Should hackers spend years in prison?

Stiff penalties for computer trespassing could create a broad new class of criminal — including you and me.

By Peter Wayner

The FBI recently declared war on those pesky hackers — again. The news is filled with the story of some group known as Global Hell that is breaking into Web sites and causing mayhem. The FBI is cracking down, confiscating computers and taking names; and some hackers are actually fighting back and shutting down some government Web sites.

The press loves hackers because computer crime is something new. (I'm using "hackers" the way the media does, to describe those who get their kicks breaking into computer systems, rather than the older usage describing those who delight in difficult software coding work.) Murder, rape, drug dealing, theft and fraud continue as always, with ups and downs in their rates — but teenagers breaking into Web sites is something no one has seen before.

The problem with the war against hackers is that most of what the hackers are supposedly doing would be trivial if it weren't happening on the Internet. The typical hacker attack on a Web site isn't much different from scrawling graffitti on the outside of a building. Many attackers are just poking around — like suburban teenagers who hop a fence to jump into a pool.

All of this would be great theater and a nice distraction from the war in Kosovo if it weren't inspiring some serious reprisals in the courts — and some ominous inflation in sentencing that could wind up affecting everyone who uses computers in his or her daily life.

Wars on hackers are usually followed by calls for legislators to "do something!" and campaigns for new laws to crack down on the bad guys. The problem is that "doing something" often produces laws that treat the same action much more harshly in cyberspace than in "meatspace."

The archetype of the demon hacker is Kevin Mitnick, a young man who has spent more than four years in jail waiting for his trial. When he was arrested, Monica Lewinsky was in her last year of college. During this time, Mitnick and his attorneys have jousted with government lawyers in endless pre-trial maneuvers that seem to have ended recently when Mitnick decided to plead guilty, probably hoping to receive a sentence that would be limited to time served. But even that deal is uncertain and taking forever to evolve; meanwhile, for Mitnick it's just prison without a trial and with no bail.

Many, no doubt, see the crackdown on folks like Kevin Mitnick as a great deal for society: Information can be stolen just like anything else; surely the thieves who traffic in such goods should be locked up, just like car-jackers and muggers.

But there's also a hidden danger. The precedents that the courts set now for dealing with demons like Mitnick will also apply equally to everyone who follows. And it's not clear that the world is ready for Mitnick-like sentences for the crimes he might have committed, which remain murkily defined.

Think about it: Someone who reads another person's Rolodex is just a snoop, but someone who clicks through somebody else's Palm Pilot is hacking a computer database.

It's easy to see just how slippery the calculus of evil gets on the cutting edge of technology. 2600 Magazine, The Hacker Quarterly, recently posted letters from computer manufacturers like Sun and Motorola estimating their losses to Mitnick's alleged theft of computer source code. After Mitnick's arrest, he was said to have stolen billions of dollars of information. Some companies calculated their loss by simply listing the hundreds of millions of dollars in development cost of the software affected — that is, the cost of all the programmers, their computers and other overhead. Other companies were a bit more careful and noted that the value was difficult to judge, but that recalls of products like cell phones could be costly.

The problem is, the price tag of information is almost impossible to determine. If Mitnick did take a copy of these companies' source code, the companies weren't denied the use of it, as when a mugger steals cash. Mitnick's lawyers seem ready to point out that the companies involved didn't bother to announce an official price on what they lost to Mitnick — something that the Securities and Exchange Commission requires public companies to do if the losses are significant enough. That would have required strict accounting measures.

To make matters even cloudier, in the meantime, Sun Microsystems began giving away the source code to its operating system to students around the world. In other words, if Mitnick had only waited a few years, enrolled in a university and asked nicely, he might have been a poster boy for Sun's charity instead of a prisoner. Today, Sun is even circulating the source code to products like Java in hope of recruiting customers and snagging bug fixes. The company is practically begging people around the world to come take a look at its code.

This big change in the customs and attitudes of the software industry strains the arguments against hackers. If giving away the source code is now a "good thing" for corporations, did Mitnick and the other hackers do a smaller good thing by grabbing it ahead of time? Is Mitnick now a bit closer to being a Robin Hood instead of a demon? If Linux triumphs, will children be told tales of the dark days when the Sheriff of Notingham sat on the boards of all of the corporations and forced them to keep their source code proprietary so only the nobles could enjoy its bounty? Is it true that begging forgiveness is always easier than asking permission?

Such questions may be impossible to answer, but they illustrate just how confusing it can be in the nether-netherworld of information's hall of mirrors. As a commodity, information is fundamentally different from objects, and society has always graced it with special respect. The journalists who printed the stories about the allegedly racist words that appeared on a secret audio tape of Texaco employees looked like crusaders. But if it had been a digital tape, the reporters could be painted as hacking data compiled by a Texaco employee on Texaco time.

In the long run, society is going to have to think differently about hackers and the crimes with which they are charged. Taking information when it's printed on paper is not always bad, and there's no reason we should change this rule just because the information is stored on a computer disk. The intent of the criminal and the extent of the malice has always played a crucial role in our system of criminal justice. Many owners of things will forgive a theft if the "borrower" merely returns it unharmed. Crimes like trespassing are rarely prosecuted if someone just hops a fence and does no damage.

Computers and the Internet continue to frighten people, but prosecuting hackers runs the danger of setting nasty precedents that will begin to snare regular people, not programmers. Many convicted hackers are released from prison only to be denied the ability to use a computer or the Internet. In the past, this made it impossible for a person to get work as a programmer; today, they can't even push the order screen at McDonald's. After all, it's hooked up to a central database — who knows what havoc a hacker could wreak while punching up an order of fries?

One of the best ways to put this all in context is to take yourself back in time 100 years to the turn of the last century, when auto racing was just beginning to roar across the scene. The machines were grand in size and sound if not in speed — Emile Levassor won the 1895 Paris-Bordeaux race with his four-horsepower jack rabbit that covered the distance at an average speed of 14.9 mph. Feats of technical prowess like that frightened the world, and by 1903 the French government was shutting down auto races — or restricting the death-defying machines to a bearable 20 mph.

A few decades later, James Dean became a rebel automobile hacker who scared parents around the globe. Today, he's just another cutie pie competing with Hanson for poster space on dorm room walls. One era's demon is another's icon. Is teen idol the next stop for Kevin Mitnick?

salon.com > Technology June 9, 1999
URL: http://www.salon.com/tech/feature/1999/06/09/hacker_penalties