ARTICLE: CYBERCRIME'S SCOPE: INTERPRETING "ACCESS" AND "AUTHORIZATION" IN COMPUTER MISUSE STATUTES
78 N. Y. U. L. Rev. 1596, November, 2003
Orin S. Kerr
…
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; the final state to enact a statute was Vermont in May 1999. 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. 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. 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 combining 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. For example, one crime prohibits unauthorized access to government computers, another prohibits unauthorized access to computers that results in damage, and a third prohibits unauthorized access or exceeding authorized access to computers such that the user obtains private information.

But what does the trigger of unauthorized access mean? What exactly do these statutes prohibit? … 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. We could say 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. 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. 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. 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. Another 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. 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.

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. 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.

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. The statutes also require that the trespasser knows that she is without license or privilege to enter or remain on the premises. 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. " Once connected to the Internet, she 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 are silent on these questions: The phrase "without authorization" generally is left undefined.

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. … Perhaps the most comprehensive discussion of "access" appears in a Kansas Supreme Court case from 1996, State v. Allen. 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. 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. Allen was charged with accessing the Bell computer without authorization in violation of the Kansas computer crime statute.

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, 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. " The court responded that this definition was so broad that if taken seriously it would render the statute unconstitutionally vague. If "access" really meant "to approach," the court noted, "any unauthorized physical proximity to a computer could constitute a crime. " 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. " 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.

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

A federal district court suggested a similar approach in Moulton v. VC3, a civil dispute between two computer security companies. The Moulton case harnessed a civil remedy added to the federal computer crime statute in 1994 to provide additional protection for computer misuse victims. 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. 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.

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. 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. 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" essentially identical to that in the Kansas statute from Allen. 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 "approaching" or "otherwise making 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.

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) This case is one of several civil cases brought by AOL against spammers, senders of bulk unsolicited commercial e-mail. 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. 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, 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. " "Access," 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.

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.

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; 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.

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.

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. 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"; 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. 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. Morris was charged with violating 18 U. S. C. 1030(a)(5)(A), which at the time prohibited "intentionally accessing a Federal interest computer without authorization" if damage resulted. 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 accounts. 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. " Some unauthorized access statutes prohibit only access without authorization; others prohibit both access without authorization and access that exceeds authorization. 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. 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). 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 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. 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.

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. However, Morris based his appeal solely on the question of authorization. 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.

The Second Circuit rejected Morris's argument. While statutes that only prohibited access without authorization may have been "aimed" 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.

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. " 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. "

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, 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. , 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 plaintiff's employees, including an employee named Eric Leland who had access to the plaintiff's confidential business plan and other trade secrets. 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 accessed [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. 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. " 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. " 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. " 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. 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 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, 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" 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. 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. Sam Fugarino was a computer programmer whose behavior at work became increasingly bizarre. When Fugarino learned that another employee had been hired at the 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. '" Fugarino then started deleting sections of code from the employer's network. 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. "

On appeal following his conviction, Fugarino argued that his conduct was not knowingly without authority. The Georgia court disagreed. Fugarino lacked authority because "the owner of the company . . . did not give Fugarino

authority or permission to delete portions of the company's program. " 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. 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 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. Olson was tried and convicted of accessing a government computer without authorization in violation of Washington's computer trespass statute. On appeal, he argued that his access was not explicitly unauthorized.

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. " 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. 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. 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. " 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. " The court disagreed, reasoning that as a system administrator, Briggs was in fact authorized to access his employer's computer. 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 authorized access, something that the Maryland statute did not prohibit). 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. 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. " 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. Explorica used the scraper twice, enough to allow it to learn and then undercut EF's tour prices, all unbeknownst to EF. 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 either without authorization or by exceeding authorized access. The district court agreed, reasoning that use of the scraper was so far beyond the "reasonable expectations" of EF that it was clearly unauthorized.

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. The court reasoned that Gormley's decision to use a scraper on EF's site (as well as his help designing the scraper) 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. 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. " 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.

A district court in Virginia took a similar approach in America Online v. LCGM, Inc. , 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- mail addresses of thousands of AOL users. 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. "

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. 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) maintained by Register . com. 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. Register. com sued Verio, and moved 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. 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. 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. "Because Register. com objects to Verio's use of search robots," the court held, "they represent an unauthorized access to the [Register. com] WHOIS database. " 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. 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 "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. The user then would encounter a text-based log-in prompt, and would need to enter a username and password to proceed. 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. 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. It is one thing to 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. 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. In response to these uncertainties, legislatures enacted computer crime statutes that prohibited accessing computers without authorization, and in some cases, exceeding authorized access.

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.

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, 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. 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. ***