicus brief, *United States v. Riggs* <http://www.eff.org> (copy on file with author). The Eleventh Circuit declined

Niedorf, however, contested the charges against him, on a variety of constitutional, statutory, and factual grounds.

In denying Niedorf's motion to dismiss,[253] the court addressed the applicability of § 2314 to physical property.[254] Niedorf argued, as summarized by the court, that "the only thing which he allegedly caused to be transferred across state lines was 'electronic impulses' . . . [and that] electronic impulses do not constitute 'goods, wares, or merchandise.'"[255] The court flatly rejected that argument:

> Niedorf's conduct is not properly characterized as the mere transmission of electronic impulses. Through the use of his computer, Niedorf allegedly transferred proprietary business information. . . . The question . . . is not whether electronic impulses are 'goods, wares, or merchandise' within the meaning of § 2314, but whether the proprietary information contained in . . . the E911 file constitutes a 'good, ware, or merchandise within the purview of that statute.[256]

Noting that "[n]o court has ever held that the electronic transfer of confidential, proprietary business information from one computer to another across state lines constitutes a violation of § 2314,"[257] the *Riggs* court proceeded to reach precisely that conclusion. Other courts had found that proprietary information, when "affixed to some tangible medium, such as a piece of paper,"[258] became "goods, wares, or merchandise." In view of that "well-settled" proposition, a short step would produce the same conclusion regarding intangible information "affixed to

---

to address the issue, holding that no effective timely objection was raised before the district court. *See Riggs*, 967 F.2d at 563. Similar conditions have been imposed on other cases. Such restrictions make sense, and indeed are constitutionally permitted, only if computers are regarded not as tools for communication, but as dangerous instruments in themselves; only if the computer itself rather than conduct is regarded as the focus of the criminal law.

[253] The court's decision of June 5, 1990, comprises the denial of the motion to dismiss the original indictment; a superseding indictment was returned only days after the court's decision. *See* United States v. Riggs, 739 F. Supp. 414 (N.D. Ill. 1990). Niedorf subsequently moved to dismiss the superseding indictment as well; that motion was denied. *See* 743 F. Supp. 556 (N.D. Ill. 1990). The later decision did not provide a detailed analysis of the § 2314 charges, relying instead on the analysis set forth in the earlier opinion. *See* 743 F. Supp. at 557-58, 561.

[254] In denying Niedorf's motion to dismiss the charges under § 1343, the court expressly found that the information contained in the E911 document, although "obtained" in electronic form only (and apparently never reproduced by either defendant in any form other than electronic), constituted "property" within the meaning of that statute. *See Riggs*, 739 F. Supp. at 418-19. "The property which forms the basis for a wire fraud or mail fraud charge can be 'intangible' property." *Id.* at 419 n.7.

[255] *Id.* at 420.

[256] *Id.*

[257] *Id.* at 419.

[258] *Id.* at 420-21.

a floppy disk."[259] "The court sees no reason to hold differently simply because Niedorf stored the information inside computers instead of printing it out on paper. In either case, the information is in a transferable, accessible, even salable form."[260] The computer itself, the court in effect held, was legally irrelevant; the only legal question was whether the *conduct* amounted to a crime.[261]

Moreover, the court expressed doubt that "tangibility is a requirement of 'goods, wares, or merchandise' under § 2314" in any event; and, even if it were, information stored in a computer was as "tangible" as information written on paper.[262] To the *Riggs* court, the key statutory issue was not tangibility, but accessibility: "The accessibility of the information in readable form from a particular storage place also makes the information tangible, transferable, salable and, . . . brings it within the definition of 'goods, wares, or merchandise' under § 2314."[263] In a sense, then, the tangibility, or accessibility, of the storage place makes the information stored there equally tangible. To the *Riggs* court, computer data are therefore "goods, wares, or merchandise," and come within the scope of § 2314.

The *Riggs* court distinguished *Dowling* as a case about copyright infringement, not about the definition of "goods, wares, or merchandise." Unlike the holder of a copyright, "[t]he owner of confidential, proprie-

---

[259] *Riggs*, 739 F. Supp. at 421.

[260] *Id.*

[261] This conclusion, never explicitly stated by the court, is one of the central theses of this article, and implies a broad range of consequences for the law of "computer crime." Specifically regarding Niedorf's situation, that conclusion has other significant ramifications. Niedorf published a newsletter. That the newsletter was published only in electronic form should be, consistent with the thrust of *Riggs*, irrelevant: Niedorf should have been entitled to the same First Amendment protections granted to any publisher. But he was not. Not only did Secret Service agents seize the allegedly "stolen" E911 document; they seized all of his equipment and prevented him from continuing to publish altogether.

As John Perry Barlow put it, "If the 911 document had been the Pentagon Papers (another proprietary document) and Phrack the New York Times, a completion of the analogy would have seen the government stopping publication of the Times and seizing its every material possession, from notepads to presses." Barlow, *supra* note 14, at 50-51. Riggs should have been entitled to the same Fourth Amendment protections granted to any citizen. But he was not. Again, in Barlow's words, "[i]t's quite as if the government could seize your house simply because a guest left a stolen VCR in an upstairs bedroom closet." *Id.* at 51. The actions of the Secret Service in connection with the arrest, search and seizure in *Riggs* should have compelled the dismissal of all charges on First and Fourth Amendment grounds; only if the court regarded the computer itself as a dangerous instrument, and utterly unlike other kinds of property, could those actions pass constitutional muster. *See id.*

[262] *See Riggs*, 739 F. Supp at 421, 422.

[263] *Id.* at 422.

tary business information, . . . possesses something which has clearly been recognized as an item of *property*."[264]

Brown, relying on language from *Dowling*, in turn rejected the *Riggs* analysis:

> We feel that the *Riggs* interpretation of the statute is in error in light of the Supreme Court's focus on 'physical goods, wares, or merchandise' that have themselves been 'stolen, converted, or taken by fraud' . . . . The element of physical 'goods, wares, and merchandise' in §§ 2314 and 2315 is critical.[265]

The *Brown* court focused on the "physical" aspect, and read *Dowling* as excluding non-physical items such as computer data from the scope of § 2314. The *Riggs* court read *Dowling* simply as rejecting the use of § 2314 as a copyright enforcement tool, not as establishing a definition of "goods, wares, or merchandise;" that reading would permit the use of § 2314 in a computer-related prosecution, so long as the computer data could be shown to have been "stolen, converted, or taken by fraud."

It is submitted here that *Brown*'s reading makes little sense and is probably inaccurate. *Dowling* did not explicitly hold that only tangible, physical objects are within the scope of § 2314; to the extent that *Brown* assumes such an explicit holding, it rests on a shaky foundation. *Dowling* did, explicitly and repeatedly, focus on the conduct at issue there and squarely held that infringement of copyrights is not equivalent to the theft, conversion, or fraudulent taking required by the statute. That focus of the *Dowling* court, relied upon by *Riggs*, seems to have been regarded as merely peripheral to the reasoning in *Brown*.

Moreover, to hold, as did *Brown*, that § 2314 applies to physical "goods" but not to intangibles such as computer data, leads to the conclusion that § 2314 would apply to the transportation of, e.g., proprietary information such as a chemical formula written on a stolen piece of paper,[266] but not to a chemical formula written on one's own paper or computer disk. That conclusion reflects a triumph of formalized hair-splitting over common sense. If the intellectual property is proprietary, and if it has been "stolen, converted or taken by fraud," then the plain language of § 2314 appears irresistibly to apply. Whether the information is written on a piece of paper or on a computer disk is a difference without any distinction; it is a detail that cannot sensibly be said to separate criminal conduct from non-criminal.

---

[264] *Id.* at 423 (citing Carpenter v. United States, 484 U.S. 19 (1987)).

[265] United States v. Brown, 925 F.2d 1301, 1308-09 (10th Cir. 1991).

[266] *See id.* at 1307-08 n.14.

As the *Riggs* court pointed out,[267] the *Brown* view would deem criminal the printing out of unlawfully obtained proprietary information from a computer to paper, but would find the storage alone on a computer of such information non-criminal. The *Brown* view focuses on the technology itself—the means—rather than on the result or the conduct. If § 2314 prohibits transportation of stolen intellectual property, then the precise technological form in which that property is stored or transported should not be used to obscure the point of the statute or to undermine its purpose. The use of a computer should not be the determining factor as to whether conduct is or is not criminal.

The difficulty in *Riggs* was not that the E911 document did not, somehow, comprise "goods, wares, or merchandise." Plainly, it did; and it did whether it happened to appear in printed form or in other easily reproducible form. The problems, instead, were factual: (1) the document did not consist of proprietary information, and (2) its value was so insignificant as to fall beneath the scope of the statute.[268] Those facts probably should have precluded any prosecution in the first place; the fact that the information was stored electronically, however, should not have compelled any particular legal conclusion.

Similarly, in *United States v. Jones*,[269] another early computer-related prosecution, defendant was convicted under § 2314 for transporting fraudulently obtained property across state lines. The defendant received checks from a corporation after her cohort, an employee of the corporation, had used a computer to set up a bogus account payable. The Fourth Circuit reversed the dismissal of the indictment, and found that

---

[267] *See Riggs*, 739 F. Supp. at 421.

[268] The document, repeatedly described by prosecutors both prior to and at trial as having been closely safeguarded and valued by a prosecution witness at $80,000, was in fact publicly available from a regional Bell publications office for $13. The publicly-available document actually contained more and more specific information than did the version published electronically by Niedorf. *See* Denning, *supra* note 246, at 29; STERLING, *supra* note 23, at 265-67. Those facts, disclosed during cross-examination to the great surprise of the BellSouth witness, resulted in the voluntary dismissal of the prosecution against Niedorf; they certainly reflect the overzealousness of the prosecution of Riggs and Niedorf and the almost comical lack of preparation, perspective, and proportion on the part of the government and BellSouth. Assistant U.S. Attorney William J. Cook, in announcing the dismissal of the charges against Niedorf, stated that: "The value of the document was one of the factors in the prosecution. There were aspects of this document that we did not know were in the public domain. It was a question of the way the phone company portrayed the document." *U.S. Drops Charges Against UM Hacker*, ST. LOUIS POST-DISPATCH, July 28, 1990, at 4B. Niedorf's attorney, Sheldon Zenner, more bluntly observed that "the government accepted lock, stock, and barrel everything that BellSouth told them without an independent assessment." Michael Alexander, *Dial 1-800 . . . for Bellsouth 'Secrets,'* COMPUTERWORLD, Aug. 6, 1990, at 8 (quoting Sheldon Zenner).

[269] 553 F.2d 351 (4th Cir. 1977).

Jones's scheme was an "indictable offense" under § 2314.[270] The use of the computer there was no more than a detail; the defendant had simply come up with a fairly clever (but not clever enough), "high-tech" means of committing fraud. Although *Jones* has been held out as an example warranting the enactment of computer-specific statutes,[271] in fact that case was, and should have been, prosecuted successfully as a fraud committed in a somewhat unusual manner. The simpler, more general statute worked effectively.

B. "Property": A Definitional Problem That Isn't

The major apparent difficulty in applying general criminal statutes, such as § 641 (theft of government money, records, or "thing[s] of value") or § 1343 (wire fraud) or § 2314 (interstate transportation of stolen property), to computer-related conduct arises from the nature of computer data, and specifically from the notion of computer data as "property" or a "thing of value" within the meaning of those statutes. The House Report accompanying the original 1984 legislation specifically noted that problem:

> Experts told the Committee that we need to shift attention in our statutes from concepts such as 'tangible property' and credit and debit instruments to concepts of 'information' and 'access to information.'[272] . . . Difficulties in coping with computer abuse arise because much of the property involved does not fit well into categories of property subject to abuse or theft; a program, for example, may exist only in the form of magnetic impulses.[273]

The allied problem, noted the Report, also arises from the nature of computer data and computer transactions: "When a program of substantial commercial value is misappropriated, the person from whom it is stolen almost always remains in possession of the original. Indeed, the original program may not have been moved so much as a single inch while being illicitly copied."[274] These difficulties led the Report directly to its central conclusion: "It is obvious that traditional theft/larceny statutes are not the proper vehicle to control the spate of computer abuse and computer assisted crimes."[275]

It is true that the electromagnetic impulses that comprise computer data do not "fit well" within the idea of "property" if that idea is re-

---

270 *See id.* at 353.

271 *See* Roddy, *supra* note 32, at 353-54.

272 H.R. REP. NO. 98-894 (1984), *reprinted in* 1984 U.S.C.A.A.N. 3689, 3690.

273 *Id.* at 3695.

274 *Id.*

275 *Id.*

stricted to the ancient common-law paradigm of one's neighbor's livestock. When the old common law conceptions of larceny, and fraud arose, the notion of intangible property was utterly outside the realm of social or legal experience. By the late twentieth century, however, intangible "things" made possible by technology have long since become an unremarkable aspect of daily life. The law has developed ample precedent for addressing problems raised by property that "does not fit well" with traditional notions of property. That body of precedent affords adequate means of addressing criminal conduct involving computer technology. Wholly new legislation, focused on specific technology, is not necessary.[276]

Indeed, the House Report itself, after identifying the definition of property as a central reason for enacting computer-specific legislation, made reference to an obvious non-computer-specific solution: defining property "to include electronically processed or stored data, either tangible or intangible."[277]

Thus, one legislative response to computer-related crime is to redefine "property" or "thing of value" so as to include computer data. Both the 1979 proposed statute[278] and a proposed 1985 amendment to the CFAA would have produced precisely that result.[279] By thus broadening (or, perhaps more accurately, clarifying) the definitions of those central terms, Congress could have made clear that the conduct of Langevin or Seidlitz,[280] constituted crimes under existing federal statutes of general application, without the need for technology-specific laws. A definitional solution would render the enactment of computer-specific statutes unnecessary.

C. Theft and Trespass: A Definitional Solution

As demonstrated earlier, numerous general criminal statutes can serve effectively in computer-crime prosecutions. The traditional crimes

---

[276] "It's just like any other form of theft, except that it's more subtle and more sophisticated." Mark Potts, *'Hacker' Pleads Guilty in AT&T Case*, WASH. POST, Mar. 23, 1991, at A1 (quoting Assistant U.S. Attorney Geoffrey R. Garinther, prosecutor in *United States v. Rose*).

[277] H.R. REP. NO. 98-894 (1984), *reprinted in* 1984 U.S.C.A.A.N. 3689, 3695.

[278] *See* S. 240, 96th Cong., (1977).

[279] See S. 1678, introduced in September 1985, that would have defined "property" to include "financial instruments or information, including electronically processed or produced data and computer programs in either machine or human readable form; computer services; and any other tangible or intangible item of value." This definition, as well as other portions of the bill, was in need of some revision. The basic thrust of its definition of "property" to include computer data, however, could have facilitated the application of general criminal statutes to the computer setting.

[280] *See supra* notes 68-73.

of theft and trespass deserve particular attention. The unauthorized transfer or copying of data could fall within the proscriptions of a larceny statute. By defining property to encompass computer data, a legislature could effectively prohibit such conduct as the taking of the property of another with the intent to deprive the owner.

A scheme to "steal" computer time and storage capacity was prosecuted successfully under 18 U.S.C. § 641 (theft, conversion, or embezzlement of government property) in *United States v. Sampson.*[281] The defendants, employees of a government contractor, used for their own purposes the government-owned computers assigned to them for their jobs. Charged with theft, they argued that computer time and capacity did not constitute property within the meaning of the statute. This argument is strongly reminiscent of the argument used to support the enactment of § 1030: that computer functions do not correspond to the familiar legal concepts associated with property. Indeed, Sampson's argument appears to carry even more weight, because his conduct involved only the use of the computer's capacity, not the transfer or alteration of data; Congress's concern, in enacting § 1030, was that information—the electronic impulses that comprise computer data—could not easily be classified as property. Yet those electronic impulses surely correspond to the notion of property more easily than the "philosophical concepts"[282] of time and capacity at issue in *Sampson*. Nevertheless, the court there held that

> [t]he consumption of [the computer's] time and the utilization of its capacities seem to the court inseparable from the physical identity of the computer itself. . . . [T]he uses of the computer . . . appear to the court to be a 'thing of value' within the meaning of 18 U.S.C. § 641, sufficient upon which to predicate a legally sufficient indictment.[283]

Thus, even where the property was considerably less tangible than in most computer prosecutions, the traditional law of theft applied.

Another very early computer-crime case provides further illustration both of the problem of "property" in relation to computers, and of a graceful and effective solution of that problem. *Ward v. Superior Court,*[284] decided under California state law, squarely presented the question of whether computer data ("impulses")[285] constituted an "article" under the trade secret[286] or theft[287] statutes. In *Ward*, the de-

---

[281] 6 Computer L. Serv. Rep. 879 (N.D. Cal. 1978).

[282] *See id.* at 880.

[283] *Id.*

[284] 3 Computer L. Serv. Rep. 206 (Cal. Super. Ct. 1972).

[285] *See id.* at 208.

[286] *See id.* (quoting CAL. PENAL CODE § 499c (prohibiting the stealing, taking or carry-

fendant had accessed without authorization proprietary computer information, downloaded it onto his own computer, and subsequently printed out a hard copy of the data. The court denied a motion to dismiss only because the defendant had printed out a "tangible" copy of the information.[288] The electronic impulses transferred by telephone and modem were held explicitly to be "not tangible and hence do not constitute an 'article'" within the meaning of the trade-secret statute.[289] The crucial word "article" was statutorily defined as an "object, material, device or substance or copy thereof, including any writing, record, recording, drawing, sample, specimen, prototype, model, photograph, microorganism, blueprint or map."[290] Reasoning that "[a]ll of the foregoing things are tangible and under the principle of ejusdem generis, telephonic impulses would not constitute an article representing a trade secret[,]"[291] the court rejected the argument that taking and carrying away computer data amounted to theft.

This decision could well be taken as support for the view that only computer-specific statutes, not statutes of general application, would be effective in combating this type of conduct. The court's opinion, however, offers support for the opposite view. First, of course, the court could have read more expansively the statutory definition itself ("or substance or copy thereof") so as to include a computerized copy as the "substance or copy" of the trade secret. More generally, however, because the court relied so heavily on the precise language of the statute, a simple amendment to the statutory definition would have compelled the opposite outcome. If the legislature had chosen to include in that definition an explicit reference to computer data, or computer-generated copies or representations, the statute would have encompassed Ward's conduct, without the need for an entirely new, computer-specific statute. If his conduct amounted to the theft of a trade secret, it could then have been prosecuted under the trade-secret statute.

Similarly, intentionally gaining unauthorized access to information could fall within the scope of a traditional trespass statute (unlawfully entering the property of another), if the definition of property under that statute explicitly included a computer, computer program, or computer system. The essence of trespass, unlawful entry, corresponds quite neatly to the unauthorized accessing of electronic property. The 1985

---

ing away of any article representing a trade secret)).

287 *See id.* at 211 (citing CAL. PENAL CODE § 487).

288 *See id.* at 208-09.

289 *See Ward*, 3 Computer L. Serv. Rep. at 208.

290 *Id.*

291 *Id.*

proposed amendment to the CFAA,[292] which included a provision punishing "[w]hoever intentionally without authorization obtains access to a computer or a computer system or computer network," was presented to the Congress with this explanation:

> The conduct proscribed in [this section] is akin to a trespass onto someone else's property. A person who rummages through the information contained in a computer . . . causes the same harm as an intruder who clandestinely enters a person's home to look through the contents of the owner's personal records and documents.[293]

The key to that analogy is its focus on "harm." The harm caused by an intrusion into one's home corresponds closely to the harm caused by an intrusion into one's computer. The details of the conduct, of course, are quite different; the means by which the intrusion is effected is vastly different. The harm, however, is the same, and can be addressed legislatively in much the same way. Far from supporting the computer-specific CFAA, that legislative history supports precisely the opposite conclusion: that unauthorized access of a computer is much like unauthorized access of real property, and could be prosecuted under a trespass statute.

By using traditional criminal statutes, most notably trespass and larceny, and by redefining property to include computer data, legislatures could avoid the problems of redundancy, overbreadth, and imprecision inherent in computer-specific legislation. That approach, both simple and effective, could avoid the problem of ever-changing technology and make use of established precedent. Reliance on traditional statutes fosters a legislative focus on harmful results, rather than on the use of technology itself.

CONCLUSION

The criminal law is, and should be, concerned with punishing or deterring harmful conduct. In the area of computer crime, as in every other area of the criminal law, the legislative focus should remain on that important goal. To the extent that lawmakers turn their attention to computers rather than to harmful conduct, they are distracted from their proper role.

By enacting computer-specific criminal statutes, legislators encourage prosecutors, the public, and themselves to think in terms of technology rather than conduct. Such statutes suggest that it is the use of tech-

---

[292] *See supra* note 279 and accompanying text.

[293] 131 CONG. REC. S11,872 (daily ed. Sept. 20, 1985).

nology itself, rather than the causation of harm, that must be punished or deterred.

By relying instead on criminal statutes of more general application, legislators can prohibit harmful conduct whether accomplished with a computer or not. Rather than being frightened or seduced into punishing the use of the computer, lawmakers can properly return their focus to the prevention of criminal conduct.