Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes

by

Orin S. Kerr
GWU Law School

NYU Law Review, Vol. 78, No. 5, pp. 1596-1668, November 2003

ARTICLES

CYBERCRIME'S SCOPE: INTERPRETING "ACCESS" AND "AUTHORIZATION" IN COMPUTER MISUSE STATUTES

ORIN S. KERR*

The federal government, all fifty states, and dozens of foreign countries have enacted computer crime statutes that prohibit "unauthorized access" to computers. No one knows what it means to "access" a computer, however, or when access becomes "unauthorized." The few courts that have construed these terms have offered widely varying interpretations. Several recent decisions suggest that any breach of contract renders an access unauthorized, broadly criminalizing contract law on the Internet. In this Article, Professor Orin Kerr explains the origins of unauthorized access statutes, and examines why the early beliefs that such statutes articulated a clear standard have proven remarkably naïve. He then shows how and why the courts have construed these statutes in an overly broad manner that threatens to criminalize a surprising range of innocuous conduct involving computers. Finally, Professor Kerr offers a normative proposal for interpreting "access" and "authorization." Courts should reject a contract-based theory of authorization, and should limit the scope of unauthorized access statutes to circumvention of code-based restrictions on computer privileges. This proposed interpretation best mediates between securing privacy and protecting the liberty interests of Internet users. It also mirrors criminal law's traditional treatment of consent defenses, and avoids possible constitutional difficulties that may arise under the broader constructions that courts have recently favored.

INTRODUCTION

Justice Holmes once noted that when a legislature enacts a new crime, "it is reasonable that a fair warning should be given to the world in language that the common world will understand, of what the law intends to do if a certain line is passed. To make the warning fair, so far as possible the line should be clear."[1] In the physical world, this aspiration retains its force because the basic language and principles of most serious crimes date back hundreds of years and have changed

* Associate Professor, George Washington University Law School. Thanks to Michael Birnhack, William Bratton, Jack Friedenthal, Stephen Henderson, Mark Lemley, Tom Morgan, Ellen Podgor, Pamela Samuelson, Peter Smith, Peter Swire, Jonathan Zittrain, and the participants in the George Washington University and George Mason University law faculty workshops for comments on an earlier draft. This Article was supported in part by a generous grant from the Dean's Fund at George Washington University Law School.

[1] McBoyle v. United States, 283 U.S. 25, 27 (1931).

little over time.[2] Although the exact contours of crimes vary from jurisdiction to jurisdiction, and ambiguities will always exist, the basic meaning of crimes such as murder, burglary, and theft is broadly understood.[3]

Not so with computer crimes. In the last quarter century, the federal government,[4] all fifty states,[5] and over forty foreign countries[6] have enacted computer crime laws that prohibit "unauthorized access" to computers.[7] The prohibition against unauthorized access to computers is new, however, and remains a mystery.[8] What does it mean to "access" a computer? Under what circumstances does access become "unauthorized?" The few courts that have reached these questions have offered inconsistent interpretations.[9] Commentators

[2] See William J. Stuntz, The Pathological Politics of Criminal Law, 100 Mich. L. Rev. 505, 512 (2001) ("Save for auto theft, everything in the list of FBI index crimes was a crime in Blackstone's day.").

[3] See Brian Leiter, Positivism, Formalism, Realism, 99 Colum. L. Rev. 1138, 1162 (1999) (noting that while "most citizens know relatively little about what the law is," criminal law's basic prohibitions of "murder, bank robberies, and rape" are well known to general public).

[4] See 18 U.S.C. § 1030 (2000).

[5] The state statutes are listed in Susan W. Brenner, State Cybercrime Legislation in the United States of America: A Survey, 7 Rich. J.L. & Tech. 28, ¶15 n.37 (2001), at www.richmond.edu/jolt/v7i3/article2.html, and are discussed in extensive detail in A. Hugh Scott, Computer and Intellectual Property Crime: Federal and State Law 639-1300 (2001).

[6] See Stein Schjolberg, Unauthorized Access to Computer Systems: Penal Legislation in 44 Countries (2002), at http://www.mosstingrett.no/info/legal.html. Those countries are Argentina, Australia, Austria, Belgium, Brazil, Canada, Chile, China, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, India, Ireland, Iceland, Israel, Italy, Japan, Latvia, Luxembourg, Malaysia, Malta, Mauritius, Mexico, New Zealand, Norway, Poland, Portugal, Philippines, Singapore, South Africa, Spain, Sweden, Switzerland, Tunisia, Turkey, the United Kingdom, and Venezuela. Id.

[7] Different jurisdictions adopt slightly different terminology. See Scott, supra note 5, at 21-22 (discussing different terminology); Brenner, supra note 5, at 35-37 (same). Most jurisdictions prohibit "access without authorization" to computers. See, e.g., 18 U.S.C. § 1030(a)(4) (2000). Some also prohibit "exceed[ing] authorized access" to computers. See, e.g., 18 U.S.C. § 1030(a)(2). For the sake of simplicity, I will refer to the different phrases collectively as "unauthorized access," and the various statutes as unauthorized access statutes. R R

Notably, most unauthorized access statutes require a knowing mens rea for both access and authorization. See, e.g., 18 U.S.C. § 1030(a)(4). The significance of this mens rea requirement hinges on the proper interpretation of access and authorization, the focus of this article. Challenges to the mens rea of unauthorized access statutes have arisen only when the statute also requires the causation of damage, e.g., 18 U.S.C. § 1030(a)(5), and defendants have argued that although they knew that they accessed the computer without authorization, they did not intend to cause damage, see, e.g., United States v. Sablan, 92 F.3d 865, 869 (9th Cir. 1996) (rejecting argument that 1994 version of § 1030(a)(5) requires intent to cause damage to victim's computer). A possible exception is *State v. Fugarino*, 531 S.E.2d 187 (Ga. Ct. App. 2000), discussed infra notes 166-73. R

[8] See infra Part III for a discussion of several analogous criminal law doctrines.

[9] See infra Part II.

have ignored these questions entirely.[10] The result is an odd situation in which nearly every Anglo-American jurisdiction has an unauthorized access statute that carries serious felony penalties, but no one seems to know what these new laws cover.

The uncertain scope of unauthorized access statutes recently assumed greater importance in the wake of a series of civil cases interpreting the federal statute, 18 U.S.C. § 1030, sometimes called the Computer Fraud and Abuse Act.[11] These decisions suggest that unauthorized access statutes broadly criminalize the law of contract involving the use of computers.[12] That is, any computer use that vio-

[10] Despite the growing body of interesting scholarly work on computer crime law, the existing scholarship has missed the difficult questions raised by the terms "access" and "authorization." The literature almost universally assumes that access and authorization have obvious meanings. See, e.g., Scott, supra note 5, at 75-122 (reviewing federal unauthorized access statute but not discussing meaning of access or authorization); Frank P. Andreano, The Evolution of Federal Computer Crime Policy: The Ad Hoc Approach to an Ever-Changing Problem, 27 Am. J. Crim. L. 81 (1999) (same); Eric J. Bakewell et al., Computer Crimes, 38 Am. Crim. L. Rev. 281 (2001) (reviewing different types of computer crimes); Susan W. Brenner, Is There Such a Thing as "Virtual Crime?", 4 Cal. Crim. L. Rev. 1 (2001) (comparing unauthorized access statutes to traditional crimes); Brenner, supra note 5 (reviewing state unauthorized access statutes); Neal Kumar Katyal, Criminal Law in Cyberspace, 149 U. Pa. L. Rev. 1003, 1021 (2001) (stating that "[t]he crime of unauthorized access is one of simply invading another's workspace," but not explaining meaning of access or authorization); Joseph M. Olivenbaum, <CTRL><ALT><DELETE>: Rethinking Federal Computer Crime Legislation, 27 Seton Hall L. Rev. 574 (1997) (discussing federal unauthorized access statute, but not discussing meaning of authorization or access); Eric J. Sinrod & William P. Reilly, Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws, 16 Santa Clara Computer & High Tech. L.J. 177 (2000) (same); Jo-Ann M. Adams, Comment, Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet, 12 Santa Clara Computer & High Tech. L.J. 403 (1996) (same); Haeji Hong, Note, Hacking Through the Computer Fraud and Abuse Act, 31 U.C. Davis L. Rev. 283 (1997) (same). Perhaps the only exception is an online article that discusses "access." See Ethan Preston, Finding Fences in Cyberspace: Privacy and Open Access on the Internet, 6.1 J. Tech. L. & Pol'y 3 (2000), at http://grove.ufl.edu/~techlaw/vol6/Preston.html. R R

[11] The Computer Fraud and Abuse Act of 1986 created the modern version of 18 U.S.C. § 1030, expanding on the initial version first enacted in 1984. See Pub. L. No. 99-474, 100 Stat. 1213 (1986) (codified as amended at 18 U.S.C. § 1030). Technically speaking, the name "Computer Fraud and Abuse Act" and its sometimes-used acronym CFAA refer only to the 1986 amendments. In practice, however, courts and commentators use both labels to refer to the entire federal unauthorized access statute, 18 U.S.C. § 1030. The civil provisions of § 1030 were first added in 1994, and allow a victim of computer crime to bring a civil action against a wrongdoer. See 18 U.S.C. § 1030(g). This provision has allowed several judicial decisions interpreting the scope of the criminal statute to arise in a civil context.

[12] See EF Cultural Travel BV v. Zefer, 318 F.3d 58, 61 (1st Cir. 2003) (noting that use of proprietary information in violation of contract to mine competitor's public website for information "exceeds authorized access"); EF Cultural Travel BV v. Explorica, 274 F.3d 577, 583 (1st Cir. 2001) (same); Register.com v. Verio, 126 F. Supp. 2d 238, 251 (S.D.N.Y. 2000) (holding use of search robot against explicit wishes of system owner to be unauthorized access). These cases are discussed extensively infra Part II.C.3.

lates an implicit or explicit contract with the computer's owner exceeds the authorization that the owner has granted the user, and therefore violates the federal unauthorized access statute.[13] These precedents have arisen in the civil context, and have not yet been applied to criminal cases. Given the usual rule that civil precedents apply to criminal cases,[14] however, these cases threaten a dramatic and potentially unconstitutional expansion of criminal liability in cyberspace. Because Internet users routinely ignore the legalese that they encounter in contracts governing the use of websites, Internet Service Providers (ISPs), and other computers,[15] broad judicial interpretations of unauthorized access statutes could potentially make millions of Americans criminally liable for the way they send e-mails and surf the Web.

This Article presents a comprehensive inquiry into the meaning of unauthorized access statutes, and particularly the foundational concepts of "access" and "authorization." Its purposes are historical, descriptive, and normative. First, the Article explains why legislatures enacted unauthorized access statutes, and why their proponents believed that such statutes could respond effectively to the problem of computer misuse. Next, the Article shows that this perception has proved strikingly naïve. Unauthorized access statutes raise rich and complex questions that the enacting legislatures never recognized, much less resolved. Courts have struggled to define these terms because the Internet offers various competing guideposts to measure access and determine authorization. Technological change has added to the problem as well. New platforms such as the World Wide Web have further complicated the search for a coherent and sensible interpretation of access and authorization.

The final Part of the Article offers a solution to the question of how courts should interpret unauthorized access statutes. Courts should distinguish between the two ways in which use of a computer may exceed the rights granted to a user. First, a user can violate a contractual agreement with the owner or operator of the computer. Second, a user can circumvent a code-based restriction on the user's

---

[13] See infra Part II.C.

[14] The courts generally apply civil precedents in the criminal context unless there is evidence that Congress did not intend the same standard to govern. See, e.g., United States v. Bigham, 812 F.2d 943, 948 (5th Cir. 1987) (noting that when Congress allows same standard to govern criminal and civil cases, it is "of no significance . . . [w]hether a case is brought on the civil or criminal side of the docket").

[15] Such agreements have become a standard aspect of many employment relationships, for example, although most employees do not know their terms. See, e.g., United States v. Angevine, 281 F.3d 1130, 1132-33 (10th Cir. 2002) (reviewing computer use policy that governed workplace use of professor's computer and included restrictions on use).

privileges. In the first case, the use of the computer is unauthorized in the sense that it violates an implicit (and sometimes explicit) contract. An example would be use that violates the Terms of Service that an ISP imposes on its customers. In the latter case, the use is unauthorized in the sense that it bypasses a code-based effort to limit the scope of the user's privileges. An example might be use of a stolen password to bypass the password gate designed to block access to a victim's account.

This Article proposes that courts should reject contract-based notions of authorization, and instead limit the scope of unauthorized access statutes to cases involving the circumvention of code-based restrictions. The fact that computer use violates a contractual restriction should not turn that use into an unauthorized access. The bypassing of a code-based restriction such as a password gate should be required to trigger criminal liability, such that hacking into a computer could be an unauthorized access, but violating Terms of Service would not be. This standard counsels future courts to reject the suggestions of recent civil decisions that the federal unauthorized access statute criminalizes contract law. Courts should require a higher threshold for access to be deemed "without authorization" under the criminal laws; they should require, at a minimum, the circumvention of a code-based restriction on computer access.

My proposal offers several distinct advantages over the alternatives. As a policy matter, it draws a workable line between privacy and openness. It protects the privacy of users who guard their information effectively, but it also allows individuals to use the Internet without fear of criminal prosecution for a violation of sometimes incomprehensible contractual limits on use. On a doctrinal level, the recommended approach tracks the traditional treatment that analogous issues have received in criminal law, namely in the interpretation of consent defenses for crimes such as burglary, trespass, and rape. The approach is also consistent with the traditional theories of criminal punishment. And finally, the approach avoids constitutional difficulties, such as vagueness or overbreadth, that broader interpretations of unauthorized access statutes may create.

My hope is that this Article will push courts, legislators, and commentators to adopt a more sophisticated understanding of the scope and meaning of unauthorized access statutes. Courts and commentators alike often speak of "access" and "authorization" as if the terms were self-defining.[16] But they are not. Blithely unaware of the diffi-

[16] See, e.g., United States v. Morris, 928 F.2d 504, 511 (2d Cir. 1991) (rejecting defendant's request for jury instruction on meaning of "authorization" on grounds that "the

cult choices that these statutes present, courts have begun to create a body of precedent that threatens to criminalize a remarkably broad range of conduct. If future courts follow the lead of recent cases, the disturbing implications of these initial cases will be realized and may prove difficult to change. This Article will attempt to illuminate the choices and dangers lurking within these statutes, and perhaps persuade judges to reject the recent precedents and embark upon a better path.

The broader purpose of this Article is to advance a critical dialogue over how the law criminalizes misconduct involving computers and the Internet, and to use the example of computer crime statutes as a case study of how law can and should respond to technological change. Unauthorized access statutes are creatures of the 1970s, when the Internet remained the domain of a few scientists and engineers. Today over 110 million Americans use the Internet,[17] employing technologies ranging from Microsoft Windows to the World Wide Web that computer scientists of the 1970s could not have imagined. While technology has advanced considerably in the last three decades, the law has not; the same one-size-fits-all prohibitions on unauthorized access still govern. The time has come to focus on the scope of these statutes, and to ask whether they have outlived their usefulness—and if so, what should replace them.

This Article proceeds in three parts. Part I introduces the concept of computer misuse and reviews the history of efforts to use criminal law to punish and deter it. The analysis explores the difficulties courts faced in applying property laws such as theft to computer crimes, and how dissatisfaction with those efforts led legislatures to enact computer crime laws that prohibit unauthorized access to computers. Part II reveals the ambiguities latent in unauthorized access statutes, and shows how the courts have struggled to define "access" and "without authorization" in a coherent way. Rather than place sensible limitations on the scope of these statutes, courts have embraced expansive conceptions that threaten to criminalize any breach of contract or employee disloyalty involving computers. Finally, Part III offers a normative proposal for the interpretation of

word is of common usage, without any technical or ambiguous meaning"). For scholarly analyses of unauthorized access statutes that reflect a similar approach, see sources cited supra note 10. A few recent court decisions have at least begun to acknowledge some of the difficulties. See, e.g, *EF Cultural Travel BV*, 274 F.3d at 582 n.10 ("Congress did not define the phrase 'without authorization,' perhaps assuming that the words speak for themselves. The meaning, however, has proven to be elusive."). R

[17] See Pew Internet and Am. Life Project, Internet Activities (2002) (estimating that 111 million Americans use Internet), available at http://www.pewinternet.org/reports/chart.asp?img=Internet_Activities.jpg.

"unauthorized access." Courts should rein in the scope of computer crime laws by rejecting contract-based notions of authorization and limiting the scope of unauthorized access statutes to the circumvention of code-based restrictions.

I
THE PROBLEM OF COMPUTER MISUSE AND THE FAILURE OF A PROPERTY-BASED SOLUTION

Computer crime statutes were first enacted in the late 1970s in response to perceived failures of preexisting laws to respond to computer misuse.[18] To understand why legislatures enacted these new statutes, it helps to understand how the prior regime failed. This Part introduces the problem of computer misuse, and reviews how courts struggled to apply traditional property laws to misuse before legislatures enacted computer crime statutes. This Part has two goals: first, to introduce the reader to the concept of computer misuse that prompted the enactment of unauthorized access statutes; and second, to explain why the failures of property-based criminal laws to address the new computer crimes made the new laws against unauthorized access to computers appear necessary. The new laws did not spring forth from a vacuum; they seemed to be a reasonable response to a particular problem. This Part explores that problem.

A. The Problem of Computer Misuse

The broad umbrella category of "computer crimes" can be divided into two types of substantive offenses: traditional crimes committed using computers, and crimes of computer misuse.[19]

Traditional crimes committed using computers are easy to understand. Examples include Internet fraud schemes, Internet gambling, online distribution of child pornography, and cyberstalking. These crimes involve the online commission or facilitation of traditional

[18] See infra Part II.

[19] This is my own dichotomy; other authors have used other approaches. See, e.g., Donn B. Parker, Fighting Computer Crime 17 (1983) (arguing that computer crimes can be divided into cases in which computers are used as object, subject, instrument, or symbol); Scott Charney & Kent Alexander, Computer Crime, 45 Emory L.J. 931, 934 (1996) (classifying computer crimes as offenses in which computer is target of offense, tool of traditional offense, or storage device for evidence). The Charney and Alexander approach is similar to my own. For example, my category of computer misuse offenses is similar if not identical to Charney and Alexander's category of offenses in which the computer is a target. I differ with Charney and Alexander primarily with regard to their third category—crimes in which a computer is used as a storage device for evidence. This is really the field of criminal procedure, as opposed to substantive criminal law, and I think it is helpful to recognize this as a distinct area.

criminal offenses. Consider the plague of child pornography and child exploitation crimes. Two decades ago, a pedophile seeking to obtain illegal images of child pornography would seek out a book or magazine containing the images. Today, the same pedophile likely would turn to the Internet, and seek out chat rooms and underground clubs that distribute these illegal images in digital form.[20] A pedophile who two decades ago might have tried to seduce children at a school playground, today would be more likely to attempt an analogous seduction in an Internet chat room. In both cases, computers and the Internet provide a new way of committing a preexisting criminal offense.

For the most part, traditional crimes committed using computers raise few new issues for criminal law. The basic crimes remain the same regardless of whether wrongdoers use computers or some other means to commit them. For example, a death threat is still a death threat regardless of whether it is transmitted via e-mail or a telephone call.[21] Reasons may exist in some circumstances to regulate such crimes differently when they occur via computers and the Internet.[22] But in general, the basic issues raised by traditional crimes do not change when they happen to be committed using computers.

Crimes of computer misuse represent a new type of crime, however, and pose fresh challenges for criminal law. We can define computer misuse as conduct that intentionally, knowingly, recklessly, or negligently causes interference with the proper functioning of computers and computer networks. Common examples include computer hacking, distribution of computer worms and viruses, and denial-of-

[20] See generally Philip Jenkins, Beyond Tolerance: Child Pornography on the Internet (2001) (detailing prevalence and ready availability of child pornography to pedophiles online).

[21] Compare United States v. Darby, 37 F.3d 1059, 1060-61 (4th Cir. 1994) (describing telephone death threat), with United States v. Scott, 42 Fed. Appx. 264, 265 (10th Cir. 2002) (describing e-mail death threat), and United States v. Kammersell, 196 F.3d 1137, 1138 (10th Cir. 1999) (describing instant message death threat).

[22] For example, the U. S. Sentencing Guidelines provide for an enhanced punishment in child pornography possession offenses "[i]f the defendant's possession of the material resulted from the defendant's use of a computer." U.S. Sentencing Guidelines Manual § 2G2.4(b)(3) (2002). The different treatment has been explained as a reaction to the fact that the Internet both facilitates such offenses and makes it more difficult to detect and prosecute offenders. As the Ninth Circuit has explained, "it is difficult to detect and prevent this traffic in cyberspace. U.S.S.G. § 2G2.4(b)(3) provides an extra deterrent to those inclined to pursue illicit pictures in the anonymity of the computer world." United States v. Fellows, 157 F.3d 1197, 1202 (9th Cir. 1998); see also Katyal, supra note 10, at 1006 R ("Cyberspace presents unique opportunities for criminals to reduce their perpetration costs; the probability of success in inflicting a certain level of harm while holding expenditures constant is greater. Accordingly, the law should develop mechanisms to neutralize these efficiency advantages.").

service attacks.[23] Computer misuse upsets users' reliance on the rights and privileges provided by computer owners and operators. For example, a personal e-mail account ordinarily gives its owner the right to access e-mail along with the privilege of exclusive access to that e-mail. An outsider who guesses the owner's password and reads the owner's e-mails denies her the assurance that her personal e-mails have remained private, secure, and confidential. Such an act of computer misuse violates the rights and privileges that the account owner was granted when she obtained the account.[24]

At a conceptual level, computer misuse can occur in two distinct ways. First, a user can exceed her privileges on a computer, either by using a computer that she has no authority to use, or by using the computer in a way that she is not authorized to use it. For example, a person can hack into a corporate network and see secret files that the person is not supposed to view. In such a case, the hacker will have exceeded her privileges on the network; she will see more than the network was configured to allow her to view. Second, a person can cause a denial of privileges, blocking another user from being able to enjoy her full privileges on a computer. For example, a person can deliver a denial-of-service attack that incapacitates a network, blocking its use. In this case, other users will try to exercise their rights to use the network, but will find that they cannot. These two types of computer misuse are two sides of the same coin: In the first case, the user exceeds her privileges; in the second, the user denies privileges to others. Both interfere with the rights and privileges that computers have been configured to allow.

Computer misuse is an important new type of criminal offense because it can cause serious harms, both economic and noneconomic. For example, computer misuse that exceeds privileges often results in serious invasions of privacy. The more that individuals store their private information in electronic form, the greater the possible invasion of privacy if others obtain access to their private information without

[23] I will assume that the reader is familiar with the basic types of computer misuse crimes such as hacking and the distribution of viruses. Many prior works explain the underlying technology and threats in considerable detail. See, e.g., Katyal, supra note 10, at 1023-27; Sinrod & Reilly, supra note 10, at 187-225. R R

[24] Notably, traditional crimes and computer misuse crimes can coexist in practice. Computer misuse sometimes occurs as part of a broader scheme to commit a traditional crime. For example, imagine that a high-tech bank thief hacks into the computer network of a major banking institution, sets up a false account remotely, and instructs the bank's computer that the false account contains $10 million. The thief then steals money from the bank by withdrawing money from the account. On one hand, this is a traditional crime: bank theft. On the other hand, the bank theft was furthered by engaging in computer misuse. The computer misuse crime of hacking into the bank's computer helped further the traditional crime of bank theft.

the owner's permission. Computer misuse can also trigger heavy economic losses. While comprehensive figures remain elusive, experts estimate that computer crimes cause many billions of dollars of loss every year.[25] These economic harms vary tremendously depending on the offense, but can reach levels rarely seen in traditional criminal offenses. For example, the "I Love You" computer virus that spread around the world in May 2000 caused losses to its victims estimated to be as high as $10 billion.[26]

B. The Use of Trespass and Burglary Law to Address Computer Misuse

The enormous potential harms of computer misuse first became apparent in the early 1970s.[27] At that time, no legislature had enacted a computer crime statute. When prosecutors considered bringing criminal charges for computer misuse, they naturally turned to existing property crime laws, such as laws prohibiting trespass, burglary, and theft. The fit proved a poor one, however. In the case of trespass and burglary, the scope of existing laws plainly did not extend to computer misuse. In the case of theft, the law could be stretched to apply, but required judicial sleight of hand and resort to an unpredictable legal fiction. Taken together, the efforts to apply existing statutes to computer misuse produced an unsatisfying, results-oriented jurisprudence that inspired the passage of dedicated computer crime statutes.

Consider the crimes of trespass and burglary, both predominantly state offenses.[28] Trespass crimes generally punish knowing entrance or presence on another person's property despite notice that the prop-

---

[25] See Charles Piller, Losses from Computer Crime Show Major Increase, FBI Survey Finds, L.A. Times, Mar. 12, 2001, at C2 (summarizing results of 2001 survey by Computer Security Institute and FBI).

[26] See Patricia L. Bellia, Chasing Bits Across Borders, 2001 U. Chi. Legal F. 35, 36.

[27] The first major computer misuse prosecution that led to a published decision was *Ward v. Superior Court*, 3 Computer L. Service Rep. (Callaghan) 206 (Cal. Super. Ct. 1972). Books on computer misuse began appearing in the early-to-mid 1970s. See, e.g., August Bequai, Computer Crime (1978); Gerald McKnight, Computer Crime (1973); Donn B. Parker, Crime By Computer (1976).

[28] Notably, no general federal trespass or burglary law exists. The only existing federal laws that apply to trespass and burglary are quite narrow laws that Congress has enacted to protect certain kinds of federal land and other protected properties. For example, a person who "goes upon" U.S. military land for an unlawful purpose commits a federal misdemeanor, 18 U.S.C. § 1382 (2000) (providing for punishment of "[w]hoever, within the jurisdiction of the United States, goes upon any military, naval, or Coast Guard reservation, post, fort, arsenal, yard, station, or installation, for any purpose prohibited by law or lawful regulation"), as does someone who "goes upon" Indian land without authorization, 18 U.S.C. § 1165. Similarly, it is a regulatory crime to trespass on a National Park. 36 C.F.R. § 261.9(e) (2002) (prohibiting "entering any building, structure, or enclosed area owned or

erty owner forbids it.[29] At common law, burglary prohibited "breaking and entering" into a building without authorization and with the intent to commit a crime therein.[30] Modern statutes tend to focus more on entering a building or occupied structure without license or privilege, combined with intent to commit a crime inside.[31] Like trespass crimes, burglary focuses on the entry onto property without permission. Unlike trespass, however, burglary requires the intent to commit a crime, and usually carries relatively stiff criminal penalties.[32]

At first blush, trespass and burglary law may appear to provide a logical starting point for applying property crimes to punish and deter computer misuse. It has been noted widely that many acts of computer misuse resemble trespasses.[33] A user can exceed her privileges on a computer much like a trespasser can exceed her privileges on physical land. Computer hacking, for example, is akin to a trespass in cyberspace.[34] Similarly, a hacker may break into a computer with intent to do mischief much like a burglar might break into a house with the same intent.[35]

Despite the common principles, it seems that criminal trespass and burglary statutes have never been used to prosecute computer misuse. The primary reason is that both trespass and burglary statutes remain closely tied to the physical world rather than a virtual one.[36]

---

controlled by the United States when such building, structure, or enclosed area is not open to the public" within National Park).

[29] See Model Penal Code § 221.2 (1962).

[30] See Wayne R. LaFave, Criminal Law § 8.13 (3d ed. 2000).

[31] See, e.g., Model Penal Code § 221.1 (1962) ("A person is guilty of burglary if he enters a building or occupied structure, or separately secured or occupied portion thereof, with purpose to commit a crime therein, unless the premises are at the time open to the public or the actor is licensed or privileged to enter.").

[32] See Model Penal Code § 221.1 (1962).

[33] See, e.g., Olivenbaum, supra note 10, at 578-79 ("Computers are not so unique that the criminal law must be rewritten to account for them; indeed, most 'computer crimes' correspond quite closely to older crimes, notably trespass or larceny."). R

[34] See Brenner, supra note 10, at ¶ 80 ("Hacking is obviously analogous to physical trespass. In both, the offender gains access to an area—a physical location in trespass and a virtual location in hacking—to which she does not lawfully have access."). R

[35] See id. at ¶ 84 ("Cracking is obviously analogous to the crime of burglary: In both, the offender gains access to that area—again, a physical location in burglary and a virtual location in cracking—to which she does not lawfully have access and does so for the purpose of committing an offense, such as fraud or theft, once inside.").

[36] Another possible reason is that few jurisdictions have trespass statutes with serious criminal penalties. Trespass did not constitute a crime at common law, but was only a civil wrong. See 3 Wm. L. Burdick, The Law of Crime § 720, at 71 (1946). Violations of the Model Penal Code's criminal trespass statute, § 221.2, are considered noncriminal; violations become criminal (and even then only a petty misdemeanor) only if a trespasser defies an order to leave personally communicated to him. See Model Penal Code § 221.2(2) (1962) ("An offense under this Subsection constitutes a petty misdemeanor if the offender

For example, trespass statutes generally require that that "part of the defendant's *person* pass[ ] the line of the threshold"[37] of the property trespassed. The same goes for burglary offenses.[38] Criminal trespass and burglary statutes focus narrowly on presence of a human body on physical land, not interference with property rights more generally. This limited scope makes it difficult to apply trespass or burglary statutes to computer misuse; because the user does not physically enter the target computer, the existing statutes do not apply.[39] Indeed, it appears that no criminal prosecution has ever used burglary or general criminal trespass statutes to prosecute computer misuse.[40]

C. The Use of Theft Law to Address Computer Misuse

In contrast with burglary and trespass, the crime of theft was often used to prosecute computer misuse in the era before unauthorized access statutes appeared.[41] Theft crimes consist of a family of

---

defies an order to leave personally communicated to him by the owner of the premises or other authorized person. Otherwise it is a violation."); see also Model Penal Code § 1.04(5) (1962) ("A violation does not constitute a crime . . . ."). Although most American jurisdictions have enacted some kind of criminal trespass statute to supplement civil remedies, most are much narrower than their common law civil counterparts.

[37] 3 C. Torcia, Wharton's Criminal Law § 331, at 202 (14th ed. 1980) (emphasis added). Notably, a few jurisdictions define "enter" more broadly. For example, the Delaware criminal trespass statute states that "[a] person 'enters' upon premises when the person introduces any body part or any part of any instrument, by whatever means, into or upon the premises." Del. Code Ann. tit. 11, § 829(e) (2003). However, even this broad statute keeps its focus on the tangible world.

[38] See, e.g., Cal. Penal Code § 459 (West 2002) ("Every person who enters any house, room, apartment, tenement, shop, warehouse, store, mill, barn, stable, outhouse or other building, tent, [or] vessel . . . with intent to commit grand or petit larceny or any felony is guilty of burglary."). Once again, the focus is solely on the location of a person in the physical world.

[39] See Olivenbaum, supra note 10, at 577 ("The paradigm of trespass, descended from centuries-old common law, is the unlawful entry onto real estate . . . . The electronic intruder has not entered the property of anyone, certainly not in the old common-law sense of entry onto real estate."). R

[40] I say "appears" because it is difficult, if not impossible, to prove a negative. Notably, however, many civil cases have proceeded on a common law trespass to chattels theory. See, e.g., Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003) (finding no trespass when electronic communication neither damages nor impairs functioning of recipient computer system). For a critique of the use of trespass to chattels doctrine applied to the Internet, see Dan L. Burk, The Trouble with Trespass, 4 J. Small & Emerging Bus. L. 27 (2000) (arguing that trespass paradigm is too broad).

[41] Almost all of the criminal charges against computer misuse have been brought under the family of theft crimes. See, e.g., infra notes 51-55 and accompanying text. A small set of cases have been brought under stolen property criminal laws. For example, in *People v. Johnson*, 560 N.Y.S.2d 238, 239 (N.Y. Crim. Ct. 1990) and *People v. Molina*, 547 N.Y.S.2d 546, 547 (N.Y. Crim. Ct. 1989), prosecutors charged defendants with possession of stolen property for knowing the passwords to stolen AT&T calling cards. In both cases, the defendants appeared to be selling long-distance phone calls at Port Authority terminal pay phones in Manhattan for a steep discount using stolen PINs that controlled access to the R

related offenses, including larceny, embezzlement, conversion, fraud, and false pretenses.[42] Today, most states have consolidated these various crimes into a single theft statute, which prohibits larceny, embezzlement, and false pretenses together.[43] Federal theft crimes are more limited in scope, reflecting the constitutional limits of federal criminal law.[44] The mail fraud and wire fraud statutes are the broadest federal theft offenses; they prohibit many interstate fraudulent schemes to obtain property.[45] These statutes make it illegal to send an interstate wire, radio, or television communication, or to place a stolen item in the U.S. mail or with an interstate mail carrier, to help further a fraudulent scheme designed to obtain money or property.[46]

AT&T computers. Lacking strong evidence of a sale that could provide a basis for fraud or theft charges, the government instead prosecuted the defendants for mere knowledge of the stolen passwords. The *Molina* court rejected the theory, but the *Johnson* court accepted it, finding that the passwords were property and that knowledge of the stolen passwords constituted possession of stolen property. See *Johnson*, 560 N.Y.S.2d at 242-44; *Molina*, 547 N.Y.S.2d at 547.

[42] See generally LaFave, supra note 30, §§ 8.1-8.8. Among these, only larceny existed at common law. See George P. Fletcher, The Metamorphosis of Larceny, 89 Harv. L. Rev. 469, 475 (1976) (describing development of larceny doctrine). Larceny was defined at common law as the trespassory taking and carrying away of the personal property of another with intent to steal it. See 4 William Blackstone, Commentaries *230; LaFave, supra note 30, § 8.2, at 795. This was a narrow offense, designed more to prevent breaches of the peace than to protect private property from misappropriation. If the wrongdoer did not first commit a trespass to take the property, or if the wrongdoer did not physically move the property after taking it, no larceny could occur. In response to these limitations, the English Parliament created the crimes of embezzlement and false pretenses. See LaFave, supra note 30, § 8.1(b). Embezzlement generally prohibits the fraudulent conversion of the property of another by one who is already in possession of it. The conversion of property requires an interference with the owner's rights so substantial that it effectively deprives the owner of the benefit or value of the property. See Restatement (Second) of Torts § 222A (1965). The crime of false pretenses is known today as fraud; it prohibits the intentionally false representation of a material fact with intent to defraud, which causes the victim to pass title to his property to the wrongdoer. See LaFave, supra note 30, § 8.7, at 828. R R R R

[43] See, e.g., Model Penal Code § 223.1 note (1962).

[44] See Sara Sun Beale, The Unintended Consequences of Enhancing Gun Penalties: Shooting Down the Commerce Clause and Arming Federal Prosecutors, 51 Duke L.J. 1641, 1644-46 (2002) (discussing traditional limits on scope of federal criminal jurisdiction, as well as challenges posed by recent efforts to federalize gun offenses). For example, one statute prohibits larceny on federally owned land. 18 U.S.C. § 661 (2000). Another statute makes it a crime to "embezzle[ ], steal[ ], purloin[ ], or knowingly convert[ ] . . . any record, voucher, money, or thing of value" that belongs to the federal government. 18 U.S.C. § 641.

[45] 18 U.S.C. § 1341 (mail fraud); 18 U.S.C. § 1343 (wire fraud).

[46] The wire fraud statute reads in relevant part:

> Whoever, 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

Efforts to prosecute computer misuse as theft crimes followed a fairly simple rationale. By upsetting intended privileges relating to a computer, the thinking went, the defendant committed a theft—the taking of property belonging to another.[47] This rationale may seem plausible at first blush, but it creates serious difficulties defining a property interest and then identifying when that property has been taken. Theft statutes presume the existence of an identifiable piece of property, some clearly-defined "thing," that when taken deprives the owner of its bounty.[48] We can understand this easily in the case of tangible property. For example, if someone steals my bicycle, it is easy to identify the property stolen (the bicycle) and to tell whether or not I have been deprived of it (either I have the bicycle or I don't). The same principle can work in the intangible world, depending upon the circumstances. If I own a power station and someone taps into my power line without my permission and saps electricity, the crime of theft fits easily.[49] Although intangible, the property readily can be identified—the charged electrons that make up the electricity—and the sapping of the electricity from my power line clearly deprives me of it.[50]

---

executing such scheme or artifice, shall be fined under this title or imprisoned not more than five years, or both.

18 U.S.C. § 1343. The mail fraud statute is quite similar, except that it prohibits a scheme that involves "plac[ing] in any post office or authorized depository for mail matter, any matter or thing whatever to be sent or delivered by the Postal Service." 18 U.S.C. § 1341. The courts have construed these statutes quite broadly. See, e.g., Carpenter v. United States, 484 U.S. 19, 27-28 (1987) (holding use of prepublication confidential information by *Wall Street Journal* reporters within reach of mail and wire fraud statutes).

[47] See infra notes 56-62 and accompanying text. **R**

[48] See Orin S. Kerr, Note, The Limits of Computer Conversion: *United States v. Collins*, 9 Harv. J.L. & Tech. 205, 209 (1996) ("When the facts happen to supply a distinctly defined res, then the doctrine [of conversion] works admirably.").

[49] Some states have statutes that criminalize tampering with electricity meters. See, e.g., Fla. Stat. Ann. § 812.14 (West 2003). Tampering then can lead to prosecutions for theft of electricity, although such prosecutions appear to be fairly rare. See, e.g., State v. Rousten, 146 A. 870 (N.H. 1929).

[50] As one court has stated in the course of analyzing New York's larceny statute in a meter tampering case:

> The cases and annotations, in holding that electricity may be the subject of larceny, are necessarily holding that it is property subject to asportation, and in most of the cases the asportation occurs by means of a diversion of the current or water from the meter which measures the flow from supplier to consumer. . . . Clearly, then, the meter tamperer who, by such tampering, has received electric current without payment has "taken" or "obtained" an "article of value" under circumstances amounting to a "deprivation" in that "the major portion" of the "economic value" of this "property" is lost to the owner. It follows without any possibility of doubt that where the meter tamperer receives for himself the diverted electricity he has thereby committed larceny . . . .

People v. McLaughlin, 402 N.Y.S.2d 137, 140-41 (N.Y. Crim. Ct. 1978).

In the case of computer misuse, however, identifying a property interest and then concluding that it was taken can require considerable creativity. Identifying a property interest proves the easy part, as the body of cases applying theft law to computer misuse illustrates. Although courts declined to find property interests in computer use in a few early cases,[51] later decisions reasoned that nearly all aspects of computers had potential economic value, so it was plausible to consider them "property" for purposes of criminal laws prohibiting theft. Courts held that the mere use of a computer was property,[52] that the data viewed when using a computer also constituted property,[53] that the data stored in a computer counted as property,[54] and even that the password that controlled access to a computer account was property.[55]

Having identified a property interest, however, the courts then struggled to explain how computer misuse actually deprived someone of that property. While this step is not problematic in a case in which misuse *denies* privileges to others, as in the case of a denial-of-service attack, all of the early cases involved defendants who exceeded their privileges. *United States v. Seidlitz* provides a helpful example. In that case, a former employee of a military contractor used a stolen password to log on to the company's network and download valuable software. The Fourth Circuit had little problem concluding that the software obtained was property.[56] However, Seidlitz's conduct did not actually deprive the military contractor of its copy of the software; Seidlitz merely copied the software and left the prior copy in its original condition.[57] This might have harmed the military contractor's

51 See Ward v. Superior Court, 3 Computer L. Serv. Rep. (Callaghan) 206, 208 (Cal. App. Dep't Super. Ct. 1972) (holding computer "impulses" intangible and so not within scope of statute); Lund v. Commonwealth, 232 S.E.2d 745, 748 (Va. 1977) (concluding that "the unauthorized *use* of the computer is not the subject of larceny"); see also United States v. Brown, 925 F.2d 1301, 1307-08 (10th Cir. 1991) (concluding intangible computer data is not "property" under federal statute prohibiting interstate transportation of stolen property).

52 E.g., United States v. Collins, 56 F.3d 1416, 1420 (D.C. Cir. 1995) (holding that federal conversion statute "prohibits the conversion of computer time and storage").

53 E.g., United States v. Seidlitz, 589 F.2d 152, 160 (4th Cir. 1978) (concluding that information viewed from inside computer is "property" under federal wire fraud statute).

54 E.g., United States v. Girard, 601 F.2d 69, 71 (2d Cir. 1979) (concluding that "computerized records" in government computer are property).

55 E.g., People v. Johnson, 560 N.Y.S.2d 238, 241, 243-44 (N.Y. Crim. Ct. 1990) (holding that knowledge of stolen AT&T calling card numbers makes defendant guilty of possession of stolen property).

56 *Seidlitz*, 589 F.2d at 160.

57 Accord Olivenbaum, supra note 10, at 578 ("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.'"). R

financial interests, but it was unclear how it deprived the company of its property, and therefore unclear how it could be a theft.

Faced with such riddles, courts tended to reach results-oriented outcomes. When computer misuse caused harm to a victim in some way, courts generally concluded that property had in fact been taken and held the defendants liable. When no appreciable harm resulted, courts tended to find that no property was taken and hold that the defendants had committed no crime. To the extent that it was made explicit, the reasoning seemed to go something like this: When a person is harmed, the person loses something of value; when a person loses something of value, they are deprived of property. Therefore the infliction of harm triggers a theft. This reasoning allowed courts to reach reasonable results in particular cases, but followed no deeper principle than the courts' ex post assessments of whether particular instances of computer misuse had caused substantial harm.

This dynamic explains the computer misuse cases involving government employees who abused their rights in government computers. For example, in *United States v. Czubinski*,[58] an Internal Revenue Service (IRS) employee used an IRS computer to view the tax returns of social acquaintances, political enemies, and government officials. In *State v. McGraw*,[59] an Indianapolis city employee used the city's computer network to run his own personal sales business. In *United States v. Girard*,[60] a corrupt Drug Enforcement Administration (DEA) agent used the DEA's computer to access and download files identifying undercover DEA agents, planning later to sell the information to drug dealers. Finally, in *United States v. Collins*,[61] an employee of the Defense Intelligence Agency used a highly classified government computer to store hundreds of personal documents about his interest in ballroom dancing. In all of these cases, government employees with rights to use government computers for official reasons instead used them for personal reasons. The courts in these cases identified, or merely assumed, a property interest in that use.[62]

But did these personal uses deprive the government of its property interest?[63] The answer tended to depend on whether the personal use harmed the government in any substantial way. Compare

[58] 106 F.3d 1069 (1st Cir. 1997).

[59] 480 N.E.2d 552 (Ind. 1985).

[60] 601 F.2d 69 (2d Cir. 1979).

[61] 56 F.3d 1416 (D.C. Cir. 1995) (per curiam).

[62] The courts identified a property interest in *Collins*, 56 F.3d at 1419, and *Girard*, 601 F.2d at 71, and assumed a property interest in *Czubinski*, 106 F.3d at 1074, and *McGraw*, 480 N.E.2d at 554.

[63] Notably, such facts also raise the possibility of criminal prosecutions for doing personal work on government time, which in some cases can be prosecuted under statutes that

Girard and *Collins*, two prosecutions for theft or conversion of government property in violation of 18 U.S.C. § 641.[64] In *Girard*, the corrupt DEA agent had used the DEA's computer for a personal use that risked major harm to the DEA: By identifying undercover agents and selling the information to drug dealers, the agent had at best thwarted DEA investigations and at worst risked the lives of DEA undercover agents. In a conclusory fashion, the Second Circuit announced that the defendant had converted the government's property.[65] In *Collins*, however, the defendant had used a classified computer to store ballroom dancing materials. While this violated workplace regulations, it did not appear to cause any particular harm to the government. The D.C. Circuit concluded that this misuse did not violate § 641, on the ground that it "in no way seriously interfered with the government's ownership rights"[66] in the computer system.

The same dynamic surfaces in *Czubinski* and *Seidlitz*, both decided under the federal wire fraud statute.[67] In *Seidlitz*, a former employee used a stolen password to download a valuable proprietary program that he planned to use in his own business.[68] The harm to the company was clear: The program was the company's primary source of competitive advantage, and the employee apparently wanted to obtain the program to further his competing business. After concluding that the program was property, the Fourth Circuit

govern theft of honest services. See, e.g., 18 U.S.C. § 1346 (2000). Such charges were brought in *Czubinski*, 106 F.3d at 1076-77, but not in the remaining cases.

64 18 U.S.C. § 641 punishes "[w]hoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof . . . ."

65 See *Girard*, 601 F.2d at 71 ("[W]e are satisfied . . . that the Government has a property interest in certain of its private records which it may protect by statute as a thing of value.").

66 *Collins*, 56 F.3d at 1421. The court wrote in full:

> [T]he government did not provide a shred of evidence in the case at bar that appellant seriously interfered with the government's ownership rights in its computer system. While appellant concedes he typed in data and stored information on the computer regarding his personal activities, no evidence exists that such conduct prevented him or others from performing their official duties on the computer. The government did not even attempt to show that appellant's use of the computer prevented agency personnel from accessing the computer or storing information. Thus, appellant's use of the government computer in no way seriously interfered with the government's ownership rights.

Id.; accord *McGraw*, 480 N.E.2d at 554 (finding "no evidence that the City was ever deprived of any part of the value or use of the computer" as required by theft statute).

67 18 U.S.C. § 1343.

68 See United States v. Seidlitz, 589 F.2d 152, 155 (4th Cir. 1978).

announced in a conclusory fashion that the defendant was guilty of wire fraud.[69]

In *Czubinski*, by contrast, the First Circuit reversed the conviction of an IRS employee who had browsed IRS records for personal reasons. Czubinski had merely browsed through the IRS database to satisfy his curiosity, which neither directly harmed the IRS nor furthered an unauthorized scheme. The First Circuit concluded: "[T]o 'deprive' a person of their intangible property interest, . . . either some articulable harm must befall the holder of the information as a result of the defendant's activities, or some gainful use must be intended by the person accessing the information . . . ."[70] Applying this test, the court concluded that Czubinski had not deprived the government of any property.[71]

In each of these cases, the courts punished computer misuse that resulted in appreciable harm, but reversed the convictions when it did not. The decisions may have a rough appeal. However, the courts achieved the results through an unpredictable legal fiction that provided little ex ante guidance. The crime of theft was transformed into the law of harm, and liability depended on ex post assessments of whether the computer misuse caused enough of a harm to be considered theft.

D. The Movement for Computer Crime Legislation

The uncomfortable fit between computer misuse and traditional property crimes triggered a great deal of commentary in the late 1970s and early 1980s about the need for computer crime legislation.[72] While some scholars maintained that it made little sense to have com-

---

[69] See id. at 160.

[70] United States v. Czubinski, 106 F.3d 1069, 1074 (1st Cir. 1997).

[71] Id. at 1076 ("Curiosity on the part of an IRS officer may lead to dismissal, but curiosity alone will not sustain a finding of participation in a felonious criminal scheme to deprive the IRS of its property.").

[72] See, e.g., Bequai, supra note 27 (arguing that legal system was unequipped to deal with computer crime); Parker, supra note 27 (presenting case studies as warning of ways computers may be abused); Parker, supra note 19 (arguing computer crimes can be divided into cases in which computers are used as object, subject, instrument, and symbol); Stanley L. Sokolik, Computer Crime—The Need for Deterrent Legislation, 2 Computer/L.J. 353 (1980) (analyzing computer crime as sociological phenomenon and providing potential legislative solutions). About thirty to forty law review articles and student notes appeared from the mid-1970s through the mid-1980s about the need for (and later, the introduction of) computer crime statutes. A good cross-section of articles can be found in the Spring and Summer 1980 issues of the Computer/Law Journal, which were dedicated solely to articles on various aspects of computer crime law.

puter-specific crimes,[73] others argued that the law of theft had proved itself poorly equipped to deal with the new kinds of computer crime.[74]

Several critics of the property-based regime drew attention to the fact that, in applying theft laws to computers, courts focused not on the misuse itself, but rather on its consequences. Donn Parker, a leading proponent of computer crime laws, argued that new laws were needed because "[s]pecific laws will avoid the legal fictions of having to use other criminal statutes that were not meant to apply to computer crime, [so that] criminals can be convicted directly for their explicit acts."[75] State prosecutor Donald Ingraham reasoned that separate computer crime laws made sense for the same reason that legislatures had burglary laws in addition to laws against theft.[76] Burglary laws punish the entering of a building with intent to commit a crime inside. Ingraham reasoned that the argument against computer crime laws could be likened to the suggestion that legislatures repeal their burglary and trespass laws and instead prosecute every invasion of property rights as a theft or attempted theft:

> For example, attempted commercial burglary could be regarded as a usurpation of store floor space, and treated as a theft of the property interest in occupancy. Under such a statute, the victim would necessarily be compelled to calculate the value of the property invaded and the duration of the invasion. The prosecution would be for the theft of those values, and not for the intrusion as a crime complete in itself. It is precisely that absurdity—the requirement that the victim prepare evidence of an injury other than that with

---

[73] Indeed, this remains a theme of current scholarship in the area of computer crime. See Brenner, supra note 10, at ¶¶ 11-12, 119-120, 129; Olivenbaum, supra note 10, at 575-76, 590-91 (arguing that Congress should not have enacted computer crime statute). My own view is that those who endorse this criticism give too much significance to the conceptual similarities between computer misuse crimes and traditional crimes. The fact that we see similarities between trespass and computer hacking does not mean that we should use the former to punish the latter. Rather, at most, it suggests that we might want to use the legal principles that apply to the former to enact a new crime tailored to punish the latter. **R**

We can see the difference clearly by considering Professor Olivenbaum's proposal to repeal the federal unauthorized access statute and simply prosecute unauthorized access under trespass laws. See Olivenbaum, supra note 10, at 638-41. Professor Olivenbaum argues that the similarities between unauthorized access to computers and physical trespass are so clear that we do not need special federal laws governing the former. Id. at 640-41. However, he overlooks a major difficulty: No federal trespass statute exists. See supra note 28. Accordingly, the law that Professor Olivenbaum wishes us to use in lieu of a computer-specific crime would need to be enacted by Congress and then expanded to include computers to satisfy his proposal. **R** **R**

[74] See, e.g., Parker, supra note 19. The journal articles collected in the Spring and Summer 1980 issues of the Computer/Law Journal also generally reflect this view. **R**

[75] Parker, supra note 19, at 244. **R**

[76] See Donald G. Ingraham, On Charging Computer Crime, 2 Computer/L.J. 429, 429-30 (1980).

> which he is really concerned—which the so-called computer crime bills have recognized and sought to redress.[77]

These comments illustrate the difficulties that courts and prosecutors encountered when they applied property crime laws to computer misuse. Although not fully articulated at the time, the harm of misuse was that it interfered with the intended function of computers by either exceeding or denying intended privileges. The intrusion itself seemed worth prohibiting, much like a burglary or a trespass. Traditional property crime laws could address computer misuse only when the misuse triggered a consequential harm, however. As a result, the existing law had no clear remedy for many instances of misuse. Although commentators did not have a specific sense of where the line should be drawn, they tended to agree that misuse alone should be a new trigger of criminal liability.

II
UNAUTHORIZED ACCESS STATUTES AS AN ANSWER TO THE PROBLEM OF COMPUTER MISUSE

Congress and all fifty state legislatures responded to the difficulties of prosecuting computer misuse as a property crime by enacting new computer crime statutes. Florida passed the first state statute in 1978;[78] the final state to enact a statute was Vermont in May 1999.[79] Congress enacted the first federal computer crime law in 1984, broadened it considerably in 1986, and then updated it in various ways in 1990, 1994, 1996, and 2001.[80] While no two statutes are identical, all share the common trigger of "access without authorization" or "unauthorized access" to computers, sometimes in tandem with its close cousin, "exceeding authorized access" to computers.[81] In most cases, the statutes prohibit accessing a computer without authorization or exceeding authorized access as a necessary but not sufficient element of criminal liability, and then create several specific offenses by com-

---

[77] Id.

[78] See Scott, supra note 5, at 763 (referring to Florida Computer Crimes Act, which outlawed computer theft and hacking). R

[79] See Julie A. Tower, Note, Hacking Vermont's Computer Crimes Statute, 25 Vt. L. Rev. 945, 945-48 (2001) (describing origin of, and critiquing Vermont's statutory approach to, computer crime).

[80] For a discussion of the ways in which Congress has changed the statute at each of these intervals, see Scott, supra note 5, at 79-84. R

[81] For a comparison of the various statutes, see Brenner, supra note 5. At the federal level, the phrase "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6) (2000). I discuss the possible difference between the prohibition on access "without authorization" and the prohibition on conduct that "exceeds authorized access," infra text accompanying notes 231-39. R R

bining this base with various additional statutory requirements. In other words, most statutes start with the basic building block of "unauthorized access" to computers, and then add additional elements to the offense to deal with specific types of computer misuse.

The influential federal computer crime statute codified at 18 U.S.C. § 1030 provides a good example. The statute includes seven distinct crimes, listed in § 1030(a)(1) through (a)(7), almost all of which are triggered by "access without authorization" to computers.[82] For example, one crime prohibits unauthorized access to government computers,[83] another prohibits unauthorized access to computers that results in damage,[84] and a third prohibits unauthorized access or exceeding authorized access to computers such that the user obtains private information.[85]

But what does the trigger of unauthorized access mean? What exactly do these statutes prohibit? In this Part, I contend that while legislatures often had a basic sense that the new statutes would cover the computer equivalent of traditional trespass or burglary crimes, that sense was overly simplistic—even naïve. The question of what these statutes prohibit turns out to be rich and complex, requiring courts to consider difficult questions about the meanings of access and authorization, questions that legislatures have never recognized, much less resolved. Both "access" and "without authorization" can have a wide range of meanings. Seeking certainty, legislatures ended up enacting new statutes that created almost as many questions as they answered.

The courts that have interpreted "access" and "without authorization" have offered a broad range of interpretations that run the gamut from quite narrow to extraordinarily broad. Precedents remain sparse; only a handful of cases have interpreted "access," and only a

---

[82] The sole exceptions are 18 U.S.C. § 1030(a)(5)(a)(i), which prohibits sending a command without authorization that causes damage, and 18 U.S.C. § 1030(a)(7), which prohibits sending a threat to cause damage to a computer.

[83] See 18 U.S.C. § 1030(a)(3), amended by Pub. L. No. 104-294, § 201(1)(c), 101 Stat. 3492, which punishes whoever

> intentionally, *without authorization* to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States.

Id. (emphasis added).

[84] See 18 U.S.C. § 1030(a)(5), which punishes whoever "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage" equal in aggregate to at least $5000.

[85] See 18 U.S.C. § 1030(a)(2).

handful of cases have interpreted "without authorization."[86] But even the few available decisions reflect a diverse range of possible approaches. Most importantly, several recent decisions point toward remarkably expansive interpretations of unauthorized access. These decisions threaten to criminalize a great deal of innocuous activity online, potentially transforming routine Internet usage into an activity that (at least based on the law on the books)[87] risks serious criminal liability.

As the following analysis will show, the conceptual foundation of unauthorized access statutes remains remarkably unclear. And without a clear foundation, the statutes may inadvertently end up prohibiting far more conduct than the legislatures intended or common sense would support.

A. The Hidden Complexities of Unauthorized Access

It is impossible to crawl into the minds of legislators and know what they had in mind when they enacted unauthorized access computer crime statutes. Still, the available evidence suggests that legislators mostly saw such statutes as doing for computers what trespass and burglary laws did for real property. For example, the House Report on the first federal computer crime legislation passed in 1984 noted that "section 1030 deals with an 'unauthorized access' concept of computer fraud rather than the mere use of a computer. Thus, the conduct prohibited is analogous to that of 'breaking and entering' rather than using a computer (similar to the use of a gun) in committing the offense."[88] Several state statutes incorporated this concept into the titles of their computer crime statutes, labeling the new unauthorized

[86] This is largely because of the small number of successful cybercrime investigations, and the high likelihood that defendants who are charged will plead guilty and waive their rights to appeal. At the federal level, for example, the government obtains convictions for unauthorized access to computers in about sixty cases every year. See Bureau of Justice Statistics, U.S. Dep't of Justice, Federal Judicial Statistics Resource Center, at http://fjsrc.urban.org/. States also bring prosecutions under their own statutes, although no systematic efforts have been made to count the number of state prosecutions and convictions brought under unauthorized access statutes. Finally, civil cases are responsible for a number of precedents interpreting unauthorized access statutes. See infra notes 122-25, 130-34, 157-63, 185-97, 199-205 and accompanying text. R R

[87] The caveat "on the books" is important because broad judicial interpretations of unauthorized access statutes would not necessarily lead to criminal prosecutions based on those broad interpretations. Federal and state prosecutors are unlikely to bring prosecutions for obviously harmless activity, even if that activity technically may constitute unauthorized access to computers. However, broad judicial interpretations would at least make such prosecutions possible, turning them into questions of discretion for the executive branch.

[88] H.R. Rep. No. 98-894, at 20 (1984), reprinted in 1984 U.S.C.C.A.N. 3689, 3706.

access crimes as crimes of "Computer Trespass."[89] The legislative histories of computer crime laws also regularly refer to the activity prohibited by unauthorized access statutes as computer trespasses[90] or "breaking into computer systems."[91] Courts have also noted the similarities approvingly.[92] As I noted earlier,[93] traditional doctrines such as trespass and burglary form a natural conceptual point of departure for computer misuse statutes: It is understandable that legislatures would see these new unauthorized access statutes as effectively prohibiting trespasses onto computers.

But does this translation from physical world trespass to computer trespass make sense? In the physical world, the crime of trespass provides a reasonably certain line between free acts and criminal conduct. Consider the Model Penal Code's trespass statute. This model trespass statute states in part that:

---

[89] See, e.g., Ark. Code Ann. § 5-41-104 (Michie 1997); Ga. Code Ann. § 16-9-93(b) (Harrison 1993); N.Y. Penal Law § 156.10 (McKinney 2000); Va. Code Ann. § 18.2-152.4 (Michie 1996 & Supp. 2003); Wash. Rev. Code Ann. § 9A.52.110 (West 2000).

[90] See S. Rep. No. 104-357, at 11 (1996) (noting that "section 1030(a)(5) criminalizes all *computer trespass*, as well as intentional damage by insiders, albeit at different levels of severity" (emphasis added)); S. Rep. No. 99-432, at 9 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2487 ("In intentionally *trespassing* into someone else's computer files, the offender obtains at the very least information as to how to break into that computer system. If that is all he obtains, the offense should properly be treated as a simple trespass. But because the offender has obtained the small bit of information needed to get into the computer system, the danger exists that his and every other *computer trespass* could be treated as a theft, punishable as a felony under this subsection." (emphasis added)).

[91] The Maryland Supreme Court has commented on that state's computer crime laws:

> Proponents of this bill testified that, under current law, simply breaking into a computer system to vandalize or cause other mischief is not illegal. Thus, the bill was introduced by those who feel unauthorized access alone should be a misdemeanor subject to penalties. . . . This legislation is intended to make it a misdemeanor for a person intentionally and without authorization to access, attempt to access or cause access to a computer system. The purpose of the bill is to deter individuals from *breaking into computer systems*.

Briggs v. State, 704 A.2d 904, 911 (Md. 1998) (emphasis added) (citation to Maryland legislative history omitted).

[92] See, e.g., State v. Olson, 735 P.2d 1362, 1364 (Wash. Ct. App. 1987). Commenting on the Washington computer trespass statute, the court wrote:

> Historically, a trespass was an intrusion or invasion into tangible property which interfered with the right of exclusive possession. In the context of computers, a trespass is an invasion or intrusion upon the data base. The general trespass statutes criminalize the entering and remaining upon premises when not licensed, invited, or privileged to enter or remain. By analogy, the computer trespass statute criminalizes the entry into the computer base . . . .

Id. (citation omitted); see also State v. McGraw, 480 N.E.2d 552, 554 (Ind. 1986) ("Under traditional concepts, the transgression is in the nature of a trespass, a civil matter—and a de minimis one, at that.").

[93] See supra notes 27-40 and accompanying text. **R**

> A person commits an offense if, knowing that he is not licensed or privileged to do so, he enters or remains in any place as to which notice against trespass is given by: (a) actual communication to the actor; or (b) posting in a manner prescribed by law or reasonably likely to come to the attention of intruders; or (c) fencing or other enclosure manifestly designed to exclude intruders.[94]

The scope of this statute is relatively clear. First, the actus reus is entering or remaining on real property. In the physical world, this has fairly certain meaning: People ordinarily know when they are entering or remaining on property because they can see the property around them. Second, the attendant circumstances of this act are also clear. For the act of entering or remaining in any place to be unlawful, the trespasser must know that his act is without license or privilege, and notice of this must either be directly communicated to the trespasser, or be reasonably likely to be seen by him.[95] While there may of course be factual questions as to when notice was communicated or likely to be seen by the trespasser,[96] or who had authority to give effective notice,[97] the basic framework of the legal test appears easy to understand.

These certainties evaporate when we apply the same concepts to the Internet. Granted, the basic framework is similar. Trespass statutes prohibit entering property without license or privilege; computer crime statutes prohibit accessing a computer without authorization. But at this point the similarities cease.

1. Access

Consider the actus reus of the computer crime statutes, "accessing a computer." What does it mean to "access" a computer? Obviously a computer user does not access a computer by physically getting inside the computer. Some other principle must govern. But what principle should that be? One approach would look at computers from the standpoint of virtual reality, and try to draw analogies between using a computer and entering real property.[98] We could say

---

[94] Model Penal Code § 221.2(2) (1962).

[95] See id.

[96] See, e.g., State v. Dupuy, 395 A.2d 851, 853-54 (N.H. 1978) (rejecting claim of insufficient notice by demonstrator at nuclear facility who claimed that she was using bathroom when notice was broadcast).

[97] See, e.g., State v. Finley, 982 P.2d 681, 687 (Wash. Ct. App. 1999) (concluding that bartender had authority to give notice to disruptive customer for purposes of Washington criminal trespass statute).

[98] I have called this approach the "internal perspective" of the Internet. See Orin S. Kerr, The Problem of Perspective in Internet Law, 91 Geo. L.J. 357, 357 (2003). The internal perspective approaches the Internet from the standpoint of virtual reality, and

that access hinges on whether the user has made a virtual entrance into the computer. For example, imagine a user tries to use a password-protected computer network and is confronted by a screen that requires a valid username and password to proceed. We might say that this screen is akin to a lock on a front door, and that entering a username and password is like using a key to open the lock.[99] This approach suggests that a user who enters a valid username and password has accessed the computer, but a user who inputs an incorrect name or password has been denied access.

Similarly, we could say that visiting a publicly accessible website is something like visiting an open store in the physical world. Determining whether access has occurred then depends on whether visiting an open store can be deemed "entering" in the physical world. The correct answer is not obvious: Visiting a website could be seen as equivalent to viewing a shop window from a public street rather than actually entering the store. But at a conceptual level, the analogy to virtual space provides one heuristic to understand what it means to "access" a computer.

The virtual analogy does not provide the only tool, however. We can also look at the question of access from the standpoint of physical reality, in which we recognize that computers are simply machines that communicate with each other by sending and receiving information.[100] For example, when a user visits a website, the user's computer sends requests to the computer that hosts the website asking the computer to send back computer files; when the files are returned to the user, the user's computer reassembles the files and presents them in the form of a website.[101] If we focus on how computers operate, we can interpret access by looking to whether a user has sent *communications* that have physically entered the computer. For example, one standard could be that a user accesses a computer when she sends a command to that computer instructing the computer to perform a task, and the computer performs the request as instructed.[102] Another

attempts to apply legal concepts to computers and the Internet by applying the law to that virtual reality. See id.

[99] See Trulock v. Freeh, 275 F.3d 391, 409 (4th Cir. 2001) ("Once password protection attaches to a computer file, that protection is the electronic equivalent of the lock on a footlocker containing items that are intended to remain private.").

[100] I have labeled this the "external perspective" of the Internet. See Kerr, supra note 98, at 357. The external perspective sees the Internet as merely a network of connected computers that send and receive information using zeros and ones rather than a "virtual reality." The external perspective thus models Internet events based on the electronic transactions that go on "behind the scenes," largely unknown to the casual user. See id. R

[101] See Preston Gralla, How the Internet Works 128-29 (2002).

[102] This appears to be the standard adopted (at least implicitly) in *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991), discussed infra notes 135-56 and accompanying text. R

standard could be that a user accesses a computer when the user sends a command requesting information in return and the computer responds by sending back information to the user.[103] In this sense, accessing a computer is no different from simply using a computer.

Notably, physical-world standards and virtual-world standards can produce different outcomes. Imagine a user wishes to log on to a password-protected computer, and sends a request to the computer asking it to send back the page that prompts the user to enter a username and password. The computer complies, sending the page back to the user. This would not access the computer from a virtual perspective, as it would be something like walking up to a locked door but not yet trying the key. From a physical-world perspective, however, the request would be an access; the user sent a command to the computer and received the desired response. Similarly, consider whether sending an e-mail accesses the computers of the recipient's Internet service provider. From a virtual perspective, the answer would seem to be no; a user who sends an e-mail to the ISP does not understand herself to have "entered" the ISP. From a physical perspective, however, the answer seems to be yes; the user has in fact sent a communication to the ISP that its servers received and processed.[104]

Which standard governs? The statutes themselves offer little guidance. Most computer crime statutes (including the federal statute) do not define access, and most statutes that do include a definition shed little light on these questions.[105] In the handful of cases that have interpreted the meaning of access, however, courts have at one point or another suggested every one of these possible interpretations of access.[106]

---

103 This appears to be the standard adopted in *State v. Riley*, 846 P.2d 1365 (Wash. 1993) (en banc), discussed infra notes 126-29 and accompanying text. R

104 See Gralla, supra note 101, at 81. R

105 Roughly half of the state unauthorized access statutes define "access." See, e.g., Kan. Stat. Ann. § 21-3755(a)(1) (1971 & Supp. 2003); Wash. Rev. Code Ann. § 9A.52.010(6) (West 2000). Many of them (especially the earlier statutes) use the definition of "access" contained in the first proposal to enact federal computer crime legislation, Senator Ribicoff's influential 1977 bill proposing a "Federal Computer Systems Protection Act." The bill stated that "access means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of, a computer, computer system, or computer network." S. 1766, 95th Cong. (1977); see also Michael M. Krieger, Current and Proposed Computer Crime Legislation, 2 Computer/L.J. 721, 723 (1980) (compiling legislation). The Justice Department criticized this definition, in part on the ground that "approach" is a physical concept and appears to include being close to a computer. See Donn B. Parker, Nat'l Inst. of Justice, Computer Crime: Criminal Justice Resource Manual 84 (2d ed. 1989). As we will see, courts have a mixed record applying state definitions based on the Ribicoff language. See infra Part II.B.

106 See infra Part II.B.

2. *Authorization*

Even greater ambiguities surface when we consider what it means for access to be without authorization. The concept of authorization seems clear in the case of traditional trespass statutes, which presume that people have a right to be where they are, and often require posted notice in that place instructing them that they cannot enter or remain there.[107] The statutes also require that the trespasser knows that she is without license or privilege to enter or remain on the premises.[108] The relevant authorization relates solely to physical presence in that location, and can be evaluated readily because most people understand the social norms that govern whether someone has permission to be present on another person's property. Everyone knows that a tall fence with an orange "No Trespassing" sign means to stay out.

The concept of authorization to access a computer is more difficult, as the following example shows. Imagine that a college student tasked with writing a research paper on the Ku Klux Klan decides to conduct her research using the Internet. She logs on to her AOL account, which is governed by a Terms of Service agreement containing the following clause: "You may not use your AOL account to post, transmit, or promote any unlawful, harmful, threatening, abusive, harassing, defamatory, vulgar, hateful, racially, ethnically or otherwise objectionable content."[109] Once connected to the Internet, she

---

[107] See supra notes 94-97 and accompanying text. R

[108] See supra notes 94-97 and accompanying text. R

[109] Am. Online, Agreement to Rules of User Conduct, at http://www.aol.com/copyright/rules.html (last visited Sept. 30, 2003) [hereinafter AOL Terms of Service]. America Online's Rules of User Conduct, which bind all of AOL's thirty million members, require members to agree that they will not:

> [u]pload, post, or otherwise distribute or facilitate distribution of any content—including text, communications, software, images, sounds, data, or other information—that:
>
> 1. is unlawful, threatening, abusive, harassing, defamatory, libelous, deceptive, fraudulent, invasive of another's privacy, tortious, contains explicit or graphic descriptions or accounts of sexual acts (including but not limited to sexual language of a violent or threatening nature directed at another individual or group of individuals), uses vulgar language in the creation of a Screen Name (AIM) or otherwise violates America Online's rules or policies or these Rules of User Conduct;
>
> 2. victimizes, harasses, degrades, or intimidates an individual or group of individuals on the basis of religion, gender, sexual orientation, race, ethnicity, age, or disability;
>
> 3. infringes on any patent, trademark, trade secret, copyright, right of publicity, or other proprietary right of any party;
>
> 4. constitutes unauthorized or unsolicited advertising, junk or bulk e-mail (also known as "Spamming"), chain letters, any other form of unauthorized solicitation, or any form of lottery or gambling;

finds a web site hosted by a KKK chapter. The main page contains a click-through agreement: "Only white supremacists are authorized to access this site," the agreement states. "Access by people who are not white supremacists is unauthorized. By clicking 'I agree,' you agree that you are a white supremacist." Although she is not a white supremacist, she clicks "I Agree" and examines the site. The site contains links to other Klan-related sites, and when she clicks on one of the links, she is connected to a university-hosted site about the history of the Klan that asks her to enter a username and password. Although she does not have an account with the university, she guesses a username and password correctly, and the site grants her access to its contents. She then copies some of the information contained in the site, and e-mails it to her best friend, who previously has told her to stop e-mailing her information about her KKK research project.

Assuming that our student has "accessed" all four of the computers used in this example, which of these acts of access were "without authorization?" Did the student access AOL's computers without authorization because she used AOL to "transmit . . . hateful . . . or otherwise objectionable content" in violation of AOL's Terms of Service? Did she access the Klan's computers without authorization because she was not a white supremacist? Did she access the university's computer without authorization by guessing the username and password, entering disguised as a legitimate user? Finally, did she access her friend's computer without authorization by sending her friend the e-mail after her friend had told her not to send it?

More broadly, who and what determines whether access is authorized, and under what circumstances? Can a computer owner set the scope of authorization by contractual language? Or do these standards derive from the social norms of Internet users? The statutes

---

> 5. contains software viruses or any other computer code, files, or programs that are designed or intended to disrupt, damage, or limit the functioning of any software, hardware, or telecommunications equipment or to damage or obtain unauthorized access to any data or other information of any third party; or
>
> 6. impersonates any person or entity, including any employee or representative of America Online.
>
> [Members] further agree that [they] will not knowingly solicit or collect personal information from a minor (anyone under 18 yrs old). Personal information includes but is not limited to name, address, phone number or name of their school.

Id.

are silent on these questions: The phrase "without authorization" generally is left undefined.[110]

B. Judicial Interpretations of Access

Only a handful of judicial decisions interpret what it means to access a computer, or when that access is without authorization. Even the few cases reflect the broad range of available interpretations. This Section explores the cases that have offered interpretations of "access," and the next Section considers the cases explaining "authorization."

Perhaps the most comprehensive discussion of "access" appears in a Kansas Supreme Court case from 1996, *State v. Allen*.[111] Allen had used his computer repeatedly to dial up a Southwestern Bell Telephone computer that controlled long-distance telephone switches and could be manipulated to allow a user to place free long-distance calls.[112] When Allen dialed up the Bell computers, he was confronted with a prompt requiring him to enter a username and password. Investigators speculated that Allen had guessed a password correctly and later erased the proof of his activity by deleting the logs. However, the forensic evidence established only that Allen had repeatedly dialed up the Bell computers and viewed the password prompt.[113]

---

[110] One exception is Michigan's computer crime statute. Michigan's law creates a rebuttable presumption that a defendant did not have authorization unless one or more of the following is satisfied:

> (a) Written or oral permission was granted by the owner, system operator, or other person who has authority from the owner or system operator to grant permission of the accessed computer program, computer, computer system, or computer network.
>
> (b) The accessed computer program, computer, computer system, or computer network had a pre-programmed access procedure that would display a bulletin, command, or other message before access was achieved that a reasonable person would believe identified the computer program, computer, computer system, or computer network as within the public domain.
>
> (c) Access was achieved without the use of a set of instructions, code, or computer program that bypasses, defrauds, or otherwise circumvents the pre-programmed access procedure for the computer program, computer, computer system, or computer network.

Mich. Comp. Laws Ann. § 752.797(6) (West 1991 & Supp. 2003). While an interesting approach, the constitutionality of this statute is suspect: The presumed lack of authorization may violate the constitutional presumption of innocence. See, e.g., Sandstrom v. Montana, 442 U.S. 510, 524 (1979) (holding that "presumption which, although not conclusive, had the effect of shifting the burden of persuasion to the defendant," violates Due Process Clause).

[111] 917 P.2d 848 (Kan. 1996).

[112] See id. at 850.

[113] See id.

Allen was charged with accessing the Bell computer without authorization in violation of the Kansas computer crime statute.[114]

Before the Kansas Supreme Court, Allen argued that there was no evidence he had actually accessed the Bell computer. The government relied on the broad statutory definition of access, fairly common among early state computer crime statutes,[115] which stated that access means "to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer."[116] The court responded that this definition was so broad that if taken seriously it would render the statute unconstitutionally vague.[117] If "access" really meant "to approach," the court noted, "any unauthorized physical proximity to a computer could constitute a crime."[118] In light of its overbreadth, the court refused to apply the definition, concluding that "the plain and ordinary meaning should apply rather than a tortured translation of the definition that is provided."[119] The court explained:

> Webster's defines "access" as "freedom or ability to obtain or make use of." This is similar to the construction used by the trial court to find that no evidence showed that Allen had gained access to Southwestern Bell's computers. Until Allen proceeded beyond the initial banner and entered appropriate passwords, he could not be said to have had the ability to make use of Southwestern Bell's computers or obtain anything. Therefore, he cannot be said to have gained access to Southwestern Bell's computer systems as gaining access is commonly understood.[120]

This concept of "access" appears to adopt the virtual reality approach, in which the correct username and password grants a user access to the files "inside" the computer, but the wrong username and password denies the user that access. Absent evidence that Allen had

---

114 Id. at 851. The Kansas statute prohibited "[i]ntentionally and without authorization gaining or attempting to gain access to and damaging, modifying, altering, destroying, copying, disclosing or taking possession of a computer, computer system, computer network or any other property." Id. (quoting Kan. Stat. Ann. § 21-3755(b)(1) (2000)).

115 The language is a slight modification of the influential language from Senator Ribicoff's 1977 proposal discussed supra note 105. R

116 *Allen*, 917 P.2d at 851 (quoting Kan. Stat. Ann. § 21-3755(a)(1)).

117 Id. at 852 ("We read certain conduct as outside a statute's scope rather than as proscribed by the statute if including it within the statute would render the statute unconstitutionally vague.").

118 Id. (citing Parker, supra note 105, at 84). R

119 Id.

120 Id. at 853 (citation omitted).

passed through the password prompt to find the information inside, he had not actually accessed the Bell computer.[121]

A federal district court suggested a similar approach in *Moulton v. VC3*, a civil dispute between two computer security companies.[122] The *Moulton* case harnessed a civil remedy added to the federal computer crime statute in 1994 to provide additional protection for computer misuse victims.[123] One company sued the second when an employee of the second company performed a "port scan" on the first company's computers. A port scan is a common network security test that sends a query to each open port on the target computer to see if that port is open and ready to receive incoming traffic.[124] A port is a sort of electronic door, and an open port is akin to an open door and therefore a possible security vulnerability. When scanned, an open port will return a message to the requesting computer instructing it that it is open; a closed port will return an error message. Consistent with *Allen*, the *Moulton* court concluded without analysis that the second company's port scan did not access the first company's computer.[125]

While both *Moulton* and *Allen* suggest that accessing a computer is limited to uses that in a virtual sense get "inside" the computer, two other opinions have adopted a significantly broader approach. Consider the Washington Supreme Court's decision in *State v. Riley*.[126] The facts of *Riley* closely resemble those of *Allen*. Joseph Riley had configured his computer to dial up the computers of the Northwest Telco Corporation and guess random passwords; a correct password allowed the user to place free long-distance telephone calls.[127] The evidence showed that Riley repeatedly had dialed the Telco access number and guessed passwords, although it was unclear whether he had guessed correctly and placed free calls.

Riley argued on appeal that he had not accessed the Telco computers. The Washington statute contained a definition of "access"

---

121 Notably, however, the court did not discuss whether Allen's conduct constituted an *attempted* access, which might have been prosecuted under attempt laws. The federal unauthorized access statute contains an explicit attempt provision, which states that "[w]hoever attempts to commit an offense under subsection (a) of this section shall be punished." See 18 U.S.C. § 1030(b) (2000). Convictions under Section 1030(b) remain very rare, most likely because of difficulties in proving attempt.

122 No. 1:00CV 434-TWT, 2000 WL 33310901 (N.D. Ga. Nov. 7, 2000).

123 See 18 U.S.C. § 1030(g).

124 See Marshall Brain, How Ports Work, available at http://www.digitalearth.net.cn/readingroom/Webgis/Work%205.htm (last visited Sept. 30, 2003).

125 *Moulton*, 2000 WL 33310901, at *6.

126 846 P.2d 1365 (Wash. 1993) (en banc).

127 See id. at 1367-68.

essentially identical to that in the Kansas statute from *Allen*.[128] In *Riley*, however, the court relied on the statutory definition to conclude that Riley had in fact accessed the Telco computers:

> Riley's repeated attempts to discover access codes by sequentially entering random 6-digit numbers constitute "approach[ing]" or "otherwise mak[ing] use of any resources of a computer." The switch is a computer. Long distance calls are processed through the switch. Riley was approaching the switch each time he entered the general access number, followed by a random 6-digit number representing a customer access code, and a destination number. Therefore, Riley's conduct satisfied the statutory definition of "access" and so was properly treated as computer trespass.[129]

It is possible to interpret the difference between *Allen* and *Riley* as simply the difference between one court that followed a common statutory definition of access and another that did not, or perhaps the difference between proof that a defendant guessed passwords and proof that he merely viewed the logon prompt. I think something else is afoot, however. In *Allen*, the court viewed computers as virtual spaces, and accessing the computer as akin to getting inside the space. Although the *Riley* court does not make its standard clear, it appeared to see computers more as physical machines, and accessing the computer as sending a communication to that machine. As a result, the conduct that did not constitute access in *Allen* did so in *Riley*.

An even broader interpretation of access appears in a civil decision, *America Online v. National Health Care Discount, Inc. (NHCD)*[130] This case is one of several civil cases brought by AOL against spammers, senders of bulk unsolicited commercial e-mail.[131] In this dispute, AOL sued NHCD, a company that sells discount health care plans, for hiring a spammer to send bulk e-mails about NHCD to AOL customers.[132] AOL contended that by harvesting e-mail addresses and sending e-mail to AOL customers in violation of AOL's terms of service, the spammers had accessed AOL's computers without authorization. AOL moved for summary judgment,

---

[128] The Washington statute said that to "access" means "to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, directly or by electronic means." Wash. Rev. Code Ann. § 9A.52.010(6) (West 2003). Note once again that this is a slight variation of the Ribicoff proposal, discussed supra note 105. **R**

[129] *Riley*, 846 P.2d at 1373. In a footnote, the court added (weakly) that "[t]his interpretation of the statute does not criminalize repeated dialing of a busy telephone number because a computer trespass conviction requires an 'intent to commit another crime.' It is not disputed that Riley had such an intent." Id. at 1373 n.5 (citation omitted).

[130] 121 F. Supp. 2d 1255 (N.D. Iowa 2000).

[131] See id. at 1259.

[132] See id. at 1259, 1262.

prompting the court to consider whether a computer user "accesses" another computer when he sends e-mail to that computer. The court answered in the affirmative, offering an expansive interpretation of "access":

> The CFAA does not define "access," but the general definition of the word, as a transitive verb, is to "gain access to." "[A]ccess," in this context, means to exercise the "freedom or ability to . . . make use of" something. . . . For purposes of the CFAA, when someone sends an e-mail message from his or her own computer, and the message then is transmitted through a number of other computers until it reaches its destination, the sender is making use of all of those computers, and is therefore "accessing" them.[133]

Although the *NHCD* court relied on the same dictionary definition of "access" as had the *Allen* court, the court in *NHCD* reached a quite different interpretation of its meaning. To the *NHCD* court, access is a physical world concept, not a virtual world concept: The question is not whether the sender of the communication gains a virtual entrance into the computer from the sender's standpoint, but whether the communication itself is transmitted through the computer. As a result, sending an e-mail through a computer accesses the computer even if a user might not perceive the interaction as an access. Despite the common term, and even common statutory and dictionary definitions, the few courts to have interpreted access have reached inconsistent conclusions.[134]

C. Judicial Interpretations of Authorization

Courts have faced even greater difficulties trying to interpret the meaning of authorization. The cases construing authorization fall into three categories: First, the leading case of *United States v. Morris*;[135] second, cases involving employee use of an employer's computer against the employer's interests; and third, cases involving breaches of contractual relationships between users and computer owners. The three categories reflect increasingly broad constructions of the scope of computer crime statutes.

---

133 Id. at 1272-73 (citations omitted).

134 At least two courts have addressed "access" to a computer in the context of computer telephone networks, also with mixed results. Compare Commonwealth v. Gerulis, 616 A.2d 686, 691 (Pa. Super. Ct. 1992) (concluding that defendant who obtained voice mailbox password had "accessed" computer hosting voice mailbox), with State v. Rowell, 908 P.2d 1379, 1384 (N.M. 1995) (concluding that use of telephone network to place phone call was not "access" under computer crime statute).

135 928 F.2d 504 (2d. Cir. 1991).

1. Morris *and the Intended Function Test*

The earliest significant case interpreting authorization is the Second Circuit's opinion in *United States v. Morris*, sometimes known as the Internet worm case. The *Morris* case introduced the "intended function" test of authorization.[136]

Robert Tappan Morris was a graduate student at Cornell in the late 1980s who authored a computer program known as a "worm" which was designed to exploit several weaknesses in Internet security.[137] Morris hoped that the code would spread across the then-nascent Internet to illustrate four common security flaws: a bug in common e-mail software, SENDMAIL; a bug in an Internet query function known as the "finger daemon";[138] a design flaw that allowed computers to use privileges on one computer to obtain privileges on another; and the use of simple, easy-to-guess passwords.[139] Morris designed the code so that it would try various of these means of infecting its targets, and then once it succeeded it would try other computers. Morris released the worm from a computer at MIT on November 2, 1988, but the worm quickly spread out of control and replicated itself so often that it eventually shut down a good portion of the early Internet.[140] Morris was charged with violating 18 U.S.C. § 1030(a)(5)(A), which at the time prohibited "intentionally access[ing] a Federal interest computer without authorization" if damage resulted.[141] A jury convicted Morris at trial.

On appeal, Morris argued that his computer access was not without authorization because he had rights to access several of the infected computers, including computers at Cornell, Harvard, and Berkeley—schools where Morris apparently held legitimate

---

136 See id. at 510.

137 See id. at 505. As the 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. at 505 n.1.

138 Although the *Morris* court referred to the "finger demon," see id. at 506, the proper term is "daemon," the word used in UNIX to refer to a program that runs by itself, usually in the background. See The New Hacker's Dictionary 141 (Eric S. Raymond ed., 3d ed. 1996).

139 See *Morris*, 928 F.2d at 506.

140 See id.

141 See id. Notably, this reference is to the 1986 version of the statute; it has changed over time.

accounts.[142] Morris based his argument on a distinction between two closely related types of abuse of authorization: access "without authorization" and access that "exceeds authorized access."[143] Some unauthorized access statutes prohibit only access without authorization; others prohibit both access without authorization and access that exceeds authorization.[144] Although courts have struggled to distinguish between these two phrases, prohibitions against exceeding authorization appear to reflect concerns that users with some rights to access a computer network could otherwise use those limited rights as an absolute defense to further computer misuse.[145] For example, an employee could hack her employer's computer and see her employer's secret files, but later claim that her limited rights to use the computer at work granted her authorization to access the computer, so that access by her could not be without authorization.

Morris drew support from a 1986 Senate report authored in support of the 1986 amendments that expanded 18 U.S.C. § 1030 from its original narrow form into the broader statute it remains today. The Senate report had suggested a difference between access without authorization and exceeding authorized access based on the difference between "insiders" and "outsiders." Insiders were those with rights to access computers in some circumstances (such as employees), whereas outsiders had no rights to access computers at all (such as hackers).[146] The report seemed to presume an *Allen*-like understanding of access, in which a user "accessed" a computer by getting inside the computer with a username and password. The report then suggested that in

142 The opinion is not clear on where Morris had preexisting accounts. The opinion merely states that Morris "was authorized to use computers at Cornell, Harvard, and Berkeley." Id. at 509.

143 The federal unauthorized access statute defines "exceed[ing] authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6) (2000).

144 Compare 18 U.S.C. § 1030(a)(3) (prohibiting access "without authorization" to government computer) with 18 U.S.C. § 1030(a)(2)(b) (prohibiting access without authorization or exceeding authorized access to government computer and thereby obtaining information).

145 This distinction has been drawn primarily in congressional reports accompanying amendments to the federal unauthorized access statute, 18 U.S.C. § 1030. See S. Rep. No. 104-357, at 4 (1996) (noting that 18 U.S.C. § 1030(a)(3), which prohibits access without authorization to government computers, "only applies to outsiders who gain unauthorized access to Federal Government computers, and not to Government employees who abuse their computer access privileges to obtain Government information that may be sensitive and confidential"); S. Rep. No. 99-432, at 10 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2488 (making same point with regard to 18 U.S.C. § 1030(a)(5)(A)).

146 See *Morris*, 928 F.2d at 510 (citing S. Rep. No. 99-432, at 10 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2488).

cases in which Congress prohibited accessing a computer without authorization but did not prohibit exceeding authorized access, it intended to prohibit the acts of outsiders but not insiders.[147] Morris reasoned that because he had several legitimate Internet accounts, he was an Internet insider and could not be convicted of accessing Internet computers without authorization.[148]

It is worth noting that there are several complex issues lurking (or at least potentially lurking) within Morris's appeal. The worm spread across the Internet, and the government accused Morris of accessing computers without authorization. This raised important questions of interpreting access; had Morris committed one act of access when he had logged on and sent the worm, for example, or did each replication of the worm constitute a separate access by him? It also raised questions about how to divide a network of computers into individual computers for the purpose of the statute.[149] However, Morris based his appeal solely on the question of authorization.[150] Accepting the government's theory that he had caused the worm to access many different computers, Morris argued only that because he had authorization to access some federal interest computers, he had not accessed any computers entirely without authorization.[151]

The Second Circuit rejected Morris's argument. While statutes that only prohibited access without authorization may have been "aimed"[152] at outsiders, the court reasoned:

> Congress was not drawing a bright line between those who have some access to any federal interest computer and those who have none. Congress contemplated that individuals with access to some federal interest computers would be subject to liability under the computer fraud provisions for gaining unauthorized access to other federal interest computers.[153]

---

147 See id.

148 See id.

149 The problem is that the statute divides the world into distinct "computers" to be accessed, and while the denomination of a computer is familiar to those of us who use laptop and desktop computers on a daily basis, the concept is more fluid in the context of a large network of machines connected together. Consider the case of a computer virus that spreads across a network. How many computers are accessed by the virus? Do you count the number of servers, the number of subnetworks, the number of client computers connected to them, the number of physical boxes, or something else?

150 Morris also argued that the statute requires intent to cause a specific threshold of monetary damage, but the court rejected that argument. See *Morris*, 928 F.2d at 509.

151 Id. at 509-10.

152 Id. at 511 (quoting S. Rep. No. 99-432, at 10 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2488).

153 Id.

The court then introduced and applied a new standard for determining when access was unauthorized: the intended function test. According to the court, Morris had accessed computers without authorization because he had used weaknesses in several programs to obtain access in unintended ways. As the court put it, Morris did not use those programs "in any way related to their intended function."[154] The SENDMAIL program was an e-mail program, and the finger daemon was designed to let users query information about other users. However, Morris "did not send or read mail nor discover information about other users; instead he found holes in both programs that permitted him a special and unauthorized access route into other computers."[155]

Although the court did not elaborate on its standard, the intended function test appears to derive largely from a sense of social norms in the community of computer users. Under these norms, software designers design programs to perform certain tasks,[156] and network providers enable the programs to allow users to perform those tasks. Providers implicitly authorize users to use their computers to perform the intended functions, but implicitly do not authorize users to exploit weaknesses in the programs that allow them to perform unintended functions. When a user exploits weaknesses in a program and uses a function in an unintended way to access a computer, the thinking goes, that access is "without authorization."

2. Employee Misconduct Cases

Several cases have examined the meaning of authorization in the context of employee misconduct. In these cases, employees used their employers' computers in ways that exceeded the scope of their employment without violating the *Morris* intended function test.

Perhaps the most remarkable of these cases is *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*,[157] which introduced an agency theory of authorization. *Shurgard* involved a civil dispute between two business competitors in the self-storage business. According to the complaint, the defendant lured away several of the

---

154 Id. at 510.

155 Id.

156 Notably, this test seems to focus on objective rather than subjective concerns. For example, the SENDMAIL program is an open-source program. See Sendmail Frequently Asked Questions, at http://www.sendmail.org (last updated Sept. 17, 2003). Accordingly, SENDMAIL does not have a particular designer or design team. Rather, the intended function appears to be what the program itself (and its supporting literature) claims that the program does. For a more thorough discussion of open source, see generally Pekka Himanen, The Hacker Ethic and the Spirit of the Information Age (2001).

157 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

plaintiff's employees, including an employee named Eric Leland who had access to the plaintiff's confidential business plan and other trade secrets.[158] Before leaving the plaintiff's company, Leland e-mailed several of the plaintiff's trade secrets and other proprietary information to the defendant. The plaintiff later sued the defendant under 18 U.S.C. § 1030(a)(2)(C), on the theory that Leland had "intentionally access[ed] [the plaintiff's] computer without authorization," or in excess of authorization, and thereby obtained information from the plaintiff's computer in violation of the federal unauthorized access statute.[159] The defendant then moved to dismiss under Federal Rule of Civil Procedure 12(b)(6), on the ground that Leland had not accessed the plaintiff's computers without authorization or in excess of authorization.

The district court disagreed. The court adopted the plaintiff's theory of authorization, which was that "the authorization for its . . . employees ended when the employees began acting as agents for the defendant."[160] The court found its guidance in the Restatement (Second) of Agency: "Unless otherwise agreed, the authority of an agent terminates, if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal."[161] Applying this standard, the court concluded that the defendant's employees "lost their authorization and were 'without authorization' when they allegedly obtained and sent the proprietary information to the defendant via e-mail."[162] In support of its holding, the court turned to the CFAA's legislative history, which the court argued showed a congressional design broadly to prohibit computer misuse, especially where intellectual property rights were at issue.[163] Notably, however, the court did not refer to the 1986 legislative history discussed extensively in *Morris*, did not mention the *Morris* intended function test, and did not explain why agency law standards should govern computer misuse law.

Shurgard's agency theory of authorization is strikingly broad. Under *Shurgard*, whenever an employee uses a computer for reasons contrary to an employer's interest, the employee does not act as the employer's agent and therefore is accessing the employer's computers

158 See id. at 1123.

159 See id. at 1124 (quoting 18 U.S.C. § 1030(a)(2)(C) (2000)).

160 Id.

161 Restatement (Second) of Agency § 112 (1958) (cited in *Shurgard*, 119 F. Supp. 2d at 1125).

162 *Shurgard*, 119 F. Supp. 2d at 1125.

163 See id. at 1127-29. The court relied primarily on general statements that section 1030 was designed to protect computers, as well as to stop misuse that might threaten businesses and intellectual property. See id.

without authorization. Motive determines whether access is authorized or unauthorized. Given that the federal computer crime statute uses access without authorization as the trigger for often-serious criminal liability, the apparent effect of *Shurgard* is to criminalize an employee's use of an employer's computer for anything other than work-related activities.

Courts have adopted slightly narrower interpretations of unauthorized access in criminal employee misconduct cases. Recall the First Circuit's decision in *United States v. Czubinski*,[164] where an IRS employee browsed computerized tax returns of his friends and enemies despite workplace rules that he could only access the database for work-related reasons. *Czubinski* was charged under both property-based statutes and 18 U.S.C. § 1030. Although the court rejected both counts of the indictment against Czubinski for reasons not relevant here, the court noted in passing that Czubinski had "unquestionably exceeded authorized access"[165] to the IRS computer for purposes of section 1030. The comment is dicta, but appears to reflect a watered-down version of *Shurgard*. Like *Shurgard*, this language in *Czubinski* suggests that employers have a right to limit their employees' use of company computers to work solely motivated by a desire to serve the company. Czubinski had exceeded his authorized access by accessing the IRS computers for personal reasons when employees were allowed to access the computer only for official reasons.

A Georgia state court applied a similar standard in *Fugarino v. State*.[166] *Fugarino* involved a computer trespass statute that prohibits use of a computer with knowledge that the use is without authority, and with intent to damage data.[167] Sam Fugarino was a computer programmer whose behavior at work became increasingly bizarre. When Fugarino learned that another employee had been hired at the

---

[164] See supra notes 67-71 and accompanying text. **R**

[165] United States v. Czubinski, 106 F.3d 1069, 1078 (1st Cir. 1997) (citing 18 U.S.C. § 1030(e)(6) (1994)).

[166] 531 S.E.2d 187 (Ga. Ct. App. 2000).

[167] The relevant statute reads:

> Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of: (1) Deleting or in any way removing, either temporarily or permanently, any computer program or data from a computer or computer network; (2) Obstructing, interrupting, or in any way interfering with the use of a computer program or data; or (3) Altering, damaging, or in any way causing the malfunction of a computer, computer network, or computer program, regardless of how long the alteration, damage, or malfunction persists shall be guilty of the crime of computer trespass.

Ga. Code Ann. § 16-9-93(b) (1999).

company, Fugarino became enraged, telling another employee that the company's code was "his product, that no one else was going to work on his code, that nobody was going to take his place and that he was 'going to take his code with him.'"[168] Fugarino then started deleting sections of code from the employer's network.[169] When the employer confronted him, Fugarino told the employer that "the blood of his dead son" was in the code and that the owner "would never get to make any money from that code."[170]

On appeal following his conviction, Fugarino argued that his conduct was not knowingly without authority.[171] The Georgia court disagreed. Fugarino lacked authority because "[t]he owner of the company . . . did not give Fugarino authority or permission to delete portions of the company's program."[172] Further, "the vindictive and retaliatory manner in which Fugarino deleted large amounts of computer code" demonstrated that he knew that he lacked authority to delete the code.[173] Although the precise statutory text differs slightly from the federal statute, the opinion echoes *Shurgard* and *Czubinski*. Fugarino was a computer programmer who presumably had the authority to delete files for work-related reasons. By deleting files to spite his employer, however, Fugarino implicitly ventured beyond the scope of his authority and into the zone of unauthorized use.

State v. Olson[174] reveals a roughly similar approach, albeit one that led to a reversal of the defendant's conviction. Laurence Olson was a police officer who used a police computer database to access and print out driver's license photographs of female college students who attended the nearby University of Washington.[175] Olson was tried and convicted of accessing a government computer without authorization in violation of Washington's computer trespass

168 *Fugarino*, 531 S.E.2d at 188.

169 Id. Fugarino also added password protections to the code to block the employer from accessing the code. Id. However, the court does not seem to have relied on the added passwords in the course of its discussion of authorization, focusing solely on section 16-9-93(b)(1), barring deletion of files, instead of the later subsections relating to interfering with computer use or altering a computer network.

170 Id.

171 Id. at 189. The Georgia statute defined "without authority" as "the use of a computer or computer network in a manner that exceeds any right or permission granted by the owner of the computer or computer network." § 16-9-92(11).

172 *Fugarino*, 531 S.E.2d at 189.

173 Id. Notably, this reflects one of the few times that mens rea was raised as an issue in the context of computer crime statutes. See supra note 7. **R**

174 735 P.2d 1362 (Wash. Ct. App. 1987).

175 See id. at 1363-64 (describing police investigation leading to this conclusion).

statute.[176] On appeal, he argued that his access was not explicitly unauthorized.[177]

The court evaluated Olson's claim by examining the workplace rules that governed Olson's conduct. After reviewing the trial record, the court concluded that while "certain *uses* of retrieved data were against departmental policy, [the record] did not show that permission to *access* the computer was conditioned on the uses made of the data."[178] The court reversed the conviction. The fact that Olson apparently had accessed the computer for personal reasons did not make his access unauthorized, the court reasoned, because only the personal use and not the access itself violated an explicit workplace rule.[179] Once again, this seems to be *Shurgard*-lite: The primary difference between *Olson* and *Shurgard* is that under *Olson* the employer must make the limits on computer access explicit.

The sole employee misconduct case rejecting such an approach to authorization is a Maryland case, *Briggs v. State*.[180] In this case, a court dismissed the conviction of a disgruntled computer system administrator who had password-protected important files on his employer's network using passwords unknown to his employer. Shortly before he resigned, Briggs had placed the password-protected files in a subdirectory named "ha-ha he-he."[181] The password protection left his employer unable to read the files, and when the employer later asked Briggs for the password, Briggs claimed that he had forgotten it. The State charged Briggs with unauthorized access to his employer's computer, reasoning that Briggs was not authorized to access the computer "in such a way as to interrupt the operation of the computer services of the system."[182] The court disagreed, reasoning that as a system administrator, Briggs was in fact authorized to access his employer's computer.[183] While Briggs had done something he was not supposed to do, he did not lack authorization to access the computer (although, the court noted, he might have exceeded his author-

176 Wash. Rev. Code Ann. § 9A.52.110(1) (West 2000) states:
A person is guilty of computer trespass in the first degree if the person, without authorization, intentionally gains access to a computer system or electronic data base of another; and (a) The access is made with the intent to commit another crime; or (b) The violation involves a computer or data base maintained by a government agency.

177 *Olson*, 735 P.2d at 1364.

178 Id. at 1365 (emphasis added).

179 See id. at 1366 (describing evidence as showing "at most, a violation of departmental policy on the use of computer data. [It does] not establish unauthorized access . . . .").

180 704 A.2d 904 (Md. 1998).

181 Id. at 906.

182 Id.

183 Id. at 909.

ized access, something that the Maryland statute did not prohibit).[184] In contrast with *Shurgard*, the *Briggs* court based authorization on conduct rather than motive. The fact that Briggs did not have his employer's interest at heart when he accessed the computer did not make his access without authorization.

3. Contractual Cases

The final and most fascinating set of cases interpreting authorization involves contracts governing the use of computers. In these cases, two parties are bound by a contract that implicitly or explicitly regulates access to a computer, and one side uses the computer in a way that arguably breaches the contract. The question: Does the breach of contract make the access unauthorized? The remarkable answer, at least in civil cases: Yes.

The most important of these cases is the recent decision by the First Circuit in *EF Cultural Travel BV v. Explorica, Inc.*[185] *Explorica* involves another civil dispute between two business competitors—in this case, the well-established student travel business, EF, and an upstart competitor, Explorica. Explorica's vice president, Philip Gormley, was a former vice president at EF who had signed a confidentiality agreement with EF promising not to disclose any of EF's "technical, business, or financial information, the use or disclosure of which might reasonably be construed to be contrary to the interests of EF."[186] When Gormley arrived at Explorica, he decided that Explorica could compete with EF by undercutting EF's prices available from its public website.

Gormley instructed a computer consultant to design an automated "scraper" program that could query EF's website for tour prices and then send the EF price list to Explorica. Each use of the scraper sent 30,000 queries to the EF computer.[187] Explorica used the scraper twice, enough to allow it to learn and then undercut EF's tour prices, all unbeknownst to EF.[188] When EF learned of the scraper program, it sought a preliminary injunction against Explorica's use of the scraper on the ground that (among other things) it violated the federal unauthorized access statute by accessing EF's computers

---

184 See id. at 910 ("The statute makes no reference to authorized users who exceed the scope of their authority. If the Legislature intended the statute to cover employees who exceeded the scope of their authority or who misused their authority, it could have done so explicitly.").

185 274 F.3d 577 (1st Cir. 2001).

186 Id. at 582 (quoting confidentiality agreement).

187 Id. at 579.

188 Id. at 580.

either without authorization or by exceeding authorized access.[189] The district court agreed, reasoning that use of the scraper was so far beyond the "reasonable expectations" of EF that it was clearly unauthorized.[190]

On appeal, the First Circuit affirmed the district court's injunction, concluding that the use of the scraper likely violated the statute because its use implicitly breached the confidentiality agreement that Gormley had signed with EF.[191] The court reasoned that Gormley's decision to use a scraper on EF's site (as well as his help designing the scraper)[192] relied on his insider's knowledge of EF's website and business practices. However, Gormley had signed a contract with EF promising not to disclose any information about EF in a way that might be against EF's interests. Because the scraper was used against EF's interests, the court reasoned, Explorica's use of the scraper relied on information obtained in violation of the contractual agreement. As a result, use of the scraper exceeded authorized access to EF's computer and violated § 1030.[193] The opinion acknowledged that any user could manually query the EF website to learn EF's prices, but concluded that the scraper's "wholesale" approach "reeks of use—and, indeed, abuse—of proprietary information that goes beyond any authorized use of EF's website."[194] Although the reasoning in *Explorica* is opaque, if not tortured, the court appears to base the question of authorization on whether the conduct surrounding the access breached the confidentiality agreement. The agreement formed a contract, and access that at least implicitly breached the contract exceeded authorization.[195]

A district court in Virginia took a similar approach in *America Online v. LCGM, Inc.*,[196] a civil case brought by America Online against a spammer. The spammer had purchased an AOL account and used it (along with special software programs) to collect the e-

189 Id.

190 See id. The district court had embraced several alternative holdings as well, including the breach of contract approach adopted on appeal by the First Circuit. See id. (summarizing district court's reasoning).

191 See id. at 582 ("EF is likely to prove such excessive access based on the confidentiality agreement between Gormley and EF.").

192 See id. at 582 (describing "Gormley's heavy involvement in the conception of the scraper program").

193 See id. at 583 (describing attempts to prove otherwise as "an uphill battle").

194 Id.

195 In a subsequent case arising from the same dispute, the First Circuit clarified this test, explaining that the key factor was an explicit restriction on the use of the computer. See EF Cultural Travel v. Zefer Corp., 318 F.3d 58, 63 (1st Cir. 2003).

196 46 F. Supp. 2d 444 (E.D. Va. 1998).

mail addresses of thousands of AOL users.[197] AOL's Terms of Service expressly prohibited AOL members from harvesting e-mail addresses, however, and AOL argued that by violating the Terms of Service the spammer had accessed AOL without authorization. The district court agreed, with exactly one sentence of analysis: "Defendant's actions violated AOL's Terms of Service, and as such was [sic] unauthorized."[198]

Although *Explorica* and *LCGM* offer remarkably broad interpretations of unauthorized access statutes, the award for the broadest interpretation goes to Judge Jones of the Southern District of New York for his decision in *Register.com v. Verio*.[199] The facts of *Verio* resemble those of *Explorica*. As in *Explorica*, the defendant in *Verio* used an automated program to send queries to a database maintained by a business competitor, the plaintiff. Specifically, employees of the Internet service provider Verio used a search robot to query the publicly available WHOIS database (a database of names and contact information for domain name registrants[200]) maintained by Register .com.[201] The Verio search robot gathered contact information about Register.com's customers, and Verio employees would then contact Register.com customers and invite them to switch service providers from Register.com to Verio.[202] Register.com sued Verio, and moved

---

197 See id. at 448.

198 Id. at 450. In a subsequent case with nearly identical facts, a district court took a more cautious approach in the course of denying a motion for summary judgment filed by the plaintiff AOL. See Am. Online v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1272-73 (N.D. Iowa 2000). Rather than conclude that the violation of the AOL Terms of Service automatically made the access "without authorization," the court noted the many difficult questions raised by the issue as a ground for denying summary judgment:

> AOL members, such as [an agent of the defendant], obviously have "authorization" to access the AOL network. Having done so, is a member's authorized access converted into unauthorized access when the member violates one of the terms and conditions of membership? Similarly, is the member converted from an "insider" to an "outsider" for purposes of the CFAA by violating AOL's policies? On the other hand, if AOL members are "outsiders," then why would AOL's membership policies apply to them at all? Furthermore, by imposing restrictions on its members, can AOL deny or restrict the rights of non-member Internet users with respect to sending any type or volume of e-mail to AOL members, including Unsolicited Bulk E-mail (UBE)? These unanswered questions represent mixed issues of fact and law.

Id. at 1273.

199 126 F. Supp. 2d 238 (S.D.N.Y. 2000).

200 See id. at 241-42 (explaining WHOIS database). See also Jay P. Kesan & Rajiv C. Shah, Fool Us Once Shame on You—Fool Us Twice Shame on Us: What We Can Learn from the Privatizations of the Internet Backbone Network and the Domain Name System, 79 Wash. U. L.Q. 89, 183 (2001) (discussing WHOIS database).

201 See *Verio*, 126 F. Supp. 2d at 242 (describing Register.com's management of WHOIS database).

202 See id. at 243-44 (describing customer complaints regarding Verio's solicitations).

for a preliminary injunction against the use of the search robots on the ground (among others) that Verio's use of the search robot constituted an unauthorized access of Register.com's database.

The district court agreed.[203] Unlike the court in *LCGM*, however, the *Verio* court did not rely on a breach of the plaintiff's terms of use; the court concluded that the plaintiff's use of the robot did not actually breach any terms of use that Register.com had enacted.[204] Instead, the court concluded that *the mere fact that Register.com had decided to sue* Verio meant that Verio's use of the search robot was without authorization. "[B]ecause Register.com objects to Verio's use of search robots," the court held, "they represent an unauthorized access to the [Register.com] WHOIS database."[205] The fact that the computer owner had decided to object to the defendant's use of its computer after the conduct occurred made the access to the computer "without authorization."

It is possible to see *Explorica*, *LCGM*, and *Verio* as merely civil cases about abusive business practices. In all three cases, plaintiffs sued to block defendants from misusing and potentially damaging their computers, and courts perhaps understandably found a basis for stopping the arguably unfair practices. In the course of reaching these decisions, however, the courts also established important interpretations of "authorization" that presumably will apply equally to cases interpreting the same text in a criminal prosecution.[206] By using the law to aid sympathetic plaintiffs, the courts inadvertently have handed prosecutors a broad and powerful tool to punish breaches of contracts relating to computer use. Nearly any use of a computer that is against the interests of its owner is an "access" to the computer either "without authorization" or "exceeding authorized access" under these precedents, triggering severe criminal penalties.

D. Why Courts Have Struggled to Interpret Unauthorized Access

Proponents of unauthorized access laws often see the laws as analogues to the burglary and trespass laws that address real property crimes. In light of the failures of property-based crimes, the new laws prohibit "breaking in" to computers, which legislatures have described as the act of accessing computers without authorization. As we have just seen, however, this understanding is simplistic: "Access" and

[203] Id. at 252.

[204] See id. at 249 ("[T]he Court does not believe that Register.com's terms of use forbid the particular use of the search robot at issue here.").

[205] Id. at 251.

[206] See supra note 16 and accompanying text. **R**

"authorization" have proven much more complicated to apply in practice than they first appear to be.

Why? In the case of access, much of the blame belongs to the advance of computer technology since the 1970s. In 1975, a person who used a remote computer typically did so by "dialing in" to the computer over a telephone line.[207] The user then would encounter a text-based log-in prompt, and would need to enter a username and password to proceed.[208] Today, in contrast, computer users utilize networks to surf the Web, send and receive instant messages, download music and videos, and perform countless other tasks, often using "always on" Internet connections that merge seamlessly with the computers themselves.[209] While the concept of access may have made sense given 1975 computer technology, the technology of 2003 presents a different case. Back then, you knew when you accessed a computer; today you might know when you *use* a computer, but the word "access" is merely a label to be assigned somewhat awkwardly to conduct that may not seem like an access at all.

There are two major reasons courts have had difficulty interpreting the scope of "authorization." The first is that courts have yet to explore exactly what kind of authorization the statutes address. Presumably the computer's owner/operator has the primary authority to control what is authorized, much like a property owner might do for physical trespass laws. But as I explain in the next Part, access to a computer can be unauthorized in different ways, and courts have not yet recognized such differences and explained which types of unauthorized conduct fall within the scope of the statutes.

The second source of the difficulty is that many cases have interpreted "authorization" in the context of civil disputes rather than criminal prosecutions. The difference tends to push courts in the direction of expansive interpretations of new laws.[210] It is one thing to

---

[207] See, e.g., United States v. Seidlitz, 589 F.2d 152, 153 (4th Cir. 1978) (describing government agency's 1970s-era network using telephone circuits).

[208] Movie buffs may recall the scene in the 1983 Matthew Broderick movie *WarGames* in which Broderick's character spends hours trying to guess Dr. Falken's password in order to gain access to his account. After significant biographical research, the protagonist eventually guesses correctly that Dr. Falken's password was his son's name—Joshua. See WarGames (Metro Goldwyn-Mayer 1983).

[209] Cf. Gary Chapman, Digital Nation: Consortium Sets Sights on a "New Internet," L.A. Times, Apr. 5, 2001, at T4 (describing "new Internet" as "complex but seamless network of high-speed wireless nodes that are cheap, prolific, always on and accessed through a variety of technologies").

[210] I explore this theme in the context of Internet surveillance law in Orin S. Kerr, Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law, 54 Hastings L.J. 805, 829-30 (2003). The same argument applies to substantive criminal laws.

say that a defendant must pay a plaintiff for the harm his action caused; it is quite another to say that a defendant must go to jail for it. Courts are more likely to hold a defendant liable under an ambiguous statute when the stakes involve a business dispute between two competitors than when the government seeks to punish an individual with jail time.[211] As a result, civil precedents tend to adopt broader standards of liability than do criminal precedents. Because many unauthorized access cases have arisen in a civil context with sympathetic facts, courts have adopted broad approaches to authorization that in a criminal context would criminalize a remarkable swath of conduct involving computers.

III
A Proposed Interpretation of "Access" and "Authorization" in Computer Misuse Statutes

The history of computer crime law shows courts and legislatures trying to define a legal response to a problem that they only partially understand. In the first two decades, courts struggled to apply preexisting laws against theft and other property crimes to computer misuse. While they reached sensible outcomes in particular cases, no clear principles emerged. When computer misuse threatened or caused substantial harms, courts tended to find it criminal; when it did not, courts interpreted the law narrowly to avoid punishing the computer users.[212] In response to these uncertainties, legislatures enacted computer crime statutes that prohibited accessing computers without authorization, and in some cases, exceeding authorized access.[213]

While proponents of the new laws believed that they would cure the old ills, the old ills have reemerged, albeit in a slightly different form. Courts previously used harm as a proxy for theft; now they appear to use harm as a proxy for lack of authorization. The reasoning seems to go something like this: Use of a computer that causes harm to its owner is use that the owner would not want; use that an owner would not want is access that the owner implicitly has forbidden; and access that an owner implicitly forbids is access without authorization. Once again, the law has failed to create workable standards to guide courts. Instead, courts have interpreted the ambiguous legal standards to reach results that seemed correct given the facts of the particular case.

---

211 See id. (describing varying interests balanced by courts in criminal versus civil cases).

212 See generally supra Part I.

213 See generally supra Part II.

Can we do better? We can, and I suspect that in time we will. One promising alternative would be to replace one-size-fits-all unauthorized access statutes with new statutes that explicitly prohibit particular types of computer misuse. As I discuss below,[214] only a handful of possible types of computer misuse exist: It should be possible for a legislature to catalog them, decide which types it wishes to prohibit, and draft a statute narrowly tailored to that misconduct. Such an approach would better satisfy the basic aspiration of criminal law by describing the harmful conduct clearly and proscribing it directly.[215] As we develop more experience with computer misuse crimes, and as the categories of misuse become clearer, the pressure for such a direct approach surely will mount.

For now, however, unauthorized access statutes are here to stay. They remain on the books of the federal government and all fifty states, continue to expand internationally,[216] and even were mandated by the first international cybercrime convention ratified by the Council of Europe in November 2001.[217] In light of this, the practical question is whether the existing statutory framework can be interpreted to achieve better the normative goals of criminal law. I think that the answer is yes, at least for the most part; courts can do indirectly by judicial construction what legislatures have not yet done directly. The considerable ambiguities of current law afford courts the wiggle room to adopt interpretations of unauthorized access that mirror potential legislative reforms.

This Section recommends a normative interpretation of "access" and "authorization" that tracks potentially useful legislative reforms. I propose that courts interpret "access" broadly, but limit the phrase "without authorization" to the circumvention of code-based restrictions. Access that merely breaches a contract conditioning access should not suffice to trigger criminal liability. This approach provides the best solution on policy grounds: It best mediates the difficult line between privacy and liberty online. The approach is also the best doctrinal interpretation in light of the traditional treatment of consent in

214 See infra notes 276-85 and accompanying text. R

215 See City of Chicago v. Morales, 527 U.S. 41, 56 (1999) (noting that under Supreme Court's vagueness jurisprudence, law is void if it "fail[s] to provide the kind of notice that will enable ordinary people to understand what conduct it prohibits").

216 See generally Schjolberg, supra note 6. R

217 See Convention on Cybercrime, Nov. 23, 2001, art. 2, Europ. T.S. No. 185, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (last visited Sept. 30, 2003) ("Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right.").

criminal law. Finally, the proposed interpretation best satisfies the basic theories of punishment and avoids constitutional difficulties.

I explain the proposal in five sections. I begin by explaining the distinction between circumventing code-based restrictions and breaching contractual restrictions. I next offer a normative interpretation of "access" followed by a normative interpretation of "without authorization." I then explain how unauthorized access statutes would coexist with other criminal statutes under my proposal, and how they create a need for special database protection laws that would address types of misuse that unauthorized access statutes should not. In the final Section, I demonstrate how my recommended interpretation would apply to several common fact patterns, including that of the outside hacker and the disgruntled employee.

A. Regulation by Code Versus Regulation by Contract

Although unauthorized access statutes speak of authorization as if it were a monolithic concept, there are in fact two fairly distinct ways in which access or use of a computer can be unauthorized. Each type corresponds to one of the basic ways that a computer owner can regulate a user's privileges. A computer owner can regulate a user's privileges by code or by contract. Similarly, a computer user can engage in computer misuse by circumventing code-based restrictions, or by breaching contract-based restrictions.

When an owner regulates privileges by code, the owner or her agent codes the computer's software so that the particular user has a limited set of privileges on the computer.[218] For example, the owner can require every user to have an account with a unique password, and can assign privileges based on the particular account, limiting where the user can go and what she can do on that basis.[219] For a user to exceed privileges imposed by code, the user must somehow "trick" the computer into giving the user greater privileges. I label this approach "regulation by code" because it relies on computer code to create a barrier designed to block the user from exceeding his privileges on the network.

Circumventing regulation by code generally requires a user to engage in one of two types of computer misuse. First, the user may engage in false identification and masquerade as another user who has greater privileges. For example, the user can use another person's password, and trick the computer to grant the user greater privileges

[218] See Lawrence Lessig, Code and Other Laws of Cyberspace 66-78 (1999) (discussing how computer owners can regulate rights of users by regulating code).

[219] See id.

that are supposed to be reserved for the true account holder.[220] If *A* knows *B*'s username and password, *A* can log in to *B*'s account and see information that *B* is entitled to see, but *A* is not.

Alternatively, a user can exploit a weakness in the code within a program to cause the program to malfunction in a way that grants the user greater privileges.[221] Consider a so-called "buffer overflow" attack, a common means of hacking into a computer.[222] A buffer overflow attack overloads the victim computer's memory buffer, forcing the computer to malfunction and default to an open position that gives the user "root" or "super user" privileges.[223] These privileges give the user total control over the victim computer: With root privileges, the user can access any account or delete any file. The attack circumvents the code-based restriction that limited the user to her own account. Such misuse violates the intended function test introduced in the *Morris* case; a user who exploits a weakness in code to trick the victim computer into granting the user extra privileges does so by using the code in a way contrary to its intended function.

The second way an owner may attempt to regulate computer privileges is by contract. The owner can condition use of the computer on a user's agreement to comply with certain rules.[224] If the user has a preexisting relationship with the owner/operator, the conditions may take the form of Terms of Service.[225] If no such relationship exists, the conditions may appear as Terms of Use to the service the computer provides, such as a click-through agreement that might appear prior to use of a website. For example, an adult website may require a user to promise that she is at least eighteen years old before

---

220 See Bruce Schneier, Secrets and Lies: Digital Security in a Networked World 136-41 (2000) (discussing how computers use passwords to authenticate users).

221 See id. at 151-75 (discussing various ways that users can exploit software weaknesses to obtain access).

222 See Ethan Preston & John Lofton, Computer Security Publications: Information Economics, Shifting Liability and the First Amendment, 24 Whittier L. Rev. 71, 72 (2002) (describing buffer overflow).

223 Preston and Lofton describe the effect of a buffer overflow as follows:

> A buffer overflow functions by inputting more data than a vulnerable program anticipates. The buffer overflow then overwrites portions of the program in the computer's memory, or RAM. Because the program only reserves memory space for the anticipated data, the extra input "overflows" into memory reserved for the program, overwriting portions of the vulnerable program's code. After processing the anticipated input in the reserved space in the memory, the computer then interprets the unanticipated overflow as part of the original, vulnerable program. The end result is that if a buffer overflow is properly constructed, it may be used to gain control over the computer.

Id. at 72-73.

224 See generally supra Part II.C.

225 See supra note 109. **R**

allowing her to access adult materials available through the website. Finally, the restriction may be implicit rather than stated in the written text.

Regulation by contract offers a significantly weaker form of regulation than regulation by code. Regulation by code enforces limits on privileges by actually blocking the user from performing the proscribed act, at least absent circumvention. In contrast, regulation by contract works on the honor system, or perhaps more accurately, the honor system backed by contract law remedies. Consider the adult website that requires users to indicate that they are at least eighteen years old before it allows users to enter. A seventeen-year-old can access the adult website just as easily as an eighteen-year-old can. The only difference is that the seventeen-year-old must misrepresent her age to access the site. To use a physical-world analogy, the difference between regulation by code and regulation by contract resembles the difference between keeping a stranger out by closing and locking the door and keeping a stranger out by putting up a sign in front of an open front door saying "strangers may not enter."

Importantly, the distinction between regulation by code and regulation by contract is less an on-off switch than a continuum with two extremes. Examples exist that blend the two concepts. For example, a computer owner could set up a website that appears to require a username and password to access the contents of the site, but that actually grants access for *any* username and password combination. Such a site would appear to a user to regulate by code, but would actually work more like a system of regulation by contract. In most instances, however, the regulation of privileges by computer owners falls relatively clearly into either regulation by code or regulation by contract.

B. A Proposal for Interpreting "Access"

Interpretations of "access" and "authorization" are inextricably linked. The phrase "without authorization" modifies "access," and it is impossible to understand the implications of one of these terms without reference to the other. A broad construction of access can balance a narrow construction of unauthorized, and vice versa. Still, I must start somewhere. I will begin with the meaning of access, and then turn to the meaning of authorization.

I propose that courts adopt a broad construction of access. *Specifically, I propose that a user accesses a computer any time the user sends a command to that computer that the computer executes. In*

effect, I would define access as any successful interaction with the computer.[226]

My approach is notably broader than the approach taken in *State v. Allen*.[227] Recall that in the *Allen* case, the Kansas Supreme Court held that a user did not access a Bell computer by repeatedly calling up the logon prompt.[228] Because the user did not get "inside" the Bell computer, the court held, he had not accessed it.[229] My approach would teach that Allen did access the Bell computer. By calling up the Bell computer, Allen sent a command asking the Bell computer to send back its logon prompt and prepare to check a password. The Bell computer did so, sending Allen the logon prompt. While the Bell computer did not permit Allen to view other information stored within it, Allen did have successful interactions with the Bell computer at the pre-logon stage. Although this does not mean that the access was without authorization (more on that shortly), it should mean that Allen did access the computer, albeit in a limited way. My approach is also consistent with the conclusion in *America Online v. National Health Care Discount, Inc*. that sending an e-mail accesses the computers through which the e-mail is transmitted in the course of delivery.[230]

The reader may wonder why I would propose such a broad definition. After all, this Article criticizes broad constructions of computer crime statutes, and surely a broad interpretation of access only compounds the problem. I have opted for this approach for a purely instrumentalist reason: It works better for the narrowing construction to come from restrictions on the meaning of "without authorization" rather than "access." Accordingly, courts should adopt a broad interpretation of access, and should rely on "without authorization" for a suitable hook to narrow the scope of unauthorized access statutes.

The problem with a narrow construction of access is that individual users interact with computers in countless ways for countless reasons, and it is difficult to carve out a type of interaction that should be exempted entirely from computer misuse laws. A typical computer user might log on to a network using a password, open files stored on a server, surf the web, and send e-mail. If any one of these activities

---

226 For purposes of this standard, I have in mind an objective measure of success, not a subjective one. This is something like the *Morris* intended function test: Did the command do what the command was designed to do?

227 917 P.2d 848 (Kan. 1996).

228 See id. at 850.

229 See id. at 851.

230 Am. Online v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1272-73 (N.D. Iowa 2000).

does not constitute an access, then that entire category of activity may be exempted from laws that are designed broadly to prohibit exceeding privileges on a computer.

Further, the distinctions between different types of use are sufficiently fluid, and the technology of the Internet changes so rapidly, that such distinctions would prove highly unstable and ultimately arbitrary. While a narrow meaning for access may have made sense in the 1970s, today's technologies cannot support it. Web-based e-mail services such as those provided by Hotmail and Yahoo! illustrate the problem. When a Hotmail or Yahoo! e-mail client logs on to send and retrieve e-mail, that user is logging on to the Hotmail or Yahoo! server, but at the same time is also surfing the web (because the e-mail software is web-based), retrieving stored files (by viewing incoming mail), and sending outgoing files (by sending outgoing e-mail). If one of these categories cannot constitute an "access" but another can, then courts must draw lines between categories that the technology and everyday use of the Internet does not support.

Such line drawing would allow computer owners to devise legally controlling but entirely arbitrary mechanisms to determine how unauthorized access laws apply to their computers. Imagine a rule stating that viewing a public website does not access the hosting computer, but that bypassing a barrier such as a password prompt triggers an access. A website owner seeking the protection of criminal law could simply create an entrance page to the site that either forces users to click-through the entrance (perhaps even with a graphic of a closed door that opens), or could prompt the user for a password but allow everyone in regardless of what password they enter. This would give the user a sense of going "inside" the computer, as opposed to merely visiting an open public place, triggering an access. But the difference would be one of form, not substance.

In light of the difficulty of drawing robust and sensible lines between different types of interactions with computers and limiting access to just some of them, the better approach is to allow access to refer broadly to any successful interaction with a computer, no matter how minor. The functional effect of this broad construction is to eliminate access as a limit on the scope of unauthorized access statutes, and to place major weight on the meaning of authorization, to which I now turn.

C. A Proposal for Interpreting the Scope of Authorization

The next and more difficult goal is to define what it means to access a computer "without authorization," and, if it is different, to

"exceed authorized access." As I explained earlier, a user can exceed privileges on a computer in two fundamental ways: by circumventing regulation by code, and by breaching regulation by contract.[231] When a user circumvents regulation by code, she tricks the computer into giving her greater privileges than she is entitled to receive. This normally can occur in two ways. First, a user can enter the username and password of another user with greater privileges, something I have labeled false identification.[232] Second, a user can exploit a design flaw in software that leads the software to grant the user greater privileges, violating the *Morris* unintended function test.[233] In contrast, when a user breaches a regulation by contract, the user need not trick the computer: The user need only take steps that breach a condition of the use imposed by the computer owner.[234]

The question is, which of these ways should suffice to establish that access was "without authorization?" *I propose that courts limit access "without authorization" to access that circumvents restrictions by code.* Breaches of regulation by contract should as a matter of law be held to be insufficient grounds for access to be considered "without authorization." In other words, I propose that courts reject contract-based theories of authorization. Access should be deemed "without authorization" only when it either violates the *Morris* intended function test, or else uses false identification to trick the computer into granting the user greater privileges. The practical effect of this proposal would be to reduce greatly the scope of unauthorized access statutes from the broad outlines seen in cases such as *Explorica*, *Verio*, and *Shurgard* to the more narrow "core" cases such as *Morris*. Why is this the best interpretation of "without authorization?" Instrumental, historical, and doctrinal rationales all support this conclusion. From an instrumentalist perspective, limiting the scope of computer misuse statutes to the circumvention of code-based restrictions would let criminal law advance two vitally important and often conflicting goals of Internet regulation: first, to allow Internet users to enjoy as much freedom as possible to do as they wish online, and, second, to protect the privacy and security of Internet users and their data. These competing concerns frame the underlying tension that should define the scope of unauthorized access statutes. On one hand, the profound social value of the Internet derives from its ability to open up new worlds to its users; to provide a forum for free expression and (within

---

231 See supra Part II.B.

232 See supra note 220 and accompanying text. **R**

233 See supra notes 136, 152-56 and accompanying text. **R**

234 See supra text accompanying note 224. **R**

limits) conduct.[235] As Professor Lessig and others have emphasized, the value of the Internet derives in large part from the values of liberty embedded in its original architecture.[236] On the other hand, the Internet's social value also depends on the existence of a combined legal and technical framework that allows Internet users to establish a zone of privacy and security, free from the intervention of others (again, within limits).[237] These two values can conflict. For example, what a hacker might characterize as an exercise in free exploration would likely be viewed by the hacker's victim as an invasion of her privacy and security.[238] But to the extent that criminal law can impact such broader questions at the margins, the normative challenge of unauthorized access statutes is to mediate the line between openness on the one hand, and privacy and security on the other.

Construing "without authorization" to include both the circumvention of code-based barriers and breaches of contract simply draws the line in the wrong place. It grants computer network owners too much power to regulate what Internet users do, and how they do it, sacrificing a great deal of freedom for a small (and arguably minimal) gain in privacy and security.

Consider the remarkable and disturbing results that a contract-based approach to authorization can create. Imagine that a website owner announces that only right-handed people can view his website, or perhaps only friendly people. Under the contract-based approach, a visit to the site by a left-handed or surly person is an unauthorized access that may trigger state and federal criminal laws. A computer

---

[235] See ACLU v. Reno, 521 U.S. 844, 850 (1997) (noting that Internet "enable[s] tens of millions of people to communicate with one another and to access vast amounts of information from around the world. The Internet is 'a unique and wholly new medium of worldwide human communication.'" (citation omitted)).

[236] See, e.g., Lawrence Lessig, Code and Other Laws of Cyberspace 6 (1999); Lawrence Lessig, The Death of Cyberspace, 57 Wash. & Lee L. Rev. 337, 344 (2000) ("[The Internet] fed on a diet of ignoring the claims of property and control that the IP lawyers insisted upon. It thrived not by hoarding or protecting or sheltering ideas, and creativity; it thrived by giving it all away. In contrast to real space, where theft is policed and criminals go to jail, cyberspace is that place where theft produced prosperity.").

[237] See Paul M. Schwartz, Internet Privacy and the State, 32 Conn. L. Rev. 815, 815 (2000) ("Millions of people now engage in daily activities on the Internet, and under current technical configurations, this behavior generates finely grained personal data. In the absence of effective limits, legal or otherwise, on the collection and use of personal information on the Internet, a new structure of power over individuals is emerging. This state of affairs has significant implications for democracy in the United States . . . ."); see also Pamela Samuelson, Privacy as Intellectual Property, 52 Stan. L. Rev. 1125, 1126 (2000) (noting challenges Internet raises to maintaining privacy in personal information).

[238] See Michael Lee et al., Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal, 14 Berkeley Tech. L.J. 839, 845 (1999) (noting tension between computer hacking and privacy).

owner could set up a public web page, announce that "no one is allowed to visit my web page," and then refer for prosecution anyone who clicks on the site out of curiosity. By granting the computer owner essentially unlimited authority to define authorization, the contract standard delegates the scope of criminality to every computer owner.

In contrast, my proposal to limit the scope of unauthorized access to the circumvention of code-based restrictions draws a more balanced line between openness and privacy that carves out zones for each. The proposal would allow Internet users to use the Internet, visit websites, and send e-mails without the chilling effect of possible criminal sanctions arising from the breach of Terms of Service, Terms of Use, or other contractual terms. My proposal would not trigger a cyberspace free-for-all: Users would still be regulated both by contract law and traditional criminal laws, just as they would be off-line. However, unauthorized access laws would no longer threaten to transform disagreements with computer owners into criminal violations.

Conversely, my proposal would extend the protection of the criminal laws to those who erect code-based restrictions on access and then have those restrictions circumvented (and their privacy invaded) by others. Those who want the criminal justice system to help protect the privacy and security of their networks and data would be free to erect code-based barriers to unwanted access. By locking away data behind a code-based mechanism such as a password gate, users could not only increase their privacy from a technical standpoint but also enjoy the additional privacy protection (albeit only a marginal one in most cases) of criminal sanction under unauthorized access statutes. The criminal law would end up encouraging users to protect their privacy in the way most likely to be technically effective, by creating accounts and password schemes rather than by attempting to establish privacy via mere contractual agreements.[239]

---

[239] Despite my focus on circumventing code-based restrictions and general endorsement of the circumvention standard, my proposal does not necessarily bolster the case for the anti-circumvention provisions in the controversial Digital Millennium Copyright Act (DMCA). See 17 U.S.C. § 1201(a)(1)(A) (2000) ("No person shall circumvent a technological measure that effectively controls access to a work protected under this title."). Unauthorized access statutes concern access to computers belonging to another. Because the owner/operator of the computer sets the rights and privileges, an owner's access to his own computer is authorized under these unauthorized access statutes. The DMCA is different. The DMCA prohibits circumvention of a code-based restriction even on a defendant's own computer. As a result, my view that circumventing a code-based restriction can be a legitimate basis for liability does not necessarily mean that it is appropriate in the specific context of the DMCA. For more on my views of the DMCA, see generally Orin S. Kerr, A Lukewarm Defense of the Digital Millennium Copyright Act, in Copy Fights 163 (Adam Thierer & Wayne Crews eds., 2002) (arguing that there is a "method to the mad-

Criminalizing circumvention of code but not breach of contract also tracks the traditional treatment of consent defenses in criminal law, and therefore offers the most correct doctrinal interpretation of unauthorized access statutes. The key is that the statutory element "without authorization" is simply a modern version of traditional statutory elements involving lack of consent found in other criminal laws. If courts interpret "without authorization" in the same way that they interpret other consent elements in criminal law, they should recreate the distinction between code-based and contract-based restrictions and limit the scope of unauthorized access statutes to circumvention of the former.

To see why, follow me on a brief detour into consent defenses in criminal law. Although many criminal law offenses do not permit a consent defense,[240] a few traditional crimes require absence of consent or permission as an element of the offense.[241] For example, trespass and burglary prohibit presence on physical property without the permission of the owner; rape and sexual assault prohibit sexual penetration without the consent of the victim. In many cases, consent or the lack of consent is clear. In some cases, however, consent raises difficult legal questions. The scope of consent is particularly difficult when a perpetrator tricks the victim into granting authorization and consent, and the court must determine whether the trickery vitiates the consent. The law recognizes the victim's consent in some contexts, but not in others.

The general approach is to focus on whether the victim actually consented to the act that occurred, regardless of whether the victim consented in reliance on representations concerning collateral matters. Courts and commentators often label this the difference between consent derived from fraud in the inducement and consent derived from fraud in the factum.[242] When a victim agrees to allow the defendant to engage in specific conduct in reliance on a misrepresentation, the consent is based on fraud in the inducement, and the consent remains valid despite the misrepresentation. The element "without

ness" of DMCA, and that anticircumvention provisions of DMCA may prove "a respectable model for how to enforce intellectual property rights and contractual rights in cyberspace").

[240] See Rollin M. Perkins & Ronald N. Boyce, Criminal Law 1075 (3d ed. 1982).

[241] The most important of these crimes is rape, which requires sex without consent. Another crime is operating a motor vehicle without the consent of its owner. See id. at 1084.

[242] See id. at 1084 ("[T]he distinction between fraud in the factum and fraud in the inducement is controlling in the prosecution of offenses in which absence of consent is an element of the crime . . . .").

consent" or "without authorization" normally will not be met.[243] In contrast, when a victim allows the defendant to engage in one kind of conduct but the defendant engages in a *different* type of conduct, the consent is based on fraud in the factum and the law will not recognize it.[244] The element "without consent" is satisfied.

Consider a few examples drawn from prior cases. A man who borrows a car from its owner after promising that he will borrow it for only a few minutes instead takes the car for several hours. The defendant is not guilty of use of an automobile without the consent of the owner.[245] Because the owner actually agreed to let the defendant drive the car, the misrepresentation is merely fraud in the inducement. Several common and quite disturbing examples of the distinction appear in cases interpreting the law of rape, which prohibits sexual intercourse without consent. For example, a man who falsely claims to be a doctor and convinces a woman that she must have sex with him to cure her of a serious disease is not guilty of rape, because the woman's consent to have intercourse derives from fraud in the inducement.[246] In contrast, a gynecologist who tricks a female patient into having sexual intercourse with him by convincing her that she merely is submitting to a nonsexual medical exam is guilty of rape because the fraud constitutes fraud in the factum.[247] Although the circumstances of property crimes and sexual assault crimes are of course dramatically different, the same basic rule has been held to apply in both contexts: The key question is whether the victim has consented to the

---

243 See id.

244 As Perkins and Boyce summarize:

> The general rule is that if deception causes a misunderstanding as to the fact itself (fraud in the factum) there is no legally recognized consent because what happened is not that for which consent was given; whereas consent induced by fraud is as effective as any other consent . . . if the deception relates not to the thing done but merely to some collateral matter (fraud in the inducement).

Id. at 1079.

245 See, e.g., People v. Donell, 32 Cal. Rptr. 232, 234-35 (Cal. Dist. Ct. App. 1973); State v. Boggs, 164 N.W. 759, 760 (Iowa 1917); State v. Mularky, 218 N.W. 809, 810 (Wis. 1928).

246 See, e.g., Boro v. People, 210 Cal. Rptr. 122 (Cal. Ct. App. 1985). In *Boro*, Ms. R., the victim, received a telephone call from a person who identified himself as "Dr. Stevens" and said that he worked at a local hospital. "Dr. Stevens" informed Ms. R. that he had the results of her blood test, and that she had contracted a dangerous, highly infectious and perhaps fatal disease. "Dr. Stevens" informed Ms. R. that the disease came from using public toilets, and that the disease could be cured only through either a painful procedure or "sexual intercourse with an anonymous donor who had been injected with a serum." Id. at 123. Ms. R. believed "Dr. Stevens" and had sexual intercourse with the defendant, who of course had posed as "Dr. Stevens." Id. at 124.

247 See, e.g., People v. Minkowski, 23 Cal. Rptr. 92 (Cal. Ct. App. 1962) (upholding conviction of doctor who raped patients under guise of performing medical tests).

specific act. Misrepresentation as to a collateral matter does not suffice to satisfy the legal requirement of lack of consent.[248]

Why is this standard relevant to unauthorized access statutes? My contention is that the distinction between circumventing code-based restrictions and breaching contract-based restrictions relates to the traditional distinction between fraud in the inducement and in the factum. The comparison may seem a bit jarring at first, as it substitutes a computer for a human victim and the nature of the harm is vastly different. But similarities exist at a conceptual level: Computer misuse laws prohibit access to a computer without authorization, whereas trespass laws prohibit physical appearance in a home without permission and (if one can pardon the comparison) rape and sexual assault laws prohibit sexual intercourse without consent. Speaking anthropomorphically for a moment, the computer is "tricked" into authorizing the defendant to access the computer, in a way conceptually similar to how a homeowner might be tricked into allowing a person into their home or a victim might be tricked into consenting to a request to engage in sexual activity.[249] From this perspective, the

[248] Importantly, the distinction between fraud in the factum and fraud in the inducement is not self-executing, but rather depends on a somewhat arbitrary definition of the scope of the factum. If the key question is whether the defendant has consented to the specific act, an important corollary is how narrowly or broadly to define that specific act. This raises a policy question with no precise answer. Courts tend to define the act with reference to policy goals driving the specific area of law. Courts have encountered this issue most often in the context of rape prosecutions, such as when a man tricks a woman into consenting to have sex with him by making her believe that the man is her husband. See Boyce & Perkins, supra note 240, at 1080-81. In these circumstances, some courts have defined the factum specifically as sexual intercourse with the victim's spouse, in which case the fraud is in the factum and the sex is rape; other courts have defined the factum more generally as the act of sexual intercourse, in which case the fraud is in the inducement and the sex does not constitute rape. See id. R

Similarly, courts construing consent in the context of trespass and burglary into a private home have tended to view most trickery used to gain access into a home as fraud in the factum, in recognition of the sanctity of the home. See, e.g., People v. Bush, 623 N.E.2d 1361, 1364 (Ill. 1993) (concluding that if "the defendant gains access to the victim's residence through trickery and deceit and with the intent to commit criminal acts, his entry is unauthorized and the consent given vitiated because the true purpose for the entry exceeded the limited authorization granted"); People v. Smith, 637 N.E.2d 1128, 1133 (Ill. App. Ct. 1994) ("[W]hen a person comes to a private residence and is invited in by the occupant, the authorization to enter is limited, and any criminal acts committed therein exceed this limited authority."); People v. Williams, 667 N.Y.S.2d 605, 607 (N.Y. Sup. Ct. 1997) (concluding that "a person who gains admittance to premises through intimidation or by deception, trick or artifice, does not enter with license or privilege" for purposes of criminal trespass liability). These cases indicate that the factum/inducement distinction offers a limiting doctrine, but one that still requires a policy decision to be made as to how much the distinction limits the scope of the law.

[249] But see Dennis S. Karjala, The Relative Roles of Patent and Copyright in the Protection of Computer Programs, 17 Marshall J. Computer & Info. L. 41, 63 (1998) ("Computers, at least at present, do not 'read,' 'interpret,' or 'understand' computer programs.

fact that a user accessed the computer means that the computer must have authorized the access. The question is, was the authorization induced by a type of fraud that voids the authorization as a matter of law? What kind of fraud negates the authorization the computer granted the user?

Access based on breach of contract resembles fraud in the inducement: The computer "agrees" to allow the user access, subject to some promise or condition. For example, if a user registers for an e-mail account and later breaches the terms of service, she in effect convinces the computer to grant her access based on the false representation that she will comply with the terms. The access breaches the terms of service, but the fraud against the computer is only fraud in the inducement. Following traditional principles of criminal law, the access should not be deemed "without authorization." No criminal violation has occurred.

In contrast, access that circumvents code-based restrictions resembles fraud in the factum. The computer has not agreed to let the user access the computer. Instead, the computer is tricked into letting the user access the computer through a misrepresentation as to whether the user is accessing the computer at all. The computer may "believe" that the user is someone else, as in the case of a defendant utilizing another person's username and password. The computer may be tricked into unwittingly giving access to the user, as in the case of a hacking exploit such as a buffer overflow attack.[250] Both cases resemble fraud in the factum because the computer does not recognize that it is consenting to access by that particular user. The fraud in the factum voids the authorization, and the access is legally "without authorization."

The common law distinction between fraud in the factum and fraud in the inducement does not clearly answer how courts should interpret unauthorized access statutes. As I noted earlier, its rationale points the way toward a narrowing of the scope of computer crime statutes, but does not necessarily define that new scope. The choice of how to define the factum remains.[251] Nor do I mean in any way to endorse the use of the common law distinction in its most controver-

---

No combination of anthropomorphic language changes the simple fact that computers process electronic signals according to the laws of physics. . . . The computer . . . is simply doing what comes naturally, that is, what it is forced to do by the laws of nature.").

[250] For a discussion of buffer overflow attacks, see supra notes 222-23 and accompanying text. R

[251] See supra note 242. Consider the case of a minor viewing an adult website after clicking on a button agreeing that the minor is at least eighteen years old. It is possible to view that as a case of fraud in the factum: The computer consented to access by an adult, not by a minor. Alternatively, it is possible to view this as fraud in the inducement: The R

sial application, the law of rape.[252] The interest in sexual autonomy protected by rape laws is clearly on a vastly different scale than the interests protected by computer crime laws. But despite these caveats, I believe that the common law distinction offers a significant doctrinal hook courts can use to reject contract-based theories of authorization and limit the statutes to the circumvention of code-based restrictions. Courts have created a roughly analogous limiting principle when confronted with analogous issues in other areas of criminal law, and should incorporate the same limiting principle here.[253]

My proposed interpretation also satisfies the normative theories of punishment that traditionally shape the contour of criminal sanctions. For the most part, legislatures limit the scope of criminal liability to conduct that satisfies both utilitarian and retributive goals.[254] Utilitarian goals include deterrence,[255] rehabilitation,[256] and incapacitation.[257] In the context of computer crimes, the most important of these utilitarian goals is deterrence: The law should use the threat of criminal prosecution to dissuade actors from engaging in harmful conduct, or more modestly, to channel actors toward less harmful conduct.[258] The retributive goal attempts to match the scope of

computer consented to the access, and was induced to consent based on the misrepresentation as to the collateral matter of the user's age.

252 Feminist legal scholars have criticized the factum/inducement distinction for not protecting women enough in the context of rape law. They note that the distinction overlooks the reality that a woman tricked into sex with a man has suffered an enormous violation of her right to sexual autonomy. See Patricia J. Falk, Rape by Fraud and Rape by Coercion, 64 Brook. L. Rev. 139, 157-61 (1998).

253 From this perspective, expansive interpretations of "unauthorized access" in cases such as *Explorica* and *Verio* are incorrect because they overlook the distinction between fraud in the factum and fraud in the inducement that traditionally has limited the scope of criminal statutes that include a consent or authorization element. *Verio* and *Explorica* treat all cases as fraud in the factum, broadening the scope of computer crime statutes beyond their natural scope.

254 See Kent Greenawalt, Punishment, in 4 Encyclopedia of Crime and Justice 1333, 1342 (Sanford H. Kadish ed., 1983) ("[S]ome mixture of utilitarian and retributive elements provides the most cogent approach to punishment.").

255 Deterrence has been defined as "the inhibiting effect that punishment, either actual or threatened, will have on the actions of those who are otherwise disposed to commit crimes." Herbert L. Packer, The Limits of the Criminal Sanction 39 (1968).

256 Professor Packer defined rehabilitation as preventing crime "by so changing the personality of the offender that he will conform to the dictates of the law; in a word, by reforming him." Id. at 53.

257 Incapacitation is the use of physical restraint to make it impossible (or at least difficult) for the defendant to commit crimes during the period of the restraint. See James Q. Wilson, Thinking About Crime 145-61 (1983).

258 See Neal Kumar Katyal, Deterrence's Difficulty, 95 Mich. L. Rev. 2385, 2386-90 (1997) (arguing that deterrence functions like pricing mechanism, causing actors to substitute some acts for others when price is too high).

criminality with a societal concern for justice.[259] When the government brings a criminal prosecution, that prosecution should address conduct that society finds morally blameworthy; by punishing the blameworthy conduct, the prosecution signals society's refusal to tolerate the injustice of the criminal act.[260]

While scholars remain split on whether breach of a contract inflicts a broader utilitarian and moral wrong,[261] I think a qualitative difference exists between the culpability and threat to privacy and security raised by breach of a computer use contract on one hand, and circumvention of a code-based restriction on the other. A breach of Terms of Use or Terms of Service is a breach of trust with the computer owner or operator, but it is a breach of trust that traditional rules and remedies of contract law are well equipped to regulate and deter. It can involve a kind of invasion of privacy, but it is a lesser invasion based on an assumption of risk, not a direct invasion of a private space.[262] A user who breaches a contractual restriction on access has seen what the computer allowed the user to see, but under circumstances different from those the owner/operator of the computer wished.

In contrast, circumvention of code-based restrictions threatens more substantial privacy interests, and involves significantly greater culpability.[263] The law of burglary traditionally has recognized that the act of "breaking in" to a protected space itself has special resonance.[264] "Breaking in" threatens the security of those who protect their most private spaces with effective physical or code-based barriers, leaving such persons with few alternative means of protecting their privacy and property. And as the commentaries to the Model Penal Code note with respect to physical-world dwellings, criminal

---

259 See Packer, supra note 255, at 37-39. R

260 See Jean Hampton, The Retributive Idea, in Forgiveness and Mercy 124-29 (Jeffrie G. Murphy & Jean Hampton eds., 1988).

261 Compare Richard A. Posner, Economic Analysis of Law 118-20 (4th ed. 1992) (arguing that breach of contract should be encouraged when breach would be economically efficient), with Charles Fried, Contract as Promise: A Theory of Contractual Obligation 13-21 (1981) (arguing that breach of promise constitutes serious moral wrong).

262 Cf. Hoffa v. United States, 385 U.S. 293, 302 (1966) (holding that Fourth Amendment is not violated in case in which defendant told friend private information on assumption that friend would not disclose, but friend disclosed information to police).

263 Cf. Preston, supra note 10, at 25-26 (arguing that courts should rely on metaphor of R electronic "fences" to determine when access occurs, because it "allows courts to distinguish between relative degrees of care that the owner has taken to restrict information flows").

264 See LaFave, supra note 30, at 883 (noting that at common law, burglary required R "the creation of a breach of an opening; a mere trespass at law was insufficient"); see also 4 William Blackstone, Commentaries *226 ("There must be an actual breaking; not a mere legal clausum fregit . . . but a substantial and forcible irruption.").

law has traditionally and sensibly offered special protection to private spaces that act as "each man's castle, . . . the place of security for . . . his most cherished possessions."[265] By analogy, many Internet users treat their password-protected accounts as their virtual homes online, and would treat an unauthorized access to their accounts as a major breach of privacy and security. Whereas a breach of a contractual restriction is a breach of trust with the computer owner, the circumvention of a code-based restriction combines breach of trust with an invasion of the privacy of the individual whose private files were accessed. The harm is considerably greater and the actor's moral culpability more substantial in the case of circumventing code-based restrictions than in the case of breaching contractual restrictions on access.

Finally, interpreting unauthorized access statutes in the way that I propose complies with the tenet of statutory construction that courts should construe statutes to avoid difficult constitutional questions.[266] Applying a contract-based theory of authorization in a criminal context would raise two significant constitutional concerns: First, the statute so construed may be constitutionally overbroad, criminalizing a great deal beyond core criminal conduct, including acts protected by the First Amendment. "[T]he overbreadth doctrine permits the facial invalidation of laws that inhibit the exercise of First Amendment rights if the impermissible applications of the law are substantial when judged in relation to the statute's plainly legitimate sweep."[267] A contract-based interpretation of "unauthorized access" could implicate this doctrine by granting computer owners the power to criminalize speech, and even mere thoughts.[268]

A contract-based approach would create overbreadth concerns because it allows a computer owner to harness the criminal law at his discretion, using his unilateral power to control authorization by contract as a tool to criminalize any viewpoint or status the owner wishes to target. For example, a pro-life owner of a computer network could insert a paragraph in the Terms of Use agreement allowing only those who express pro-life opinions (or even only those who are pro-life) to use the network. Expressing pro-choice viewpoints would violate the

[265] Model Penal Code § 221.1 cmt. at 67 (Official Draft & Revised Comments 1980).

[266] See INS v. St. Cyr, 533 U.S. 289, 299-300 (2001) ("[I]f an otherwise acceptable construction of a statute would raise serious constitutional problems, and where an alternative interpretation of the statute is fairly possible . . . we are obligated to construe the statute to avoid such problems." (quotations and citations omitted)).

[267] See City of Chicago v. Morales, 527 U.S. 41, 52, 56 (1999) (quotations omitted).

[268] Cf. Lewis v. City of New Orleans, 415 U.S. 130, 132-34 (1974) (invalidating for overbreadth ordinance making it criminal "to curse or revile or to use obscene or opprobrious language toward or with reference to" police officer performing official duties).

Terms of Use, making the access "without authorization" or "exceeding authorized access" and triggering criminal liability.[269] Because protected expression would breach the contract and implicate criminal law, the contract theory could be used to suppress a significant amount of free speech.[270] The precise contours of the overbreadth doctrine remain notoriously difficult to apply, and courts may not accept the argument that overbreadth renders unconstitutional a contract-based interpretation of authorization.[271] However, the potential constitutional difficulties raised by such an expansive construction of computer crime statutes counsel in favor of a narrower interpretation such as the one that I propose.

A contract-based approach to authorization may also render unauthorized access statutes void for vagueness on the ground that the statutes "fail to provide the kind of notice that will enable ordinary people to understand what conduct it prohibits."[272] Few users read the terms of service or terms of use of any of the computers they access, much less all of them, and many restrictions feature ambiguous terms that can be quite difficult to interpret.[273] It is difficult, if not impossible, for a typical user to know for sure whether he is in compliance with all of the contractual restrictions regulating each of the computers he has accessed at any given time. Under the broad contractual theory of authorization, however, *any* violation of the terms of service or terms of use of *any* computer a person accesses violates the statutory prohibition on unauthorized access.

State v. Allen provides a notable example of a court harnessing constitutional objections to narrow the scope of an unauthorized access statute. In *Allen*, the Kansas Supreme Court relied on vagueness and overbreadth concerns to reject a broad statutory definition of "access" and adopt a dictionary definition instead. "We read certain

---

269 Notably, however, some courts appear willing to allow such a result in the civil context. See Intel Corp. v. Hamidi, 114 Cal. Rptr. 2d 244, 255 (Cal. Ct. App. 2001) (rejecting First Amendment challenge to rule holding defendant civilly liable under trespass to chattels theory for sending e-mails to corporate mail server), rev'd, 71 P.3d 296 (Cal. 2003) (holding trespass to chattels theory not valid when no actual impairment or damage done to computer hardware or network, employee's storage of data on employer's computers did not result in injury required to establish trespass to chattels, and employer's claimed consequential damages did not amount to an injury to support trespass to chattels theory, and holding that even assuming employer did have First Amendment right not to listen, employee did not violate that right here).

270 See *Morales*, 527 U.S. at 55.

271 See Richard H. Fallon, Making Sense of Overbreadth, 100 Yale L.J. 853, 853 (1991) ("More than fifty years after its inception, First Amendment overbreadth doctrine remains little understood.").

272 *Morales*, 527 U.S. at 56.

273 See, e.g., AOL Terms of Service, supra note 109. **R**

conduct as outside a statute's scope rather than as proscribed by the statute if including it within the statute would render the statute unconstitutionally vague,"[274] the court wrote. "Consequently, although [the Kansas computer crime statute] defines 'access,' the plain and ordinary meaning should apply rather than a tortured translation of the definition that is provided."[275] Although the *Allen* court opted to narrow the scope of "access" rather than "without authorization," its approach also could be used to narrow the scope of "without authorization" to the circumvention of code-based barriers to access.[276]

D. The Need for Criminal Laws on Damaging Computers and Database Abuse, and the Limits of Exceeding Authorized Access

At this point, the reader may wonder whether the approach I propose is not too narrow. After all, many types of computer misuse other than circumvention of code-based restrictions may deserve punishment. For example, Sam Fugarino deserved punishment for deleting his employer's files, even if under the offered approach he did not access his employer's computer without authorization. Similarly, we reasonably may conclude that, in at least some cases, employees should be prosecuted for misusing sensitive databases. For example, some might conclude that Richard Czubinski should be guilty of a crime for misusing the IRS tax return database.

If we say that these accesses are not without authorization, does it mean that the criminal law necessarily will permit such conduct? No. Unauthorized access statutes should be only one of several computer crime statutes in a legislative arsenal. Unauthorized access statutes effectively address computer misuse that exceeds privileges. As Part I explained, however, the problem of computer misuse extends beyond acts exceeding privileges to acts that interfere with others exercising their own privileges. Many of the harms in computer crime cases involve the latter types of harm rather than the former.

---

274 State v. Allen, 917 P.2d 848, 852 (Kan. 1996).

275 Id.

276 Whether the *Allen* court opted to narrow either "access" or "without authorization" to avoid vagueness difficulties was essentially an interpretive choice, perhaps one framed by the litigating parties rather than the court. The *Allen* court understood the need to narrow "access" because it presumed a broad reading of "without authorization." See id. However, the court could have envisioned a need to narrow "without authorization" by first arriving at a broad construction of "access." Thus, Allen's act of dialing the access number to the Bell computer could have been seen as an access, but an access with authorization because the mere act of dialing the computer did not circumvent a code-based barrier.

While it is possible to construe unauthorized access statutes broadly to encompass misuse that denies privileges, the better approach is for legislatures to enact statutes that prohibit the willful destruction of computer files without the owner's permission. For example, in *Fugarino*, the defendant's harmful act was interfering with his employer's business; by deleting his employer's files, Fugarino ensured that the business and its employees would be unable to exercise their usual privileges of using the files. The *Fugarino* court apparently reasoned that this was an unauthorized access because the destruction was unauthorized, and to destroy the files, Fugarino had to access the computer that hosted them. But Fugarino's crime was not really unauthorized access; it was willful destruction of his employer's files with the intent to deprive the employer of their use.

Congress enacted an intentional damage statute to complement the federal unauthorized access statute in 1986.[277] Codified at 18 U.S.C. § 1030(a)(5), this statute in its current form states that whoever "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer"[278] commits a federal felony. The statute defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information."[279]

This provision complements the unauthorized access language more commonly used in computer crime statutes, and adds protection against interference with others' privileges in a way that supplements unauthorized access statutes that address exceeding privileges. An arguable flaw with this federal damage statute is that it uses the same phrase, "without authorization," that unauthorized access statutes use, but in a very different way. In the unauthorized access statutes, the access is without authorization; in the federal damage statute, it is the causing of damage that is without authorization. Thus the damage statute uses the phrase "without authorization" to mean merely "without permission," and should use the latter phrase instead. With that caveat in mind, however, the federal damage statute adds a very important weapon to the arsenal of computer crime statutes. States should enact similar provisions, and courts should interpret unautho-

277 See 18 U.S.C. § 1030(a)(5)(A) (1986) (current version at 18 U.S.C. § 1030(a)(5)(A) (2000)). Congress intended that this statute would be used "to penalize those who intentionally alter, damage, or destroy certain computerized data belonging to another." S. Rep. No. 99-432 at 10 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2488.

278 18 U.S.C. § 1030(a)(5)(A) (2000).

279 18 U.S.C. § 1030(e)(8).

rized access statutes while mindful of the existence of computer damage statutes.

Database protection statutes should provide the second supplement to unauthorized access statutes. Such statutes could address the problem of insiders who misuse their access to sensitive databases, especially in the context of government employment. The prohibition should be narrow. For example, a law designed to protect federal government databases from insider abuse might make it a crime for a federal government employee intentionally to obtain information from a particular type of sensitive database for reasons unrelated to the scope of their employment, or in violation of an official policy.[280] Such laws could focus specifically on a particular class of individuals who breach particular contractual provisions to obtain specific types of information—a prohibition much narrower than unauthorized access statutes that in theory apply to any access by any person to nearly any computer. The approach achieves the intuitively correct result in cases like *Czubinski*, without drawing the average user into the realm of possible criminal sanction.

One doctrinal objection to this proposal is that federal law arguably already attempts to protect these interests through prohibitions on "exceeding authorized access" to computers. As I mentioned earlier, the prohibition on exceeding authorized access appears to have been directed at misuse committed by insiders, those with preexisting rights and privileges.[281] Precedent exists to support the view that this prohibition covers breach of contractual restrictions by otherwise-legitimate users.[282] Such an interpretation is not inevitable, however, and should be avoided. It is not entirely clear whether the prohibition on exceeding authorized access was designed to cover breaches of contract-based restrictions, or was designed merely to

---

[280] Virginia has enacted a computer invasion of privacy statute that adopts one of these limitations, focusing on the types of information obtained. See Va. Code Ann. § 18.2-152.5 (Michie 1996). The statute states:

> A person is guilty of the crime of computer invasion of privacy when he uses a computer or computer network and intentionally examines without authority any employment, salary, credit or any other financial or personal information relating to any other person. "Examination" under this section requires the offender to review the information relating to any other person after the time at which the offender knows or should know that he is without authority to view the information displayed.

Id. This statute is quite poorly drafted, but it has been used to convict at least one government employee who abused sensitive government databases, though that conviction was reversed. See Plasters v. Commonwealth, No. 1870-99-3, 2000 WL 827940 (Va. Ct. App. June 27, 2000).

[281] See supra notes 157-59 and accompanying text. **R**

[282] See, e.g., EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58 (1st Cir. 2003); S. Rep. No. 99-432, at 7-8, reprinted in 1986 U.S.C.C.A.N. 2479, 2485-86.

ensure that owning an account on a network did not excuse a person from liability if he hacked into the network to exceed his network privileges.[283] In other words, it is not clear whether "exceeding authorized access" governs an insider who breaches contract-based restrictions or an insider who circumvents code-based restrictions.

To the extent that existing legal materials do not settle this question, considerations of policy favor the latter interpretation. Statutes prohibiting acts of exceeding authorized access tend to be quite broad. For example, the federal law codified at § 1030(a)(2)(C) makes it a crime to exceed authorized access to essentially *any* computer connected to the Internet.[284] If we interpret the phrase "exceeds authorized access" to include breaches of contract, we create a remarkably broad criminal prohibition that has no connection to the rationales of criminal punishment.[285] The better approach is for legislatures to enact new criminal statutes focused directly at the problem of employee database abuse.

E. Examples

I will conclude with several examples that illustrate how my proposal would work in practice. Each example starts with a fact pattern in italics, and then applies the proposed standard in the nonitalicized portion that follows.

---

[283] For example, imagine that employee *A* steals employee *B*'s password, accesses *B*'s account, and reads *B*'s e-mail. Arguably this is a case of "exceeding authorized access"—*A* had some authorization to use the company server, but exceeded his authorized access by viewing *B*'s e-mail on the computer. Under this approach, "access without authorization" would apply to the circumvention of code-based restrictions by users without any privileges to access the network, and "exceeding authorized access" would apply to the circumvention of code-based restrictions by those who did have preexisting rights. One of the difficulties with this approach is that it places great importance on the tricky question of defining the scope of a computer, which as I noted supra note 149, can be quite difficult in the context of a network. For example, if a company has a webserver that the public can access, does that mean that outsiders have rights to access the company's computer, and become insiders who can be punished only through prohibitions against exceeding authorized access? Does the picture change if the webserver resides on a different physical box than the mailserver, and the outsider only hacks into the mailserver? R

[284] The section punishes "[w]hoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer if the conduct involved an interstate or foreign communication." 18 U.S.C. § 1030(a)(2)(C) (2000). The term "protected computer" is defined extremely broadly to include essentially every computer connected to the Internet: Any computer qualifies that "is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B).

[285] This rationale matches the rationale for not having an overly broad interpretation of "without authorization." See supra Part III.C.

Password guessing: Joe fears that his girlfriend is cheating on him, and he wants to see what is in his girlfriend's e-mail account. Joe logs on to her ISP, enters in her username, and starts guessing passwords. Joe finally guesses correctly on his eleventh attempt, and then reads his girlfriend's private e-mail messages. Under my proposal, by visiting the ISP and guessing combinations of usernames and passwords, Joe did not access the ISP's computer without authorization, although Joe would be guilty of an attempted unauthorized access.[286] Joe did access the computer in his first ten visits, but that access was not without authorization. However, the access that occurred when Joe typed in the correct password after his eleventh attempt *was* unauthorized. That access occurred under false identification: The computer "believed" that Joe's girlfriend had entered in the password (or had authorized Joe to do so), rather than Joe himself. Because false identification circumvents regulation by code, it triggers lack of authorization, and Joe's access violated the prohibition against unauthorized access.

Employee looking to leave: Fred is an employee at a pharmaceutical company who wants to start a competing business. Before Fred quits, he spends a few hours looking through his employer's computer network, and then copies specific files on to diskettes that he takes with him when he leaves. Fred has accessed his employer's computers, but as an employee he has authorization to do so. Therefore Fred has not violated an unauthorized access statute. Fred still can be prosecuted for any traditional crime he may have committed, of course, such as theft of trade secrets[287] or interstate transportation of stolen property.[288] But the fact that Fred took the information from a computer rather than a file cabinet makes no difference to Fred's criminal liability.

Employee sabotage: Sam is a computer programmer who is angry at his employer for denying him a promotion. Sam decides to take revenge by deleting some of his employer's important files, and by launching a denial-of-service attack that overwhelms his company's

286 Under 18 U.S.C. § 1030(b), attempts to access a computer are prohibited in the same way as the completed offense. See id. ("Whoever attempts to commit an offense under subsection (a) of this section shall be punished . . . .."). Of course, state provisions may vary.

287 See, e.g., United States v. Martin, 228 F.3d 1 (1st Cir. 2000) (affirming conviction for theft of trade secrets under 18 U.S.C. § 1832(a) of employee who e-mailed his employer's secrets to business competitor).

288 See, e.g., United States v. Farraj, 142 F. Supp. 2d 484 (S.D.N.Y. 2001) (allowing prosecution for interstate transportation of stolen property in violation of 18 U.S.C. § 2314 for law firm employee who e-mailed part of firm's trial strategy to opposing counsel with offer to sell rest for $2 million).

webserver with requests and takes it offline for a few hours. The deletion of the files will not constitute an unauthorized access. Sam accessed his employer's computer when he used it to delete files, but as a programmer he was authorized to access those files and therefore has not committed access without authorization. Similarly, the denial-of-service attack will not itself constitute an unauthorized access crime. Sending the data to the computer does access the computer, but the access is not without authorization: The webserver has been configured to accept all web traffic requests, such that sending many requests will not circumvent any code-based restrictions.[289]

Sam does not avoid criminal liability, however. The deletion of the files may constitute destruction of property or conversion and, depending on the applicable state laws, he could be prosecuted under general property crime statutes.[290] Sam could also be prosecuted for damaging the computer under the federal computer damage statute, 18 U.S.C. § 1030(a)(5)(A)(i).

Employee with free time: Jane is bored at her job, and spends a few hours a day at work surfing the web and e-mailing her friends. The computer use policy at Jane's workplace states that personal use of company computers is strictly prohibited. Jane accessed her employer's computers, but that access was not without authorization because it breached a regulation by code but did not circumvent a code-based restriction. While Jane's personal use disregarded company policy, it did not violate the intended function test of *Morris*, or the false identification rule. Jane may lose her job or receive a reprimand from her boss, but she cannot be prosecuted under computer crime laws.

E-mail virus: George writes a computer virus to be distributed as an e-mail attachment. When a recipient clicks on the attachment, the program launches and sends out e-mails to every address in the recipient's address book. George sends out the virus, and it infects tens of thousands of machines. These facts present difficult questions for unauthorized access statutes, although not for computer damage statutes. George accessed the computers to which he directly distributed the virus because the computer accepted the e-mail he sent. This access did not lack authorization, however, as George used e-mail as it was intended to be used (at least so far). But how should the law treat a recipient clicking on the attachment and distributing the virus to other computers? Did George access the recipient computer *again* at

289 Notably, however, if Sam launches his attack using distributed "zombie computers" that have themselves been compromised, the act of compromising the zombie computers would constitute separate accesses without authorization.

290 See generally LaFave, supra note 30, § 8.6(b). **R**

that point, or did the recipient access the computer, or did no second access occur? These are tricky questions. If George accessed the computer again, the access is unauthorized under the *Morris* intended function test: George used an attachment feature designed to show the user a file as a means of executing a command to spread a virus.

On the question of access, the answer depends in part on whether we construe access as a result (in the sense of a user causing an access to occur) or as an act (in the sense of a user accessing the computer).[291] If we see it as the former, then George probably did cause an access to occur: Under traditional criminal law principles, George's conduct was likely the proximate cause of the unauthorized access and George violated the statute.[292] Admittedly, however, whether these facts present an access without authorization is not entirely clear. If access signifies an act, then the recipient caused the access to occur, not George. Of course, as I suggested earlier, the government can bypass these questions by prosecuting such a case under the existing computer damage statute, which clearly would reach George's conduct, rather than an unauthorized access statute.

Wireless networks: A local hospital uses a wireless network. Jennifer finds that if she stands outside the hospital's entrance she can access the network using her laptop computer. Although she does not have an account, Jennifer uses the hospital's network to browse patient files stored on the hospital's server. Wireless networks raise particularly difficult questions for interpreters of unauthorized access statutes. Once again, access is the easy part, and the difficult question is when that access becomes access without authorization. Here the code-based restriction presumably includes the network's encryption scheme. Under this approach, access is without authorization only if the user bypasses the wireless network's encryption scheme. If the hospital left the network open and unencrypted, however, use would not be circumventing a code-based restriction and could not be without authorization.

---

291 Here I am using the Model Penal Code's distinctions between acts, results, and attendant circumstances. See Paul H. Robinson & Jane A. Grall, Element Analysis in Defining Criminal Liability: The Model Penal Code and Beyond, 35 Stan. L. Rev. 681, 694-99 (1983).

292 Under most formulations of proximate cause, an act *A* is a proximate cause of result *B* if, "but for" *A*, *B* would not have occurred, and *B* is a foreseeable result of *A*. See Joshua Dressler, Understanding Criminal Law 187-96 (2001) (discussing proximate cause). In this case, the act of sending out the virus as an e-mail attachment made the spread of the virus a foreseeable (and even intended) result.

CONCLUSION

Substantive criminal law has a long tradition of remaining surprisingly undertheorized. As Professor Kadish has noted, criminal law has often been "archaic, inconsistent, unfair and unprincipled, . . . saved from disaster only by the sensible exercise of discretion by prosecutors and judges."[293] Even foundational concepts such as mens rea remained poorly understood for centuries, awaiting the Model Penal Code's masterful treatment of the concept that did not arrive until 1962.[294] Given this tradition, perhaps it is not surprising that the recently-enacted computer crime statutes lack a clear conceptual basis. Courts have struggled to apply computer misuse statutes much like courts have struggled with criminal law concepts such as mens rea, mistake, and impossibility.[295] Perhaps the difficulty that courts have encountered with concepts such as "access" and "authorization" present the rule, not the exception. Given the high-technology atmospherics of the fact patterns and the rapid advances in computer technology, confusion over the purpose and scope of the statutes may have been inevitable.

This Article has used two primary tools to advance a new understanding of how courts should interpret computer crime statutes. The first tool is a basic appreciation of computer technologies, combined with an eye towards reconciling the contours of the technology with the contours of the applicable law. Thus, the technology itself reveals the basic distinction between regulation by contract and regulation by code, offering a principle that the criminal law can harness to interpret the scope of computer crime statutes. Similarly, technological changes during the last two decades illustrate the difficulty of using the concept of "access" as a significant limiting principle. The common theme raised by these two insights is that focus on the technology can help point the way toward more enduring legal principles less likely to prove arbitrary in the future.

The second primary tool that I have used is analogy to questions of criminal law that have arisen in the interpretation of longstanding criminal prohibitions such as burglary, trespass, rape, and theft. This Article has approached the interpretation of computer crime statutes as a problem of criminal law rather than as a problem of "cyberlaw."

---

293 Sanford H. Kadish, Fifty Years of Criminal Law: An Opinionated Review, 87 Cal. L. Rev. 943, 947 (1999).

294 See id. at 952-53 (discussing impact of Model Penal Code's mens rea provisions on understanding of mens rea within criminal law).

295 See, e.g., People v. Thousand, 631 N.W.2d 694, 697 (Mich. 2001) ("[C]ourts and scholars alike have struggled unsuccessfully over the years to articulate an accurate rule for distinguishing between the categories of 'impossibility.'").

I have tried to explain the existence of specialized computer crime statutes based on the structural difficulties courts encountered when applying existing property crimes to computer misuse. And more importantly for the future, I have attempted to show that courts have developed limiting doctrines, such as the distinction between fraud in the factum and fraud in the inducement, that narrow the scope of traditional crimes that contain an element such as lack of consent or authorization. The same doctrines could be used to impose analogous limitations on the scope of computer crime statutes. The common aspiration is to understand computer crime statutes by looking for similarities and occasional differences between the new statutes and existing problems, rather than approaching the new statutes as sui generis enactments.

More broadly, this Article suggests that the traditional principles of criminal law still provide a powerful tool to understand unauthorized access statutes. The facts of computer crime cases seem new at first, but once understood, they tend to reveal familiar dynamics that criminal law has faced in the past. The basic mechanics of accessing a computer without authorization resemble the basic mechanics of existing crimes that protect the security and privacy of property and person. The facts are new, but the concepts need not be, and they may provide the key to correcting expansive interpretations of the new statute. The most useful guide to interpreting the newest statutes may be found in the past.