

U.S. Information Security Law, Part 3

Steven Robinson 2003-05-12

This is the third part of a four-part series looking at U.S. information security laws and the way those laws affect security professionals. This installment begins the discussion of information security in the public sector. Government's involvement with information security takes place in two unique contexts: criminal justice and national defense. (Of course, government agencies also have information security concerns that are analogous to those of private industry, which were considered in the first [two articles](#) in this series.) In this installment, we will look at the basics of the criminal information security law.

As we discussed in the first article in this series, the [Computer Fraud and Abuse Act](#), 18 U.S.C. § 1030 (the "CFAA") is the primary computer crime statute in the United States. The CFAA imposes criminal liability [\[1\]](#) for:

1. Knowingly accessing a computer without authorization, or in excess of authorization, and obtaining classified information;
2. Intentionally accessing a computer without authority and obtaining consumer financial information, information from any department or agency of the federal government, or information from any protected computer where access involves an interstate or foreign communication;
3. Intentionally accessing, without authorization, a non-public computer of any department or agency of the federal government that is either used exclusively for governmental purposes, or with respect to a computer that is not used exclusively for government purposes, where the conduct affects the use of that computer by or for the federal government;
4. Knowingly, and with wrongful intent, accessing a protected computer, without authorization or in excess of authorization, and by doing so, obtaining anything of value, other than the use of the computer itself (if the value of the computer use is less than \$5,000 in any one year);
5. Knowingly causing the transmission of a program, information, code, or command, and by doing so, intentionally causing unauthorized damage to a protected computer; or recklessly or negligently causing damage to a protected computer by intentionally accessing that computer without authorization or in excess of authorization;
6. Knowingly, and with wrongful intent, trafficking in user names, passwords or other access credentials through which a computer may be accessed without authorization, if

that conduct affects interstate or foreign commerce or if the computer is used by or for the federal government; or

7. With the intent to extort money or anything of value from any person, firm, association, educational institution, financial institution, government entity, or other legal entity, transmitting in interstate or foreign commerce any communication containing a threat to damage a protected computer [2].

There is not much question that the conduct described above is antisocial and destructive and that criminalizing it is rational public policy. That said, these provisions reflect the issues inherent in criminalizing the abuse of computers and systems.

Criminalizing the Abuse of Computers and Networks - Issues

The term "computer crime" may be used in two senses. In one respect, it means the use of computers as the means to a criminal end; basically, computers as high-tech burglars' tools. The other sense of the term "computer crime" involves computers and information technology systems as the targets of destructive or disruptive behavior that is criminalized as a matter of public policy. The provisions of the CFAA summarized above prohibit both types of computer crime.

Shortly after the 1996 amendments to the CFAA, some commentators questioned whether there was any need to legislate separately against the sort of computer crime in which computers are the means to a criminal end [3]. After all, when the CFAA was passed, espionage, the theft of money and property, and fraudulent schemes had long been illegal regardless of how they were committed. It seemed redundant to enact another statute prohibiting already criminal conduct to apply solely when that conduct was committed using computers.

Computer and violent crimes impose different social costs [4]. In any event, Congress made the policy decision that separate, specific prohibitions of computer-mediated crime were required, and there is an important benefit that flows from that decision. Consider a hypothetical theft from a bank by a criminal who hacks into the bank's system. Under current law, charging this crime involved a violation of both the federal bank larceny statute and the CFAA [5]. But in theory, the use of a computer could be punished as part of the bank larceny statute, as an aggravating factor that increases the applicable sentence for theft from a bank. This is the method that the federal bank larceny statute uses to punish assaults or homicides committed in

the course of a bank robbery [6]. This leads to charging a computer mediated bank larceny as one crime rather than two. This is, as the commentator cited above might agree, a neater and more logical approach as an academic matter. Theft from a bank is always a crime, and when the theft is mediated by a computer, the punishment would be enhanced accordingly.

But in practice, it is entirely possible that the evidence against a defendant accused of a computer mediated theft would support a determination of guilt beyond a reasonable doubt as to unauthorized access to a computer, but fail to provide sufficient proof as to a theft or attempted theft. In such cases, without a separate prohibition of the computer abuse, the defendant would be acquitted. If the underlying theft offense cannot be proven, the aggravating factor would arguably be irrelevant, in at least some cases. So, by enacting a separate provision for computer abuse, the Congress put a statutory scheme in place under which the criminal use of computers could be charged independently of the substantive offenses that the computers were used to commit. This approach increases the probability that criminal use of computers would be punished, even when proof of the substantive offense is lacking.

Of course, when the conduct to be prohibited is harmful to computers, systems, or data, the need for specific prohibitions is much clearer. Although, in theory, intrusion into a computer system can be analogized to the common law crime of trespass (an unauthorized intrusion into physical premises), the obvious fact that an electronic intrusion may occur with no physical manifestations means that that analogy has limitations, and that electronic "trespass" might be difficult to prove. Similarly, unauthorized access to or copying of data can be analogized to theft, but common law theft requires the taking of property. There are problems under the law of some states in treating data and property as equivalent, and it is by no means clear that making a copy or accessing information is a "taking", as that term is ordinarily used or as it is defined at common law.

Apart from variations in state laws in terms of definition, the variations in penalties and procedures among the states do not constitute an adequate response to the problem of either electronic intrusion onto systems that affect interstate and foreign commerce or the related risks to the data they contain. To address unauthorized electronic access to and copying of data with a consistent, predictable approach that protects Internet-based activity (that is, activity that takes place across and regardless of state lines), national uniformity was required, and in the United States, that means federal legislation. The CFAA, the Electronic Communications Privacy Act (18 U.S.C. §§ 2510-22 and §§ 2701-12), the Digital Millennium Copyright Act (17 U.S.C. §1201- 05), the No Electronic Theft Act (amending 17 U.S.C. §§ 101, 506-07 and 18 U.S.

C. §§ 2319-2320), and the Economic Espionage Act of 1996 (18 U.S.C. §§ 1831- 1839), all expanded the prior criminal law at the federal level to address various destructive uses of information technology.

Applying the CFAA: United States v. Lloyd

Let's look at how the CFAA was applied in a scenario that is of particular concern to information security professionals. [United States v. Lloyd \[7\]](#) involved the disabling of the computer system of Omega Engineering Corporation (hereafter referred to as "Omega"), by Timothy Lloyd, who had worked at Omega since 1985 as its only computer system administrator. The prosecution's case was that in 1994 or 1995, Lloyd became physically and verbally abusive to fellow employees. Lloyd was transferred to a position in what proved to be an unsuccessful attempt to improve his performance. In June 1996, Lloyd instituted a "clean up" policy that involved the removal of files from individual computers, the prohibition of individual backups, and transfer of certain safety-related software from individual computers to Omega's file server. Several managers became concerned that Lloyd had acquired too much control over Omega's system, and he was asked him to provide those managers with access to file server. Lloyd never did so.

After another incident of bad workplace conduct, Lloyd was fired without notice and escorted from Omega's premises on July 10, 1996. On July 31, 1996, Omega's file server did not boot, and it subsequently became apparent that more than 1,200 programs had been lost and purged, meaning that the files had been deleted and were unrecoverable. At trial, experts testified that the purge had been intentional and could only have been accomplished by someone with the level of access that Lloyd had. Lloyd was the only person at Omega who had that level of access. Expert testimony supported the implication that Lloyd had programmed the mass deletion of data to occur the first time that anyone attempted log on to the server after July 30, 1996, referring to the commands in question as a "time bomb." There was evidence indicating that Lloyd had tested the "time bomb" on several occasions prior to his termination.

The defense disputed essentially every material aspect of the prosecution's case, but after three days, the jury convicted Lloyd of one count of computer sabotage in violation of 18 U.S.C. § 1030 (a)(5)(A). As such, the CFAA imposes criminal liability in one of the most disturbing situations that information security professionals confront: the disgruntled, technologically sophisticated employee who is prepared to take out his or her frustrations on an employer's systems.

Sentencing for Computer Crimes

Sentencing for computer crimes requires some interesting departures from the approach taken under pre-information age criminal law. Sentences for theft are often graduated according to the value of the money or property taken or the level of violence with which the theft was committed. Neither concept works well with respect to computer crime. A very serious computer crime compromising government or industry secrets may involve a breach of security with respect to only a small amount of data. Accordingly, sentences under the CFAA are graduated in terms of the state of mind of the perpetrator and the type of information taken. A comparison of two provisions of the CFAA illustrates this approach clearly:

Offense	Punishment
<p>Whoever intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage. 18 U.S.C. § 1030 (a)(5)(c) (emphasis supplied).</p>	<p>1st Offense or Attempt: Imprisonment for not more than one year, fine, or both. 18 U.S.C. §1030 (c)(2)(A). Subsequent Offense or Attempt: Imprisonment for not more than ten years, fine, or both. 18 U.S.C. §1030 (c)(3)(B).</p>
<p>Offense: Whoever having knowingly accesses a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government ... to require protection against unauthorized disclosure for reasons of national defense or foreign relations, ... with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered,</p>	<p>1st Offense or Attempt: Imprisonment for up to 10 yrs., fine or both. Subsequent Offense or Attempt: Imprisonment for up to 20 yrs., fine, or both. 18 U.S.C. §1030 (c)(1).</p>

or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it." 18 U.S.C. § 1030(a)(1)(emphasis supplied).

It is important not to overstate the role of the CFAA as the "primary" computer crime statute in the United States. As noted above, a number of federal statutes criminalize conduct involving information technology systems that violates intellectual property or privacy rights or is otherwise destructive. In addition, computers can be used as tools to commit a wide variety of crimes under state or federal law. The CFAA remains a good starting point for the consideration of such issues, but that should not be taken to mean that other federal or state laws are of less use. The applicability of state and federal law in the criminal context depends, as it generally does, on the facts of each case.

Information Security and Criminal Investigations

There is, of course, a third aspect of the relationship between computers and criminality. In addition to the prospect that computers may be either the tools for or the targets of criminal activity, computers store information, and some of that information may be evidence of criminal activity. The legal framework for how investigators acquire such evidence is beyond the scope of this series, but it involves both compulsory means (warrants and subpoenas) and voluntary cooperation. It is essential that information security professionals consult their legal counsel as to what they must do and what they may do in response to investigations. Moreover, there are business issues associated with voluntary cooperation that are not typically resolved by either information security professionals or legal counsel, although both should have a role in advising the pertinent business decision makers. For a brief overview of some of the issues involved in these situations, readers are referred to the SecurityFocus article [Incident Management with Law Enforcement](#).

Conclusion

The discussion of information security in the public sector will continue in the next installment, when we look at the law of information security as it applies to national security.

References

[1] The CFAA also imposes civil liability for the conduct described. 18 U.S.C. § 1030 (g). The civil aspects of the CFAA were discussed in Article 1 of this series.

[2] 18 U.S.C. §§ 1030 (a)(1)-(7).

[3] Olivenbaum, Joseph M., : Rethinking Federal Computer Crime Legislation, 27 Seton Hall L. Rev. 574 (1997).

[4] A theft by computer does not involve a threat of physical violence. That arguably lowers and changes the social cost of a theft committed using a computer, rather than by means requiring a physical confrontation. That said, theft by computer may not be perceived as such. It may not be immediately apparent that a crime has occurred. Consider a computer-mediated theft of money from a bank. The first thing that would arguably be noticed is that funds have disappeared from one account and been transferred elsewhere. It may not be immediately possible to distinguish between an erroneous or improperly documented transfer, bad enough but arguably not illegal, and a theft. The expense of the resources required to make this determination are additional costs of computer crime. In addition, the time required to make that determination may give the thief an additional opportunity to abscond, destroy, or alter evidence. That makes computer mediated crime inherently more difficult to detect, investigate and punish than the same crime committed by less technologically sophisticated means.

[5] 18 U.S.C. § 2113 (bank larceny); 18 U.S.C. § 1030 (a)(4).

[6] 18 U.S.C. §§ 2113 (d)&(e).

[7] 269 F. 3d 228 (3rd Cir. 2001); <http://www.ca3.uscourts.gov/opinarch/002409.txt>

[Privacy Statement](#)

Copyright 2006, SecurityFocus