Do Hackers Provide a Public Service?

Verna V. Gehring

> I am sort of a gadfly . . . and the state is like a great and noble steed who is tardy in his motions owing to his very size, and requires to be stirred to life.
>
> —Plato, *Apology*

These days hardly anyone is surprised to receive a high priority e-mail message from the office information technology specialist warning that a computer virus is loose in the network. The risk of computer viruses, which hijack e-mail address books and erase drives, is now a routine part of work life. Most of us respond to office alerts with a sigh; we might turn on a quarantine protocol and perhaps mutter an oath about "hackers" before resuming our workday. Typically, news reports soon detail the extent of the damage caused by the virus, and we might later hear that a suspect has been arrested—somewhere in the world.

Media reports commonly refer to "hackers" as responsible for these exploits. After discussing some recent cases of cybercriminal behavior and legal responses, I will briefly describe the history of hackers and draw distinctions among several kinds of contemporary computer enthusiasts. After arguing that the term 'hacker' is used imprecisely and too broadly, I contend that hackers possess ethical scruples that both guide their lives and also serve the public interest.

Recent Exploits of Computer Vandals

News stories abound concerning those who illegally gain access to credit card information and go on to charge thousands of dollars, or who commit corporate espionage by computer and cost millions in lost profits. The losses caused by identity theft can be enormous, but the costs incurred by computer criminals who compromise network systems on a large—even global—scale are far more difficult to calculate. Malicious software programs are now routinely hidden in attachments to e-mail messages with subject headings—such as "The Info. You Requested" or "Hi:Check This!"—that encourage recipients to believe that the e-mails come from friends or trusted colleagues, or are worded in ways that pique the recipients' curiosity. Typically, opening the attachment enables a secret program, or "worm" to send itself to everyone in the victim's e-mail address book, spreading the virus—sometimes worldwide—and bringing network traffic to a halt. Following his arrest in December 1999, David Smith pled guilty to charges in connection with his creation of the "Melissa" virus, and he acknowledged that his program caused $80 million in damage, an estimate that reflects the time spent by systems administrators to clear the virus from affected computers.

The losses caused by identity theft can be enormous, but the costs incurred by computer criminals who compromise network systems on a large—even global—scale are far more difficult to calculate.

Perhaps inspired by "Melissa," in early 2000 the "Love Bug" virus—which one computer security expert described as "'Melissa' on steroids"—spread globally via a similar but more comprehensive e-mail piggyback system. Because the virus replaced media files with copies of itself, the damage was far more extensive—according to some estimates, in excess of U.S. $1 billion. The virus seems to have been unleashed from the Philippines, raising questions about whether the program's creator must answer only to Philippine law—which lacks a well defined area of computer jurisprudence—or whether he can be held legally accountable in other countries. Finally, computer security specialists have remarked at how few, and relatively unsophisticated, programming skills were needed for the virus to immobilize communication worldwide. The notoriety of the "I Love You" virus has encouraged copycats (such as "Joke," and "Anna Kournikova"—which entice recipients to open what they believe is a humorous attachment, or a photo of the famous tennis star), and it is unclear whether creators of one type of virus might be legally responsible for at least some of the damage caused by subsequent copycat programs.

Legal Responses

Legal responses to computer information tampering or theft are still under development. In the U.S., the FBI's National Infrastructure Protection Center is

responsible for tracking denial-of-service problems and defacement of Web sites. Both tampering and theft crimes fall under Title 18 of the United States Code, which covers damage to a computer "used in interstate or foreign commerce." The maximum penalty under the law is ten years in prison and twice the gross monetary loss to victims. Software theft and piracy are considered copyright infringement, a part of Federal law, and carry as little as $2,500 in fines or as much as three years' probation and $40,000 in fines.

To date, the person who has served the most prison time for computer meddling is Kevin Mitnick, who spent nearly five years in Federal prison for admitting to access device, wire, and computer fraud, and for intercepting electronic communications and copying confidential materials. As part of his plea bargain, Mitnick accepted the government's accusation that he caused in excess of five million dollars in damage; yet his fine was slightly above $4,000.

Congress, vexed by the imaginative activity of cybercriminals, is considering enacting new laws or changing existing ones to better protect computer technology. One proposal, for instance, would double prison sentences, allowing ten years' jail time for a first offense and twenty years for subsequent convictions. Another proposal would ease wiretap laws so that officials could more easily examine data traffic and spot illegal activity. The USA Patriot Act, a sweeping resolution passed by Congress shortly after the events of September 11 and intended to streamline detection and obstruction of terrorist activity, may increase surveillance of cybercriminal activity as well. And late in 2001, the FBI announced formation of a Cybercrime Division to investigate intellectual property, high-tech, and computer crimes. Although its organizational structure is not yet clear, this division may be part of the National Infrastructure Protection Center (an interagency group that tracks cybercrime), and primarily concerns counterterrorism measures.

"In your computer files you refer to me as a snoop."

A Brief History of Hackers, Crackers, Phreaks, and Others

Although media reports of computer vandalism commonly blame "hackers," this use is imprecise. To understand why, one must look to the history of computer enthusiasts and the lexicon they have developed to detail their pursuits.

The first computer programmers did not call themselves "hackers," which derives from the seventeenth-century 'hacker,' a "lusty laborer" who harvested fields by dogged and rough swings of his hoe. Many of these early programming enthusiasts came from engineering or physics backgrounds, and were amateur radio or model train hobbyists. But from about 1945 onward (and especially during the creation of the first ENIAC computer) some programmers realized that their expertise in computer software and technology had evolved not just into a profession, but into a *passion.* Not until the 1960s did these extraordinarily devoted and talented programmers describe themselves as "hackers," their term of self-identification capturing the tenacious and methodical nature of inquiry considered essential to technological innovation.

One such group became the heart of the MIT Artificial Intelligence Laboratory, and its influence spread to ARPAnet, created by the Department of Defense in 1969 and precursor of the first transcontinental, high-speed computer network. Stanford University's Artificial Intelligence Laboratory (SAIL) and Carnegie-Mellon University (CMU) also became thriving centers of computer science, artificial intelligence, and ultimately gave rise to the Internet, the Unix and Linux systems, and the World Wide Web, among other accomplishments.

These early programmers also recognized a burgeoning hacker culture, typified by a resentment of bureaucratic hurdles—such as restricted access to computer mainframes and telephone systems—that frustrated their efforts to explore fully the technological

systems that so intrigued them. Richard Stallman is today best known for such innovative programs as the text-editor program Emacs, and GNU (which, together with Linux, forms an open source operating system rivaling that offered by Microsoft). Stallman offers a colorful description of the nascent "hacker attitude" at the time he joined the MIT Artificial Intelligence laboratory in 1971:

> Bureaucracy should not be allowed to get in the way of doing anything useful. Rules did not matter – results mattered. Rules, in the form of computer security or locks on doors, were held in total, absolute disrespect. We would be proud of how quickly we would sweep away whatever little piece of bureaucracy was getting in the way, how little time it forced you to waste. Anyone who dared to lock a terminal in his office, say because he was professor and thought he was more important than other people, would likely find his door left open the next morning. I would just climb over the ceiling or under the floor, move the terminal out, or leave the door open with a note saying what a big inconvenience it is to go under the floor, 'so please do not inconvenience people by locking the door any longer.' Even now, there is a big wrench at the AI lab entitled, 'the seventh-floor master key,' to be used in case anyone dares to lock up one of the more fancy terminals.

The fundamental characteristic of hackers can be distilled into one simple criterion: a hacker is one who enjoys the intellectual challenge of creatively overcoming and circumventing limitations of programming systems and who tries to extend their capabilities. Just as important, hackers insist that 'hacker' is a term of respect, which can be conferred only by other hackers on those whose creative skills entitle them to membership in a wider community of proficient enthusiasts.

With this brief history in mind, one can easily see why many hackers insist that their term of self-description has been applied too broadly—commonly referring to *anyone* who seeks to extend or circumvent technological limits. The malicious meddler looking to discover sensitive information by "poking around" is not properly called a hacker since, for one thing, sensitive information is often uncovered not by skill but simply by stumbling upon it. "Crackers" are, according to the hackers who disdain them, no more than unskilled stumblers, petty thieves and vandals who rely on luck. Further, not all *skilled* enthusiasts are hackers, either. One sort of skilled cracker, a "phreak" (or "phone phreak"), breaks into telephone networks or security systems in order to make free calls or commandeer services. Another kind of cracker, sometimes referred to as "warez" or "warez d00dz," tries to obtain copies of copyrighted software, break the protection on the software, and then globally distribute the pirate program. Ideally, a warez d00d tries to release "0-day warez," copies of commercial software copied, cracked, and re-released on the first day the software is available for retail sale.

While crackers are gatecrashers—for them breaking in, perhaps copying, stealing, or commandeering are ends in themselves—hackers are driven by curiosity and a desire for proficiency, even elegance, in their endeavors. They are typically libertarian in their insistance on access—Stallman refused to allow "fancy terminals" in the A.I. lab to remain locked up—but they tend not to be cavalier about the law. Further, as evidenced by the various codes of ethics hackers have formulated for themselves, hackers have attempted to convey the normative character of their work and the importance of a personal philosophy to develop their intellectual and moral strength and guide their actions.

A hacker is one who enjoys the intellectual challenge of creatively overcoming and circumventing limitations of programming systems and who tries to extend their capabilities.

The Development of Hacker "Manifestos"

The first thorough discussion of an ethical code for hackers appears in Steven Levy's 1984 work, *Hacker: Heroes of the Computer Revolution.* Levy formulates six criteria that summarize hacker behavior and, to some extent, disclose their general attitude. Although this "code" has been reprinted widely, because it reflects attitudes and technical concerns dating from the 1970s, the first two criteria in particular have seen refinement:

- Access to computers—and anything that might teach you something about the way the world works—should be unlimited and total.
- All information should be free.
- Mistrust authority—promote decentralization.
- Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
- You can create art and beauty on a computer.
- Computers can change your life for the better.

At about the same time (in 1986) *Phrack,* the "official" hacker newsletter, published "The Manifesto" (see inset on page 24), intended both as a statement of the hacker attitude as well as a work of art created by computer technology. Finally, in that same year, 1986, "Doctor Crash" summarized the hacker attitude in three principles:

- Hackers reject the notion that "businesses" are the only groups entitled to access and use of modern technology.
- Hacking is a weapon in the fight against encroaching computer technology.
- The high cost of equipment is beyond the means of most hackers, and therefore hacking and phreaking are the only recourse to spreading computer literacy.

The following was written shortly after my arrest . . .

The Conscience of a Hacker
by
The Mentor

Written on January 8, 1986

Another one got caught today, it's all over the papers. "Teenager Arrested on Computer Crime Scandal," "Hacker Arrested after Bank Tampering. . . ."
Damn kids. They're all alike.
But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him?
I am a hacker, enter my world. . . .
Mine is a world that begins with school . . . I'm smarter than most of the other kids, this crap they teach us bores me. . . .
Damn underachiever. They're all alike.

I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head. . . ."
Damn kid. Probably copied it. They're all alike.

I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed up.
Not because it doesn't like me. . . .
Or feels threatened by me. . . .
Or thinks I'm a smart ass. . . .
Or doesn't like teaching and shouldn't be here. . . .
Damn kid. All he does is play games. They're all alike.

And then it happened. . . a door opened to a world. . . rushing through the phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought. . . a board is found.
"This is it . . .this is where I belong. . . ."
I know everyone here. . . even if I've never met them, never talked to them, may never hear from them again. . . I know you all. . . .
Damn kid. Tying up the phone line again. They're all alike. . . .

You bet your ass we're all alike. . . we've been spoon-fed baby food at school when we hungered for steak. . . the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.

This is our world now. . . the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore. . . and you call us criminals. We exist without skin color, without nationality, without religious bias. . . and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I'm a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all. . . after all, we're all alike.

Phrack
Volume One, Issue 7. Phile 3 of 10

Though all of the criteria have been interpreted variously, Levy's first two criteria (and all three of Dr. Crash) have raised contentious discussion about what is meant by "total" and "free" access to computers and information. Particularly in the 1970s and 1980s, and into the 1990s, some argued that free access should be understood literally—computers and software should be cost free and available to anyone—and, consequently, one is justified in lifting restrictions to access and need feel no twinges of guilt about theft.

Few make this argument any longer, and "free" has come to be understood in a more specialized sense. Richard Stallman, for instance, distributes his Emacs program free of charge with a novel agreement requiring its users to share and improve on the software and then pass along source code "when you distribute any version of Emacs or a related program, and give the recipients the same freedom that you enjoyed." Other programs, such as GNU-Linux, also rely on this notion of "open source" software—that is, a program's software code is made available for anyone to modify or improve upon. Further, one can sell the "free" software—incorporating modifications that make the software easier to use, offering customization, or even simply supplying the software accompanied by directions for its use. (Again, in selling any open source software, the code must be available for the buyer to modify, perhaps to offer for resale.)

In addition to discussion of what constitutes "free access," among other ethical issues debated by hackers are what it is to cause "damage" or "harm" by one's work, the role of intention—whether someone should be morally responsible for harm caused accidentally (as when one inadvertently erases data), and whether a hacker is responsible for the effects of his or her ignorance or lack of skill. Debates also continue

over the ethical appropriateness of covering one's tracks, which may require erasures and alterations of data. Privacy is another important ethical issue discussed by hackers; for instance, they disagree about the circumstances that make access to confidential information permissible and they disagree about whether the standards for ethical access to confidential information are today lower because private information about most U.S. citizens is contained in huge databases and is routinely available for purchase.

Samurai

Hackers also debate the possibility that some of their number, while elite in their programming skills, have decided that one should not, need not, or in some circumstances are absolved from, working in service of the good. Some hackers insist that such "dark-side hackers"—although they work with criminal or malicious intent—are not crackers. ("Dark-side hacker" derives from George Lucas' character Darth Vader, who is "seduced by the dark side of the Force.")

Without resolving the issue of whether hackers are ethically justified in working in the service of a "dark side," hackers tend to agree that one can ethically use the *techniques* of the "dark-side hacker" and the "cracker" to achieve *good* ends. A number of self-professed "good" hackers call themselves "samurai" and model themselves after the historical samurai of Japan (and the "net cowboys" of William Gibson's cyberpunk novels). Samurai are hackers who hire themselves out for legal "electronic locksmith work." A samurai might take part in corporate espionage, aid lawyers pursuing privacy-rights and First Amendment cases, or help track down a cracker. Some samurai profess loyalty to their employers, and disdain vandalism, theft, and any extra-legal means of obtaining information. (Two other groups, "sneakers" and "tiger teams," are paid professionals who use cracking techniques to test security.) The evolution of informal but enforced norms (combined with, perhaps, respect for the law—or *most* laws) has led samurai to reject acting as a law unto themselves.

Falling into this class also is, one might reasonably suggest, the work of the steganographer. Steganography (which derives from the Greek for hidden writing or drawing) allows one to embed, inject, or substitute hidden material in an existing computer text, graphic, or music file. Unlike cryptography, in which an encoded message is in plain sight and one needs a decoder ring, say, to interpret the message, in steganography anyone—other than the informed recipient—who looks at, reads, or listens to an encoded file will be unaware of its hidden material. Public interest in steganography has burgeoned since September 11, with renewed questions about the FBI's Internet monitoring program, Carnivore (which, according to public information about the system, is of limited use in finding such encrypted material) and the National Security Agency's efforts (including, possibly, Echelon, which can capture all telecommunications signals). Hackers might justify their work on samurai grounds—in this case, patriotic loyalty motivates the search for hidden information and the imperatives of national security broaden what is considered lawful.

Hacking as a Public Service

Hackers possess qualities that serve the public and help citizens discern the difference between the splashy, headline-grabbing exploits of the cracker, and the usually more quiet and certainly more useful work of the hacker. The remainder of this article articulates several of the qualities hackers display in their work that also serve the public interest.

Curiosity and a Healthy Skepticism. Hackers find fascinating problems, tackle them with skill, determination, and discipline, and they admire those who work to develop those same qualities. One also encounters frequent reminders to employ the "hand's-on imperative" and warnings against "reinventing the wheel." That is, hackers enjoin others to apply their curiosity to the truly novel and noteworthy. Anything that inhibits one from recognizing problems or their possible solutions—out of ignorance, vanity, or lack of access to information that would raise a question or reveal a view as merely conventional—is curiosity misapplied, and a life lived less well than its potential. Furthermore, hackers approach large or authoritative structures with mistrust. But their skepticism is not paranoia—hackers are driven to find out for themselves and to verify conventional truths.

Hackers enjoin others to apply their curiosity to the truly novel and noteworthy.

In this hackers are solidly in line with the traditional ethical tenets of the Western philosophical tradition. Many have echoed the belief of Plato and Aristotle that the life of inquiry—a life that requires self-discipline, and often the rejection of accepted tradition—leads not just to knowledge, and being a good person, but to becoming a good citizen as well. These philosophers, as their successors, also insisted that one must remain mindful of the crippling effects of ignorance and vanity. In response to the teachers of his time (and ours) who quizzed their students with rhetorical questions,

thereby stifling inquiry, the Renaissance thinker, Michel de Montaigne would frequently ask, "What *do* I know?"—reminding himself that knowledge begins with the recognition of one's own ignorance and acceptance of mere convention. Only then can one find the roots of true knowledge.

Autonomy and Responsibility. Related to the ethical injunction to ground our knowledge is the imperative that we must exercise our autonomy and shape our lives according to our own ends. One interpretation of the hacker's command to "hate boredom," for instance, is that hackers accept that self-actualization is one's own responsibility. Any condition of life that one finds unsatisfactory—as Jean-Paul Sartre or a number of existentialists are well known for insisting—one should not endure, and one certainly should not simply hope that someone else will bring relief. The source of dissatisfaction should be eliminated immediately, and by oneself. Boredom and apathy are symptoms of one's ceasing to ask the right questions and proposing alternative solutions; instead, one has abandoned the responsibility for self-reliance.

Although hackers tend to have a libertarian streak, the insistence on autonomy and responsibility does not mean that we may ignore obligations to others and our wider community. Instead, the hacker attitude that directs energy to finding new problems and novel solutions also accepts that dissatisfaction with the status quo and with one's own efforts at effecting change signal the lack of effort, or misapplied efforts, which are one's personal responsibility to correct.

Mutual Aide and Public Involvement. Although debate continues about "free access" in the sense of what ought to be free of cost, the hacker attitude of "free access" also suggests the notion that one ought not hoard what one learns. Just as curiosity often leads to utility, giving—as many classic morality tales conclude—often leads to getting. Hackers tend to share what they know and to help others, learning and being helped in return.

When we share and help, we tend to work in transparency—everyone can see what we are doing, which can have mixed consequences. One good result of transparancy is that, since the term "hacker" is a compliment within the community of hackers, if one has the skills, competence, and—as I argue—the ethics of a hacker—one's peers recognize one for those attributes.

But another consequence of transparency tends not to be celebratory. When hackers work openly, their results are for all to see. When those results embarrass others—revealing their incompetence, laziness, pridefulness, or ignorance, for instance—the natural human response tends to be an attempt to silence the source of the disclosure. In his defense against charges that he was a traitor to Athens, Socrates famously made just that claim, suggesting that by revealing the proud and wrongheaded views of his peers—many of whom also held political power—he guaranteed personal attack. Although Socrates crafted his role as the "gadfly" of Athens, biting and pricking the minds of his fellow citizens, the tendency to respond defensively to embarrassment remains.

The success of both types of technology enthusiasts—both dark-side hackers and crackers, as well as the self-professed "good" hackers of various types—at times rely on the ignorance of others. For instance, dark-side hackers (and crackers) exploit human weakness and gullibility to gain access to sensitive information. They might trick others into revealing their bank account passwords (by, for instance, telephoning an intended victim and posing as a field service representative with an urgent access problem). The success of samurais and other "good" hackers also depends as much on human gullibility, ignorance, and laziness as on their own skill. For instance, the samurai who reads the deleted e-mail messages of those employees who work on sensitive areas and unwittingly divulge useful information—would see vulnerabilities within the organization better than the employees themselves. In short, weaknesses in "wetware"—in thinking—rather than in software aid the work of both the good and the bad. The "I Love You" virus illustrates perfectly what some call "social engineering"—that is, vulnerabilities in human psychology. The "I Love You" virus relied on human weakness—in this case vanity—for its successful dissemination. Most who receive such a message would not be able to resist opening the file in hopes of learning the identity of their admirer.

When hackers work openly, their results are for all to see. When those results embarrass others . . . the natural human response tends to be an attempt to silence the source of the disclosure.

Knowledge transforms and can elevate, but not all knowledge is knowledge of the good. Although knowledge can be put to bad use, however, the Western philosophical tradition has also insisted that full knowledge requires full understanding of its application—both its good and bad uses. When Renaissance thinker and master political strategist Niccolo Machiavelli called on a ruler to be both a fox and a lion, he suggested that it was inadequate to have knowledge of only the noble and good. One also had to know the ways of the fox, in order to both complete one's knowledge and eliminate the possibility that one could be fooled by another fox. And to *know* good and bad but *choose* the good gives real moral worth to one's actions.

These elements go a long way in explaining the reputation of hackers. In using the term too broadly, we confuse hackers with crackers. And even in their proper role, since gadflies sometimes act as foxes, we are irritated and at the same time fooled by them.

An Aesthetic Life. A final characteristic, one difficult to describe, concerns the hacker attitude toward life. Some hackers express this attitude as the belief that "computers change life for the better," and that one can "create art and beauty on a computer."

Though hackers believe that computers are a necessary part of the search for the good life—they typically urge proficiency in specific programs (html is a must, according to many accounts), insist that one write open-source software and help test and debug the software of others, and encourage the dissemination of useful information—the *spirit* of their advice is to strive to know and to share one's knowledge. One hacker, who wrote an on-line primer on hacking (thereby following the dictum that one publish useful information) also suggests ways to develop one's style and approach to being a hacker. Eric Raymond (who is the author of, among other works, the *Jargon File,* an encyclopedic work about hacking and programming) advises reading widely, studying philosophy (especially the Eastern traditions), developing an appreciation for music, and seeking to refine one's ear for word play and puns. Above all, Raymond enjoins, a hacker must write well in order to clarify his or her thoughts and communicate them effectively. Raymond also follows his additional advice to not use silly or grandiose user identification names; he simply uses his own name.

Clearly, this is good advice for anyone. Thinking about these attributes, one sees a fundamental difference between hackers—who build—and everyone else, such as crackers, who destroy and trespass for its own sake, or people like me—novice users of the computer who use but make no contribution. It's not always easy to see an act as one of destruction or creation. Did Socrates create or destroy? Knowledge of the full consequences of one's actions is a tall order.

Verna V. Gehring
Institute for Philosophy and Public Policy
University of Maryland
vg33@umail.umd.edu

Sources: For just one example of illegal credit access, see usdoj.gov/criminal/cybercrime/diekman4.htm; and for information concerning corporate espionage involving computer access, see "`Netspionage' Costs Firms Millions," msnbc.com/new, posted 11 September 2001; for information about the David Smith case, see "Smith Pleads Guilty to Melissa Virus Charges," by Erich Luening, news.cnet.com; for one account of the "Love Bug" virus and its connection to the Philippines, see "Computer Virus Hits Businesses, Governments Around the World," by K.S. O'Donoghue, www.foxnews.com); on Federal law concerning software theft, see for instance, 17 U.S.C. §301(a)). Among the numerous sites devoted to Kevin Mitnick, see www.takedown.com; *2600-The Hacker's Quarterly,* and the "official" Kevin Mitnick site at kevinmitnick.com. The USA Patriot Act was introduced as H.R. 3162, and was passed October 24, 2001. On the source of the word "hacker," see the *Oxford English Dictionary,* 1971 edition (volume 1), page 1237. As part of the history of hackers, some have distinguished among pre-hacker "Real Programmers," and first-, second-, and now third-generation hackers; for discussions on these various subgroups, see "A Brief History of Hackerdom," which can be found among the writings of Eric Raymond at www.tuxedo.org; also Steve Mizrach, "Is there a Hacker Ethics for 90s Hackers?" copyright 1997 and posted on www.infowar.com; also Steven Levy, *Hackers: Heroes of the Computer Revolution* (Delta, 1984). Richard Stallman describes his life and work at www.stallman.org; his description of the atmosphere at MIT is quoted from project.cyberpunk.ru/-idb/hacker_ethics.html. Some have argued that one can be a hacker in a variety of areas, not just computer and information technology. For an example of this argument, see Pekka Himanen, *The Hacker Ethic and the Spirit of the Information Age,* (Random House, 2001). For a useful discussion of hackers, and distinctions among types of computer enthusiasts, see Eric S. Raymond's (esr@snark.thyrus.com) work at, among other places, www.tuxedo.org; also a variety of hacker terminology can be found in the *Jargon File,* created by Eric Raymond and maintained at www.jargon.org. The *Jargon File* relied on in this article is *Jargon File 4.2.0,* dated January 31, 2000; for hacker codes, see Steven Levy's, *Hacker,* Dr. Crash, Volume One, Issue Six, Phile 3 of 13, "The Techno-Revolution," www.phrack.org. Dr. Crash goes on to insist that every hacker must also be a phone phreak, "because it is necessary to utilize the technology of the phone company to access computers far from where they live. The phone company is another example of technology abused and kept from people with high prices." For excerpts from a number of hacker codes of ethics, see Mizrach article. The copy available was last modified on June 7, 2000. Although numerous versions of hacker ethics abound, most restate Levy , and make additions or revisions. For instance, a 1998 version of the hacker ethics, which identifies itself as the code of the MIT community, adds that, in addition to causing no damage, hacker's work should "be funny, at least to most of the people who experience it." See hacks.mit.edu/Hacks/misc/-ethics.html, (March 28, 1998 version). On Richard Stallman's novel agreement regarding open source software, see: www.gnu.ai.mit.edu/copyleft. Some might claim that a special case of samurai is the "hactivist" whose aims are ideological. Hacktivists typically justify computer sabotage as necessary to promote political ends. The Pakistan Hackerz Club, for instance, advocates an India-free Kashmir, and has made regular attacks on American and Indian Internet sites (such as Lackland Air Force Base, in Texas), inserting a "Save Kashmir" message. Another common technique is "pinging," that is, one computer repeatedly calls another, shutting down its connections. As one might imagine, as tension between China and Taiwan has grown, programmers on both sides of the Taiwan Strait have plagued the sites of the other, tying up networks and displaying messages in support of one or the other regime. For a useful discussion of recent "hacktivist" activities, see "School for Hackers," Adam Cohen, *Time,* (May 22, 2000). Plato's quote concerning Socrates as gadfly of the state is found in the *Apology*: " I am sort of a gadfly . . . and the state is like a great and noble steed who is tardy in his motions owing to his very size, and requires to be stirred to life." Machiavelli's discussion of the importance of knowledge and cunning is found in the *Prince,* Chapter 18.