Online Ethics Center
FOR ENGINEERING AND SCIENCE

Government: Cops on the I-Way

Author(s)

Anonymous

Description

An article detailing the increasing use of computers to help commit crimes, and the relation of such crimes to the David Lamacchia case.

Body

Computer crimes are becoming more daring and imaginative.

By Mike Godwin

***ATTENTION** - The FORMAT of the following article has been modified from its original appearance for ease of reading. No content or information has been removed from this article.

Here's the plot: short of cash but endowed with a wealth of computer skills, a clever employee is able to reach inside the boss's private data base and "kidnap" invaluable company secrets by locking them with a sophisticated encryption program. She then sends an anonymous electronic ransom note demanding a wire transfer of $3 million to a blind account in the Cayman Islands - or the boss's proprietary data will be lost forever.

Extortion - in this case hypothetical - is only one of the many imaginative, daring and increasingly publicized crimes that have gone high tech in recent years. In addition to the predictable tax, insurance and credit-card scams, software infringements and

eavesdropping, the computer is now the site of crimes that range all the way up to homicide. "Law enforcement is becoming aware that computers can be used to facilitate just about any type of crime," says Jack King, legal editor of the Bureau of National Affairs Criminal Practice Manual.

One of the most emotion-raising illegal activities is the occasional use of the Internet and online services by pedophiles, who can not only transmit child-pornography images but also have been known to use the Net to make assignations with youngsters. As for homicide, while it's hard to imagine that someone could actually be killed online, police in a Pennsylvania murder-kidnapping case found critical evidence, including a ransom note, on the defendant's computer. The computer can also be a tempting conduit for anonymous threats; the Secret Service tracked down one perpetrator who sent a threat to President Clinton's well-known E-mail address.

Computer crimes are hardly new. In California prosecutors have been pursuing high-tech crime in Silicon Valley for a couple of decades. But the focus and nature of the crimes have changed dramatically. When the Department of Justice set up a computer-crimes unit in September 1991, it was intended to cope primarily with threats to computer security posed by hackers, toll-fraud artists and electronic intruders. But the new crimes, says Jim Thomas, a criminology professor at Northern Illinois University, "aren't simply the esoteric type they were five years ago." They are "computer crimes," he adds, "only in the sense that a bank robbery with a getaway car is an "automobile crime.' " And computers are fast approaching the ubiquity of automobiles.

The ever richer variety of criminal activities has had law-enforcement officials scrambling - largely because neither the laws nor the enforcement structures were designed to deal with them effectively. A recent case that illustrated this was watched closely by just about everyone in the computer world. It was that of David LaMacchia, an M.I.T. undergraduate who was charged last April with conspiring to distribute millions of dollars' worth of illegally copied commercial software over the Internet. LaMacchia allegedly set up and ran an online bulletin board that allowed anyone who accessed it to copy for free a variety of software programs. Touted as the largest single instance of software piracy ever uncovered, LaMacchia's case was thrown out last December by Massachusetts Federal Judge Richard Stearns, who decided that the senior from Rockville, Maryland, had in fact committed no crime at all. In January U.S. Attorney Donald Stern announced that he would not appeal the decision.

The Copyright Act, which covers software as well as tangible commodities like books, records, tapes and film, did not specifically criminalize LaMacchia's alleged conduct because he did not benefit from the venture. Instead, the feds chose to indict him on a charge of conspiracy to commit wire fraud. That was not a particularly good fit either, but government officials felt they had to charge him with something. "If the government did not respond when someone gave away a million dollars in software," says Scott Charney, who heads the U.S. Justice Department's computer-crimes unit, "we'd essentially be saying that you can give away software as much as you want."

Protecting the rights - in fact the livelihood - of commercial software makers is only one of many challenges facing authorities as they try to police cyberspace. Tricky legal issues abound, such as the admissibility of computer evidence. And law enforcers are often inadequately prepared for the tasks. As a result, more and more federal agents at the FBI Academy in Quantico, Virginia, and at the Federal Law Enforcement Training Center in Glynco, Georgia, are being trained to deal specifically with the complex issues involved in computer crime.

Shadowing every issue is the need to balance law enforcement with the constitutional rights of the burgeoning population of Internet users in the U.S. as they communicate in a universe without borders. One of the chief problems, for example, is how to write a search warrant for computer evidence. Warrants for physical evidence are relatively easy, but finding the "location" of computer evidence on a network - or on the Internet - can be downright metaphysical. Is the evidence really on this computer terminal, or is it being accessed from a hard disk in another state? In addition, searching a computer bulletin-board system with two gigabytes of data on it may require agents to spend weeks scanning through irrelevant material to find what they want. Last year Charney co-authored a set of federal guidelines for searching and seizing computers, designed to provide answers to some of these questions.

Authorities are also concerned about the adequacy of current laws in dealing with computer and network crime. While most states now have some kind of computer-crime laws, those laws often go uninvoked, largely because such crimes are still rare and prosecutors have little experience with them. To circumvent this problem, Massachusetts Governor William Weld recently signed into law a set of amendments that integrate computer crimes into existing criminal statutes.

Then there is the question of exactly what should qualify as a crime. The LaMacchia case, for example, illustrates a serious risk to system operators (sysops) on the Net: To what extent will they be held criminally responsible for the acts of their users? Computer networks, both public and private, have become an important forum for public discourse and activity. Laws that hold sysops responsible for their users' online actions might drive them to quit operating those forums altogether.

That outcome would be disastrous for the Internet, whose major appeal has been as a "digital space" where individuals and societies can explore freedom of expression and self-definition. That is why the fine line between legitimate deterrence and constitutionally protected speech is coming under increased scrutiny. "If you "walk the beat' on the Internet too vigorously," says the Justice Department's Charney, "you have a chilling effect on First Amendment rights." Rather than patrol the Net themselves, cybercops increasingly urge citizens to contact the FBI or the Secret Service if they learn about crimes or threats.

Law-enforcement agencies, in turn, are using the Net to help solve crimes. The FBI, for example, has begun putting requests for information about lawbreakers on its Mosaic home page, the electronic equivalent of a WANTED poster. Late last year the agency posted details of the so-called Unabomber case, a series of 14 unsolved bombing incidents in the U.S. dating back to 1978 - and offered a $1 million reward.

Constitutional rights aside, the government often feels pressure to put a lid on activities that are seen as antisocial - even when the laws don't directly address such conduct. In the LaMacchia case, civil libertarians were disturbed at what they saw as strong-arm tactics: an attempt to mold criminal law according to what the Justice Department wanted. Judge Stearns, in his decision to dismiss the case, suggested that it was up to Congress to amend the copyright laws if it wanted to encourage this sort of prosecution.

At the same time, the judge warned that interpreting the criminal law too broadly "would serve to criminalize the conduct of not only persons like LaMacchia, but also the myriad of home computer users who succumb to the temptation to copy even a single software program for private use." That, he said, was not something "that even the software industry would consider desirable."

Stearns' opinion outlines the balance of concerns that must guide any attempt to pursue law and order in cyberspace. This new jurisprudential battleground is littered with double-edged swords. While it is clearly important that the laws of this new

realm be explicit and enforceable, it is even more vital that the legal system have enough perspective and flexibility to deal with a world that is changing at fiber-optic speeds.

Notes

TIME Domestic

SPECIAL ISSUE, Spring 1995 Volume 145, No. 12

(Complete issue can be found at Time World Wide)

Rights

Resource Type

Essay

Topics

Privacy and Surveillance
Public Well-being
Security

Discipline(s)

Criminology and Criminal Justice
Information Sciences
Computer Sciences
Computer, Math, and Physical Sciences
Social and Behavioral Sciences