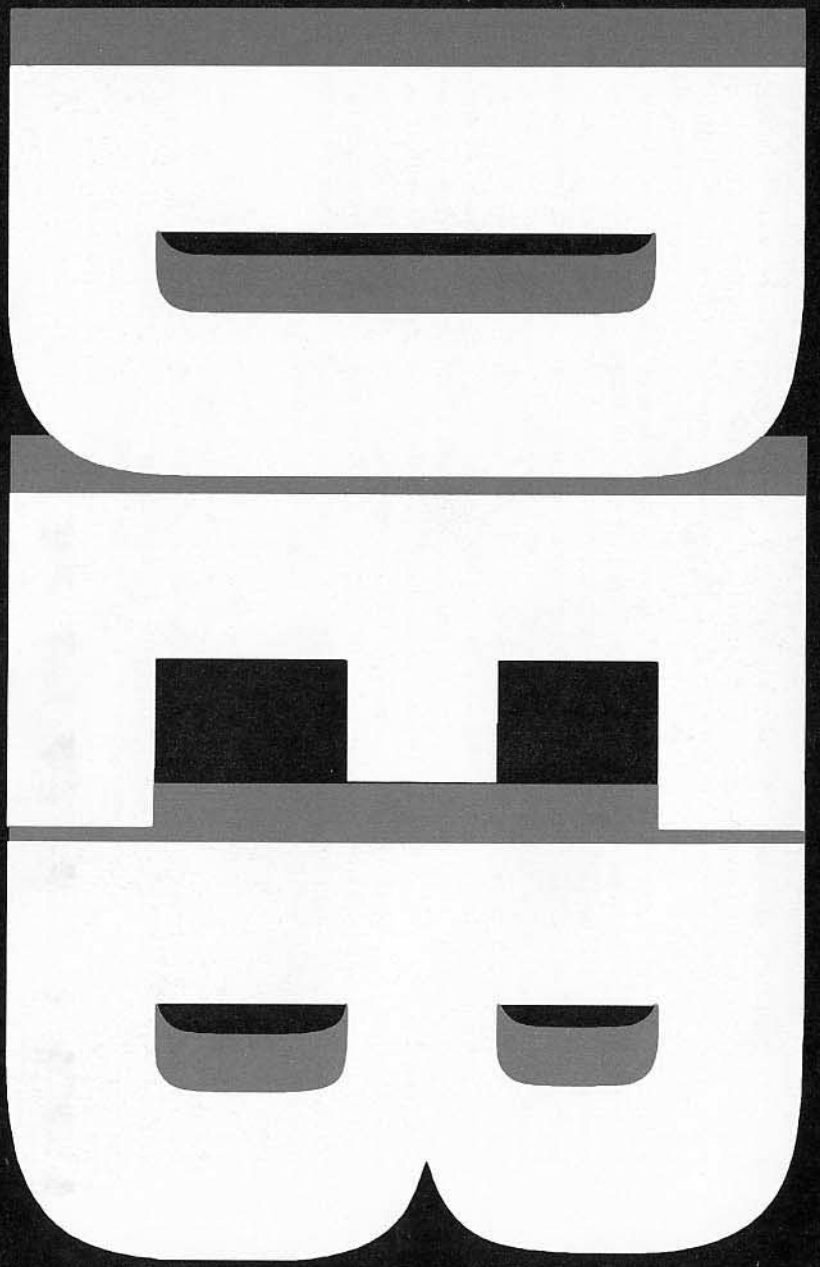
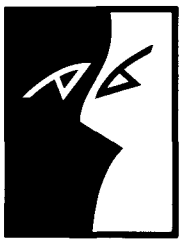
THE UNITED STATES



# ACM VS. CRAIG NEIDORF

**The following debate** examines a landmark electronic publishing case where the U.S. government indicted the publisher of an electronic newsletter on 10 felony counts of wire fraud and interstate transportation of stolen property. Before the trial was over, such awesome issues as freedom of the press, the right to privacy, public security, and the Constitution were called into question. At the center of it all was Craig Neidorf, then a 20-year-old college student. • *Communications* asked Dorothy E. Denning, an expert witness for Neidorf's defense, to explore the case and its far-reaching ramifications. She paints an insider's view of the event; recounting the indictments, the resulting trial, the rights of hackers, the role of government, and the responsibilities—and liabilities—of the computing community. • We then invited seven of Denning's colleagues to comment on her conclusions as well as provide their own assessments of the way the case was handled. Donn Parker, Steven Levy, Eugene Spafford, Paula Hawthorn, Marc Rotenberg, J.J. Buck BloomBecker, and Richard Stallman all voice their individual concerns over the rights of hackers vs. the risks to security. Interspersed throughout the commentaries are quotes gleaned from a panel discussion which occurred during the 13th National Computer Security Conference last October when a group of writers, editors (and one attorney) examined the question of "Hackers: Who Are They?" Denning wraps up the discussion with a rejoinder. • No doubt there are more Craig Neidorfs in our future; and many more questions to be raised as technology continues to allow us greater access to information not intended for publication or public scrutiny. This debate spurs us to consider: **Does publishing sensitive information of specific interest to hackers add fuel to a smoldering fire? Or does the U.S. Constitution indeed protect us from enveloping flames?**



# The United States

## A Debate on Electronic Publishing, Constitutional Rights and Hacking

Dorothy E. Denning

# vs. Craig Neidorf

In 1983, the media publicized a series of computer break-ins by teenagers in Wisconsin nicknamed "414 hackers." At about the same time, the popular movie *Wargames* depicted a computer wizard gaining access to the North American Air Defense (NORAD) Command in Cheyenne Mountain, Colorado and almost triggering a nuclear war by accident. Since then, a stereotype of a *computer hacker*[1] has emerged based upon unscrupulous young people who use their computer skills to break into systems, steal information and computer and telecommunication resources, and disrupt operations without regard for the owners and users of the systems.

Well-publicized incidents, such as the Internet worm [6] and the German hackers who broke into unclassified defense systems and sold information to the KGB [7], have reinforced that stereotype and prompted policy makers and law enforcers to crack down on illegal hacking. In May 1990, 150 Secret Service agents executed 27 search warrants and seized 40 systems as part of Operation Sun Devil, a two-year investigation led by Arizona prosecutors into incidents estimated to have cost companies millions of dollars. Another investigation involving prosecutors in Atlanta and Chicago led to several indictments.

Reports on some of the seizures and indictments provoked an outcry from people in the computer industry who perceived the actions taken by law enforcers as a threat to constitutional rights. One case in particular that was cited as an example of threats against freedom of the electronic press was that of *Craig Neidorf*—a college student accused by the U.S. government of fraud and interstate transportation of stolen property regarding a document published in his electronic newsletter, *Phrack*. The trial began on July 23, 1990, and ended suddenly four days later when the government dropped the charges. I attended the trial as an expert witness for the defense.

[1]The term "hacker" originally meant anyone with a keen interest in learning about computer systems and using them in novel and clever ways. Many computer enthusiasts still call themselves hackers in this nonpejorative sense.

## Overview of the Case

Craig Neidorf is a pre-law student at the University of Missouri. At the age of 13, he became interested in computers, an extension of an earlier intense interest in Atari 2600 and other video games. At 14, he adopted the handle Knight Lightning on computer networks and bulletin boards. At 16, he and a childhood friend started an electronic newsletter called *Phrack*. The name was composed from the words *phreak* and *hack*, which refer to telecommunications systems (phreaking) and computer systems (hacking). To *Phrack* readers and contributors, phreaking and hacking covered both legal and illegal activities, and some of the articles in *Phrack* provided information that could be useful for someone trying to gain access to a system or free use of telecommunications lines. To some law enforcers and computer security professionals, *Phrack* was seen as a possible breeding ground for computer criminals. They found issues of *Phrack* among the evidence of cases under investigation, and a hacker told them that *Phrack* had provided information that helped him get started.

*Phrack* published 30 issues from November 1985 through 1989. Neidorf's main role with the newsletter was editor of a column called "Phrack World News." In addition, he was the publisher of issue 14, and co-editor/publisher of issues 20–30. As publisher, he solicited articles from authors, assembled the articles he received into an issue, and distributed the issue to an electronic mailing list.

On January 18, 1990, Neidorf received a visit from an agent of the U.S. Secret Service and a representative of Southwestern Bell Security regarding a document about the Enhanced 911 (E911) emergency system. This document, which was in the form of a computer text file, had been published in Issue 24 of *Phrack*. During this visit, Neidorf, believing he had done nothing wrong, cooperated and turned over information. The next day, the visitors returned with a representative from the campus police and a search warrant. Neidorf was also asked to contact the U.S. Attorney's office in Chicago. He did, and on January 29 arrived at that office, accompanied by a lawyer, for further interrogation. Again, the young publisher turned over information and answered their questions. Neither he nor his attorney were informed that four days earlier evidence had been presented to

a federal grand jury in Chicago for the purpose of indicting him. On February 1, the grand jury was given additional evidence and charged Craig Neidorf with six counts in an indictment for wire fraud, computer fraud, and interstate transportation of stolen property valued at $5,000 or more.

In June 1990, the grand jury met again and issued a new indictment that dropped the computer fraud charges, but added additional counts of wire fraud. Neidorf was now charged with 10 felony counts carrying a maximum penalty of 65 years in prison.

The indictment centered on the publication of the E911 text file in *Phrack*. The government claimed the E911 text file was a highly proprietary and sensitive document belonging to BellSouth and worth $23,900. They characterized the document as a road map to the 911 phone system, and claimed that its publication in *Phrack* allowed hackers to illegally manipulate the 911 computer systems in order to disrupt or halt 911 service. They further claimed that the document had been stolen from BellSouth by Robert Riggs, also known as The Prophet, and that the theft and publication of the document in *Phrack* was part of a fraudulent scheme devised by Neidorf and members of the hacking group Legion of Doom, of which Riggs was a member. The object of the scheme was to break into computer systems in order to obtain sensitive documents and then make the stolen documents available to computer hackers by publishing the documents in *Phrack*. The government claimed that as part of the fraudulent scheme, Neidorf solicited information on how to illegally access computers and telecommunication systems for publication in *Phrack* as "hacker tutorials." The term hacker was defined in the indictment as an individual "involved with the unauthorized access of computer systems by various means."

On May 21, 1990 Neidorf called me to request a copy of my paper about hackers, which I was preparing for the National Computer Security Conference [1]. Although I had not talked with him before that time, I knew who he was because I had been following his case in the *Computer Underground Digest*, an electronic newsletter, and in various Usenet bulletin boards. Based on what I had read, which included the E911 file as published in *Phrack*, I did not see how the E911 file could be used to break into the 911 system or, for that matter, any computer system. I was concerned that Neidorf may have been wrongly indicted. I was also concerned that a wrongful conviction—a distinct possibility in a highly technical trial—could have a negative impact on electronic publication.

In late June, I received a call from Neidorf's attorney, Sheldon Zenner of the firm Katten, Muchin & Zavis in Chicago. After several conversations with Neidorf and Zenner, I agreed to be an expert witness and provide assistance throughout the trial.

Zenner told me that John Nagle, an independent computer scientist in Menlo Park, California, had gathered articles, reports, and books on the E911 system from the Stanford University library and local bookstores, and by dialing a Bellcore 800 number. After Nagle showed me the published documents, I agreed with his conclusion that *Phrack* did not give away any secrets. Nagle was also planning to go to Chicago to help with the defense and possibly testify.

Meanwhile, I gathered articles, books, and programs that showed there are plenty of materials in the public domain that are at least as useful for breaking into systems as anything published in *Phrack*. (Some of these are referenced later.)

## THE TRIAL

The trial began on July 23, 1990 in Chicago's District Court for the Northern District of Illinois. It was expected to last two weeks, with the government presenting its case during the first week. I helped prepare the cross examinations of the government's witnesses and expected to testify sometime during the second week.

After a day of jury selection, the trial began with Assistant U.S. Attorney William Cook making the opening remarks for the prosecution. Cook reviewed the government claims, weaving a tale of conspiracy between Neidorf, Riggs, and members of the Legion of Doom who had broken into BellSouth computers.

Zenner then presented his opening remarks for the defense. He reviewed Neidorf's history and involvement with *Phrack*, noting that the goal of the newsletter was the free exchange of information. He challenged the claims of the government and outlined the case for the defense. He noted how the government had indicted Neidorf despite his extensive cooperation with them. He said that Neidorf believed his actions were covered by the First Amendment, and that his beliefs were formed from college classes he took as a pre-law student on constitutional law and civil liberties.

The government's witnesses through Thursday afternoon included Riggs, the Secret Service agent, and employees of Bellcore and of BellSouth and its subsidiaries. The evidence brought out during the examination and cross-examination of these witnesses indicated the E911 text file was not the highly sensitive and secret document that BellSouth had claimed, that BellSouth had not treated the document as though it were, and that Neidorf had not conspired with Riggs. Although this seemed like cause for optimism, Zenner

reminded us that the government loses very few cases.

On Friday morning, I arrived at the law offices to learn the government had been talking with Zenner about dropping the felony charges in exchange for a guilty plea to a misdemeanor. Neidorf, however, would not accept a charge for something he had not done. Meanwhile, Zenner was meeting with the U.S. attorneys. I went to the courtroom, where Zenner told me the government was now considering dropping all charges. Zenner was willing to lay out the case for the defense to the prosecution; he asked Nagle and me to go to the U.S. Attorney's office and answer all their questions. We went, and Cook went through the E911 file paragraph by paragraph asking us for evidence that the material was in the public domain. Nagle answered most of the questions, pointing Cook to the relevant public documents and demonstrating that the E911 *Phrack* file did not give away any secrets.

We then went to the courtroom to await the final decision. Shortly thereafter, the court resumed, and Judge Nicholas Bua announced the government's decision to drop charges, dismissed the jury, and declared a mistrial. Five of the jurors were asked to remain and were interviewed by Bua and both attorneys. At midday, the court adjourned.

Although Neidorf was freed of all criminal charges, he was not free of all costs. The trial cost of $100,000 was incurred by him and his family.

## KEY DOCUMENTS

The government's case focused on several documents that were published in *Phrack* or were included in electronic mail between Neidorf and others. These included the following: the E911 text file and *Phrack* version of that file; the hacker tutorials published in *Phrack* Issue 22; a Trojan horse login program; an announcement of The Phoenix Project in *Phrack* Issue 19; and some email correspondence between Neidorf and Riggs. All these documents were introduced as evidence by the government during the presentation of its case.

## The E911 Text File

Riggs testified that sometime during the summer of 1988, he accessed a BellSouth system called AIMSX and downloaded a file with a document issued by BellSouth Services titled "Control Office Administration of Enhanced 911 Services for Special Services and Major Account Centers," Section 660-225-104SV, Issue A, March 1988. The document, which contains administrative information related to E911 service, installation, and maintenance, bears the following notice on the first page: "Not for use or disclosure outside BellSouth or any of its subsidiaries except under written agreement." Sometime prior to September 1988, Riggs transferred the file to a public Unix™ system called Jolnet, where it remained until July 1989.

Riggs testified he sent the E911 text file to Neidorf via email from Jolnet in January 1989 for publication in *Phrack*. He said he asked Neidorf to edit the file so that it would not be recognizable by BellSouth, and to publish it under the handle "The Eavesdropper." Neidorf removed the nondisclosure notice and deleted names, locations, and telephone numbers, and published it in *Phrack* Issue 24 on February 24, 1989. The edited document was less than half the size of the original document, and was split into two *Phrack* files, the first (file 5) containing the main text and the second (file 6) containing the glossary of terms.

The government claimed that the E911 text file and *Phrack* version contained highly sensitive and proprietary information that provided a road map to the 911 system and could be used to gain access to the system and disrupt service. The claim was based on a statement made by an employee of Bellcore.

> "Congress shall make no laws . . . abridging the freedom of speech, or of the press; or the right of the people peacefully to assemble . . ." FIRST AMENDMENT

As noted earlier, Nagle had located articles and pamphlets that contained much more information about the E911 system than the *Phrack* file. During cross examination of the government's witness who was responsible for the practice described in the E911 document, Zenner showed the witness two of these pamphlets available from Bellcore via an 800 number for $13 and $21 respectively. The witness, who had not seen either report before and was generally unfamiliar with the public literature on E911, agreed that the reports also gave road maps to the E911 system and included more information than was in *Phrack*. The witness also testified that a nondisclosure stamp is routinely put on every BellSouth document when it is first written, thereby weakening any argument that the document contained particularly sensitive trade secrets.

The defense was prepared to argue that the E911 text file con-

tained no information that was directly useful for breaking into the E911 system or any computer system. There were no dial-up numbers, no network addresses, no accounts, no passwords, and no mention of computer system vulnerabilities. The government claimed that the names, locations, organization phone numbers, and jargon in the E911 text file could be useful for *social engineering*—that is, deceiving employees to get information such as computer accounts and passwords. However, the *Phrack* version omitted the names, locations, and phone numbers, and the jargon was all described in the published literature. Thus, the E911 *Phrack* file seemed no more useful for social engineering than the related public documents.

The defense was also prepared to show that BellSouth had not treated the document as one would expect a document of such alleged sensitivity to be treated. Riggs testified that the account he had used to get into AIMSX had no password. AT&T security was notified in September 1988, that the E911 text file was publicly available in Riggs's directory on Jolnet, and Bellcore security was notified of this in October. This was two months before Riggs mailed the file to Neidorf for inclusion in *Phrack,* and about four months before its publication in *Phrack.* Still, no legal action was taken until July 1989, nine months from the time Bellcore was aware of the file's presence on Jolnet. At that point, Bellcore and BellSouth asserted to the government that a highly sensitive and dangerous document was stolen. They urged the U.S. Secret Service to act immediately because of the purported risk posed by the availability of this "dangerous" information. However, they did not tell the Secret Service that they had discovered all of this nine months earlier. The government responded immediately with a subpoena for Jolnet. The defense believed that BellSouth's delay in acting to protect the E911 document was inconsistent with its claim that the document contained sensitive information. To its credit, however, BellSouth did strengthen the security of its systems following the breakins.

## The Hacker Tutorials

The government claimed that three files in *Phrack* Issue 22 were tutorials for breaking into systems and, as such, evidence of a fraudulent scheme to break into systems, steal documents, and publish them in *Phrack.* These files, which corresponded to one count of the indictment, were:

4. "A Novices Guide to Hacking—1989 Edition" by The Mentor.
5. "An Indepth Guide in Hacking Unix and The Concept of Basic Networking Utility" by Red Knight.
6. "Yet Another File on Hacking Unix" by Unknown User.

Files 4 and 5 of *Phrack* 22 briefly introduce the art of getting computer access through weak passwords and default accounts, while File 6 contains a password-cracking program. Most of file 5 is a description of basic commands in Unix, which can be found in any Unix manual. After examining these and other *Phrack* files, I concluded that *Phrack* contained no more information about breaking into systems than articles written by computer security specialists and published in journals such as the *Communications of the ACM, AT&T Bell Technical Journal, Information Age,* and *Unix/WORLD,* and in books. For example, Cliff Stoll's popular book *The Cuckoo's Egg* [7] has been characterized as a "primer on hacking." Information that could be valuable for breaking passwords is given in the 1979 paper on password vulnerabilities by Morris and Thompson of Bell Laboratories [4]. A recent article by Spafford gives details on the workings of the Internet worm [6].

Password-cracking programs are publicly available intentionally so that system managers can run them against their own password files in order to discover weak passwords. An example is the password cracker in COPS, a package that checks a Unix system for different types of vulnerabilities. The complete package can be obtained by anonymous FTP from ftp.uu.net. Like the password cracker published in *Phrack,* the COPS cracker checks whether any of the words in an on-line dictionary correspond to a password in the password file.

Another file that the prosecution brought into evidence during the trial was file 6 in *Phrack* Issue 26, "Basic Concepts of Translation," by The Dead Lord and The Chief Executive Officers. This file, which described translation in Electronic Switching System (ESS) switches, contained a phrase "Anyone want to throw the ESS switch into an endless loop????" in a section on indirect addressing in an index table. This remark can be interpreted as a joke, but even if it were not, the information in the article seems no worse than Ritchie's code for crashing a system, which is published in the Unix Programmer's Manual with the comment "Here is a particularly ghastly shell sequence guaranteed to stop the system: . . ." [5].

The government's claims that these files were part of a fraudulent scheme were disproved by Riggs's testimony and email (discussed later) showing that Neidorf and Riggs had not conspired to commit fraud by stealing property and publishing stolen documents.

By publishing articles that expose system vulnerabilities, *Phrack,* in one sense, is not unlike some professional publications such as those issued by the ACM. The As-

sociation encourages publishing such articles on the grounds that in the long term, the knowledge of vulnerabilities will lead to the design of systems that are resistant to attacks and failures. But, there is an important difference between the two publications.

ACM explicitly states that it does not condone unauthorized use or disruption of systems, it discourages authors of articles about vulnerabilities from writing in a way that makes attacks seem like a worthy activity, and it declines to publish articles that appear to endorse attacks of any kind. In addition, the ACM is willing to delay publication of an article for a short time if publishing the information could make existing systems subject to attack.

By comparison, *Phrack* appears to encourage people to explore system vulnerabilities. In "A Novice's Guide to Hacking," The Mentor gives 11 guidelines to hacking. The last says "Finally, you have to actually hack. . . . There's no thrill quite the same as getting into your first system . . . " Although the guidelines tell the reader "Do not intentionally damage *any* system," they also tell the reader to alter those system files "needed to ensure your escape from detection and your future access."[2] The wording can be interpreted as encouraging unauthorized but nonmalicious break-ins. Thus, whereas reading *Phrack* could lead one to the assessment that it promotes illegal break-ins, reading an ACM publication is likely to lead to the assessment that it discourages such acts and promotes protective actions.

The actual effect of either publication on illegal activities or computer security, however, is much more difficult to determine, especially since both publications are available to anyone. Computer security specialists who read *Phrack* may have found it useful to know what vulnerabilities intruders were likely to exploit, while hackers who read *Communications of the ACM* may have learned something new about breaking into systems or implanting viruses. The *Phrack* reports on people who were arrested may have discouraged some budding young hackers from performing illegal acts; they also may have reminded hackers to take greater measures to cover up their tracks and avoid being caught.

Even if *Phrack* promoted certain illegal actions, this does not make the publication itself illegal. The First Amendment protects such publication unless it poses an imminent danger to society. The threshold for this condition is sufficiently high that, although courts have discussed its theoretical existence, it has never been met.

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . " FOURTH AMENDMENT

## The Trojan Horse Login Program

The government found a modified version of the AT&T System V 3.2 login program in Neidorf's files. The program, which was modified and sent to Neidorf by someone currently under indictment, was part of the AT&T Unix source code and had "copyright" and "proprietary" stamps scattered throughout. The modifications included a Trojan horse that captured accounts and passwords, saving them in a file that could later be retrieved. The government claimed that Neidorf's possession of this program demonstrated his intentions to promote illegal break-ins and the theft of proprietary information. To support its case, it brought into evidence email where Neidorf was relaying messages between two other parties. One party said he had other Unix sources, including 4.3 BSD Tahoe; the other asked for the Tahoe source so he could install the login program on some Internet sites.

The defense believed the government's allegations against Neidorf were weak on three grounds.

First, as with any publisher, the mere receipt of a document is not proof of intent to perform illegal acts.

Second, after observing that the source code contained notices that the code was copyrighted and proprietary, Neidorf asked someone at Bellcore security for advice on what to do. This action added credibility to his claim that he had no intent to perform illegal acts and that he did not know that publishing the E911 text could be illegal. Although the E911 file had a nondisclosure notice, the notice did not contain the words "copyright" or "proprietary."

Third, how to write a Trojan horse login program is no secret. For example, such programs have been published in Stoll's book [7] and an article by Grampp and Morris [2]. Also, in his ACM Turning lecture, Ken Thompson, one of the Bell Labs coauthors of Unix, explained how to create a powerful Trojan horse that would allow its author to log onto any account with either the password assigned to the

[2]Most system managers regard any modification of system files as damage, because they must restore these files to a state that does not permit the intruder to re-enter the system.

account or a password chosen by the author [8]. Thompson's Trojan horse had the additional property of being undetectable in the login source code. This was achieved by modifying the C-compiler so that it would compile the Trojan horse into the login program.

### The Phoenix Project and Email Correspondence

Issue 19, File 7 of *Phrack* announced "The Phoenix Project," and portrayed it as a new beginning to the phreak/hack community where "Knowledge is the key to the future and it is FREE. The telecommunications and security industries can no longer withhold the right to learn, the right to explore, or the right to have knowledge." The new beginning was to take place at SummerCon '88 in St. Louis.

The government claimed this announcement was the beginning of the fraudulent scheme to solicit and publish information on how to access systems illegally, and its publication accounted for one of the counts in the indictment. Yet, the announcement explicitly says "The new age is here and with the use of every *LEGAL* means available, the youth of today will be able to teach the youth of tomorrow. . . . the practice of passing illegal information is not a part of this convention." Security consultants and law enforcers were invited to attend SummerCon.

Although Neidorf was not charged with any crimes in 1988, the Secret Service sent undercover agents to SummerCon '88 to observe the meeting. They secretly videotaped Neidorf and others through a two-way mirror during the conference for 15 hours. What did they record? A few minors drinking beer and eating pizza! Zenner asked to introduce these tapes as evidence for the defense, but the prosecution objected and Judge Bua sustained their objection.

Two counts of the indictment involved email messages from Neidorf to Riggs and "Scott C." These messages, which were also alleged to be part of the fraudulent scheme, were basically discussions of particular individuals, mainly members of the Legion of Doom. The messages contained no plots to defraud any organization and no solicitations for illegal information.

## RIGHTS AND RESPONSIBILITIES

Neidorf's indictment came in the midst of a two-year investigation of illegal activity that involved the FBI, Secret Service, and other federal and local law enforcement agencies. As part of the investigation, the government seized over 40 systems and 23,000 disks. Several bulletin board systems were shut down in the process, including the Jolnet system on which Riggs stored the E911 document. In most cases, no charges have yet been made against the person owning the equipment, and equipment that seemed to have little bearing on any illegal activity, such as a phone answering machine, was sometimes included in the haul. The *Phrack* case and computer seizures raised concerns about freedom of the press, protection from unnecessary searches and seizures, and the liabilities and responsibilities of system operators and owners. In this section, I shall discuss these issues and give some of my own opinions about them.

### Electronic Publications

Some observers interpreted Neidorf's indictment as a threat to freedom of the press in the electronic media. The practice of publishing materials obtained by questionable means is common in the news media, and publication of the E911 file in *Phrack* was compared with publication of the Pentagon Papers in the *New York Times* and *Washington Post*. The government had tried unsuccessfully to stop publication of the Pentagon Papers, arguing that publication would threaten national security. The Supreme Court held that such action would constitute a "prior restraint" on the press, prohibited by the First Amendment. It therefore surprises me that there is any doubt that electronic publications should be accorded the same protection as printed ones.

Shortly before the *Phrack* case came to trial, Mitchell Kapor and John Barlow founded the Electronic Frontier Foundation (EFF) in order to help raise public awareness about civil liberties issues and to support actions in the public interest to preserve and protect constitutional rights within the electronic media. The EFF hired the services of Terry Gross, attorney with the New York law firm Rabinowitz, Boudin, Krinsky & Lieberman, to provide legal advice for the *Phrack* case; Gross submitted two friend-of-the-court briefings seeking to have the indictment dismissed because it threatened constitutionally protected speech. The trial court judge denied EFF's motion, but as it turned out, the charges were dropped before the issue was seriously discussed during the *Neidorf* trial.

Although certain information may be published legally, authors and publishers should consider how such information might be interpreted and used. In the case of hacker publications, the majority of readers are impressionable young people who are the foundation of the future. Articles which encourage illegal break-ins or contain information obtained in this manner should not simply be dismissed as proper just because they are protected under First Amendment rights.

## Searches and Seizures

The seizures of bulletin boards and other systems raised questions about the rights of the government to take property and retain it for an extended period of time when no charges have been made. At least one small business, Steve Jackson Games, claims to have suffered a serious loss as a result of having equipment confiscated for over three months. According to Jackson, the Secret Service raid cost his company $125,000, and he had to lay off almost half of his employees since all of the information about their next product, a game called GURPS CYBERPUNK, was on the confiscated systems. Some of the company's equipment was severely damaged, and data was lost. No charges have been made.

Seizing a person's computer system can be comparable to taking every document and piece of correspondence in that person's office and home. It can shut down a business. Moreover, by taking the system, the government has the capability of reading electronic mail and files unrelated to the investigation; such broad seizures of paper documents are generally not approved by judges issuing search warrants.

For these reasons, it has been suggested that the government not be allowed to take complete systems, but only the files related to the investigation. In most cases, this seems impractical. There may be megabytes or even gigabytes of information stored on disks, and it takes time to scan through that much information. In addition, the system may have nonstandard hardware or software, making it extremely difficult to transfer the data to another machine and process it. Similarly, if a computer is seized without its printer, it may be extremely difficult to print out files. Finally, originals are needed for evidence in court, and the evidence must be protected up to the time of trial. However, if the government can be reasonably confident that the owner of the system has not participated in or condoned the activities under investigation, then it may be practical for the government to issue a subpoena for certain files rather than seize the entire system.

When a complete system is seized, it seems reasonable that the government be required under court order to provide copies of files to the owner at the owner's request and expense within some time limit, say one week or one month.

If a system shared by multiple users is seized, the search should be restricted to mail and files belonging to the users under investigation.

> "No person shall be . . . deprived of life, liberty, or property, without due process of law . . ." FIFTH AMENDMENT

## Liabilities and Responsibilities of System Operators and Owners

The bulletin board seizures sent a chill through the legitimate network community, raising questions about the liabilities of an operator of a bulletin board or of any system. Operators of these boards asked if they needed to check all information passing through the system to make sure there is nothing that could be interpreted as a stolen, proprietary document or as part of a fraudulent scheme.

Computer bulletin boards have been referred to metaphorically as electronic meeting places where assembly of people is not constrained by time or distance. Public boards are also a form of electronic publication. It would seem, therefore, that they are protected by the constitution in the same way that public meeting places and nonelectronic publications such as newspapers are protected. This, of course, does not necessarily mean they should be free of all controls, just as public meetings are not entirely free of control.

Bulletin board systems often provide private directories and electronic mail. Private mail and files should be given the same protections from surveillance and seizure as First Class Mail and private discussions that take place in homes or businesses. I believe the Electronic Communications Privacy Act provides this protection.

The E911 text file was obtained from a system with a null password. While this does not excuse the person who got into the system and copied the file, I believe that system owners should take greater measures to prevent break-ins and unauthorized use of their systems. There are known practices for protecting systems. While none of these are foolproof, they offer a high probability for keeping intruders out and detecting those that enter. Although the risks associated with insecure systems may not have been great until recently, thereby justifying weak security in favor of allocating more resources for other purposes, the risks are now sufficiently great that weak security is inexcusable for many environments. Moreover, system owners may be vulnerable to lawsuits if they do not have adequate protection for customer information or for life-critical operations such as patient monitoring or traffic control.

Our current laws allow a person

to be convicted of a felony for simply entering a system through an account without a password. I recommend we consider adopting a policy where unauthorized entry into a system is at most a misdemeanor if certain standards have not been followed by the owner of the system and the damage to information on the system is not high. However, I recognize that it may be very difficult to set appropriate standards and to determine whether an organization has adhered to them.

I also recommend we consider establishing a range of offenses, possibly along the lines of those in the U. K. Computer Misuse Act, which became effective in August 1990:

- **Unauthorized access:** seeking to enter a computer system, knowing that the entry is unauthorized. Punishable by up to six months' imprisonment.
- **Unauthorized access in furtherance of a more serious crime:** Punishable by up to five years' imprisonment.
- **Unauthorized modification of computer material:** introducing viruses, Trojan horses, etc., or causing malicious damage to computer files. Punishable by up to five years' imprisonment.

## CONCLUSIONS

Making a sound assessment of the claims made in the *Phrack* case requires expertise in the domains of computers, the Unix system, computer security, phone systems, and the public literature. Whereas Zenner brought in outside technical expertise to help with the defense, the prosecution relied on experts belonging to the victim, namely, employees of Bell. The indictment and costly trial may have been avoided if the government had consulted neutral experts before deciding whether to pursue the charges. The professional community represented by ACM may be a good source of such help.

In the context of the new milieu created by computers and networks, a new form of threat has emerged—the computer criminal capable of damaging or disrupting the electronic infrastructure, invading people's privacy, and performing industrial espionage. While the costs associated with these crimes may be small compared with computer crimes caused by company employees and former employees, the costs are growing and are becoming significant.

For many young computer enthusiasts, illegal break-ins and phreaking are a juvenile activity that they outgrow as they see the consequences of their actions in the world. However, a significant number of these hackers may go on to become serious computer criminals. To design an intervention that will discourage people from entering into criminal acts, we must first understand the hacker culture since it reveals the concerns of hackers that must be taken into account. We must also understand the concerns of companies and law enforcers. We must understand how all these perspectives interact.

The 1985 ACM Panel on Hacking [3] offered several suggestions for actions that could be taken to reduce illegal hacking, and my own investigation confirmed these while speculating about others [1]. Teaching computer ethics may help, and I applaud recent efforts on the part of computer professionals and educators to bring computer ethics not only into the classroom, but into their professional forums for discussion.

**Acknowledgments**

Special thanks to Chuck Bushey, Peter Denning, Jef Gibson, Cynthia Hibbard, Steve Lipner, Craig Neidorf, Mike Schroeder, and Sheldon Zenner for many helpful suggestions; to Pete Mellor for information about the U. K. laws; and to my many friends and colleagues who patiently educate me in areas where I am vulnerable to my own blindness. The views here are my own and do not represent those of my employer.

**References**

1. Denning, D.E. Concerning hackers who break into computer systems. In *Proceedings of the 13th National Computer Security Conference* (Oct. 1990).
2. Grampp, F.T., and Morris, R.H. UNIX operating system security. *AT&T Bell Lab. Tech. J., 63,* 8 (Oct. 1984).
3. Lee, J.A.N., Segal, G., and Stier, R. Positive alternatives: A report on an ACM panel on hacking, *Commun. ACM, 29,* 4 (Apr. 1986), 297–299; full report available from ACM Headquarters, New York.
4. Morris, R., and Thompson, K. Password security: A case history. *Commun. ACM 22,* 11 (Nov. 1979).
5. Ritchie, D. On the security of Unix. Unix programmer's manual, Section 2, AT&T Bell Laboratories.
6. Spafford, E.H. The Internet Worm: Crisis and aftermath. *Commun. ACM 32,* 6 (June 1989).
7. Stoll, C. *The Cuckoo's Egg.* Doubleday, N.Y. 1990.
8. Thompson, K. Reflections on trusting trust. Turing Award Lecture, *Commun. ACM 27,* 8, 761–763.

TMUnix is a trademark of AT&T Bell Laboratories

# Colleagues Debate Denning's Comments

Twenty years of studying and writing about computer crime and the malicious hacker culture leads me to conclude that Denning's article presents a biased description of a criminal case. The author states some ill-conceived and naive conclusions and recommendations along with some sound and practical ones. For example, well-publicized incidents have not, as she concludes, necessarily prompted law enforcers to crack down on illegal hacking. Rather, the actions of law enforcers have revealed a criminal problem that results in publicity. Otherwise, the incidents would not be publicly known, since victims usually attempt to keep their embarrassing losses to themselves.

Contrary to the author's statement, the outcry about computer seizures and indictments from people in the computer industry is not overwhelming. It comes from a very small number of people concerned about two or three (seemingly extreme) incidents which are still open questions since we have not yet heard the victims' and law enforcers' sides of them. Of course, law enforcers will use significant force when the suspects brag that they will use guns against officers serving search warrants. And, of course, computers and computer media are going to be seized and kept as long as possible when the hacker-owners publicly claim they are going to bring down our telephone systems in retaliation for indictment.

Denning asserts that although *Phrack's* publication of information from E911 may have been improper, it was still protected by the First Amendment as free speech. It was, of course, protected to the extent that any publication is protected unless it is part of a conspiracy to commit a crime. But the freedom of the electronic press had nothing to do with the *Neidorf* case—at least according to the judge and the indictment. That issue was a smoke screen used by the defense and the EFF. The judge in this case stated that, "The First Amendment does not act as a shield to preclude the prosecution of that individual [who violates an otherwise valid criminal statute] simply because his criminal conduct involves speech. . . . In short, the court finds no support for Neidorf's argument that the criminal activity with which he is charged in this case is protected by the First Amendment." Neidorf and the EFF failed to stop the trial on First Amendment rights issues.

If the trial had not been cut short by one flaw in the prosecutor's case, I suspect that Neidorf would have been easily convicted—if even a few of the offenses and evidence in the indictment were valid. After all, Neidorf apparently did not know that some of the information in the stolen BellSouth proprietary E911 report was being sold legally elsewhere, and his denial of knowing that the information he used was stolen or sensitive seems, in view of his admitted actions, implausible.

On strictly moral and professional grounds, I believe that publishing criminal methods is important and fully justified when done with the intent of helping people to protect themselves. However it is antisocial, irresponsible, and immoral to publish the same material when the intent is to amuse other people and tempt them to violate the rights and property of others. Those who engage in this activity are abusing their civil rights, and I believe we should treat such people as our adversaries, not our colleagues.

Denning writes, ". . . articles in *Phrack* provided information that could be useful for someone trying to gain access to a system or free use of telecommunication lines." These are euphemisms for breaking into others' computers and engaging in toll fraud. Her choice of words shows a bias toward treating at least some criminal activities against systems too lightly, even though she has spent a good part of her distinguished career engaged in research to defend potential victims from such acts. Her bias also shows when, describing the opening remarks at the trial, she states that the prosecutor "weaved a tale of conspiracy," while Zenner for the defense "reviewed . . . noted . . . challenged . . . and outlined" in justifying Neidorf's actions. And she cites the maximum possible sentence facing Neidorf, even though such sentences are extremely rare; it would have been more objective and less explosive to state the range or average. Denning presents the trial strictly from the defense perspective. I would want to hear the prosecutor's and victim's perspectives before reaching the same conclusions as the author.

The author says that publication of the E911 document owned by BellSouth was inconsequential. But she leaves us wondering why Neidorf removed the nondisclosure notice and deleted names, locations, and telephone numbers from the document before publishing it. She also states that it was only claimed that Neidorf's alleged conspirator, Riggs, stole the document from BellSouth, when in fact Riggs was convicted of the theft before the Neidorf trial.

The author reports that publishing criminal methods in *Phrack* has been compared with publishing the Pentagon Papers in the *New York Times* and claims the publications should be accorded the same protection. Although she is right about equal protection in general, the comparison is weak. *Phrack* was publishing methods used in an alleged criminal conspiracy for an audience of malicious juvenile hackers. The *New York Times* was publishing information alleged to be of national policy importance, under the ethical constraints imposed by society and the journalistic

profession.

The author states that, "*Phrack* appears to encourage people to explore system vulnerabilities." This is another euphemism for taking advantage of vulnerabilities in other people's computer systems by breaking into them and violating their privacy. She further uses the term, "unauthorized but nonmalicious break-ins." I conclude that the author believes that at least some unauthorized break-ins are not malicious. This is surprising coming from someone so dedicated to protecting civil rights, and privacy in particular, since breaking into other people's computer systems without their knowledge or permission is surely a violation of privacy as well as an offense in federal and most states' criminal laws.

Denning suggests that adequate security of systems be a criterion for whether an attack is a minor or a severe crime. I would rather keep the tradition of the criminal code that determining if an offense is a crime depends on the intent of the perpetrator and the seriousness of the act, and not on the vulnerability of the victim. There are specific criminal laws such as the Foreign Corrupt Practices Act and creating a public nuisance to deal with failure to meet a standard of due care. Denning wants to make unauthorized entry into a system at most a misdemeanor if certain standards have not been followed by the owner. But unauthorized entry alone can do tremendous damage and deserves felony status in some cases—for example, in a time-sensitive process control computer that normally has protection but was vulnerable during a momentary lapse. We must not bind the hands of the criminal justice system in dealing with simple break-ins that are made with intent to cause massive losses.

Denning calls the majority of readers of hacker publications "impressionable young people who are the foundation of the future." I dispute this generality. In 20 years of interviewing malicious hackers, I have found that many spent their teen years in a culture dedicated to antisocial behavior, and that they lie, cheat, exaggerate, and steal, as a matter of course. Understanding the hacker culture does not mean that we must accept the hackers' "program" and values.

Contrary to popular belief, there is no single profile of malicious hackers. There is a broad spectrum of individual wrongdoers, each having a unique motive and rationale for the offense; each having a different set of ideals, ethics, family background, peer relations, goals, education, religious beliefs, and other values. Malicious hackers range from pranksters to attention seekers, followers (groupies), hero idolizers, antisocial aberrants, delinquents, occasional or part-time criminals, career criminals, extreme advocates, and terrorists. Therefore, solutions must also be highly varied and precisely applied, because if not carefully matched to the particular individuals, they will fail. For some young hackers, a strong dose of applied ethics and law instruction will suffice. For others, forced removal from a peer group and use of computers is necessary. For some, severe financial penalties on parents may work. Some require criminal convictions with light to severe sanctions, including incarceration. We, as computer professionals and scientists, can play personal roles—one on one—and can also help with ethical instruction as a group. However, many of the solutions require the efforts of competent and experienced psychologists, social workers, penologists, probation officers, law enforcers, prosecutors, defense lawyers, judges, and legislators. We must also work indirectly by educating, encouraging, and supporting these other professionals in their work.

The broadest and best solution to the many malicious hacker problems I have seen was expressed by Senator Pat Leahy (D-VT) in his opening remarks to a U.S. Senate subcommittee meeting on October 31, 1990: "As a prosecutor for more than eight years in Vermont, I learned the best deterrent for

"The human mind has a great capacity to rationalize its own conduct."

**SHELDON ZENNER**
**Attorney**
**Represented Craig Neidorf**



"It is important to have people around who challenge our assumptions."

**KATIE HAFNER**
**Author**
**On the worthwhileness of hackers**



"Hackers don't go around reading other people's electronic mail. It's boring."

**FRANK DRAKE**
**Editor**
***W.O.R.M.***
**(defunct cyperpunk magazine)**

crime was the threat of swift apprehension, conviction, and punishment. Whether the offense is murder, drunk driving, or computer crime--we need clear laws to bring offenders to justice!"

Shouldn't our limited time be spent encouraging and supporting young people whose behavior is good, as an example for the bad ones? Shouldn't we leave the determined offenders to the systems of juvenile courts, social workers, and other professionals that we as a society have established? Shouldn't we, as Denning recommends, be devoting our time to persuading young people, before they enter that dark culture, that their success in our field depends on behaving ethically and obtaining the formal education that we have established? Shouldn't we be supporting and educating the law enforcers who are sworn to uphold our civil rights and protect us from crime by working with them instead of complaining about their shortcomings and giving aid and comfort to our adversaries?

DONN B. PARKER
*Senior Management Systems Consultant*
*SRI International*
*Menlo Park, Calif.*

The most striking aspect of Denning's account is the government's willingness to investigate and prosecute without ascertaining whether the effort is justifiable. Not only was the government case nonexistent on a legal basis, but the effort was a questionable priority for an investigative institution with limited resources. After the government spoke to Neidorf and found him anything but malicious, what could have been gained by bringing him to trial? Nothing, unless the motive was to "set an example" to other youths who flout authority.

In short, the *Neidorf* case begs for an investigation as to why the hacker culture—which on balance has been a boon for our economy and intellectual vitality—is seen by certain officials as something to be stamped out. While Denning's conclusions are reasonable, I think that some deeper questions remain. In my point of view, the problems we are seeing in electronic publishing, constitutional rights, and hacking are not caused by hacker criminals, which despite the wide-open nature of our computer systems have yet to grind the wheels of computation to a standstill. No, the difficulty seems to be in getting these rights extended to the electronic realm. And certainly matters are only made more difficult by the government's scapegoating a small, though high-profile, group of high-tech antiauthoritarians in the hope that our security will be heightened by throwing a few teenagers in jail.

STEVEN LEVY
*Author of "Hackers: Heroes of the Computer Revolution" (Doubleday, 1984)*
*N.Y., N.Y.*

Denning has summarized a number of concerns about the use of computers, personal freedoms, and criminal prosecution. The topics are broad and difficult to discuss briefly, but she touched upon many important concerns. With the exception of a small disagreement with one of her conclusions, my comments are directed to adding further material for the reader to consider.

First, I think it is necessary to realize that while there have been examples of improper prosecution of computer-related incidents, such as the *Neidorf* and *Steve Jackson* cases, there have also been a number of quiet, fair, and successful prosecutions at the state and national levels. Crimes related to computers have occurred, are occurring, and will continue to occur; the need for effective law enforcement and prosecution will only increase as our internetworking of systems and our reliance on computer technology increases.

Most of the prosecutors and investigators I have met over the years are well-meaning, earnest people. They are concerned about the need to temper rigorous law enforcement with a hefty respect for civil rights and liberties. Unfortunately, when it comes to computers, they are often at a loss. Computing courses are not required in law school or criminal justice programs. As a result, most law enforcement personnel are without the necessary background to understand the subtleties involved in computer-related investigations. Often, they are forced to rely on outside advice—with unfortunate results if their advisors are inappropriate, poorly informed, or biased.

Part of this gap in understanding undoubtedly exists because computer technology is so new and, in many ways, unpolished. Until recently, people in law enforcement and the justice system have had little need to understand issues of networks and computer security. Also, not until recently has there been any substantial concern within the profession to make computing and policy issues concerning computers accessible to "outsiders." I think it is clear that, in addition to pointing out the instances in which those individuals who make and enforce our laws make mistakes, we need to make a better effort to educate and assist them. As Denning notes in her conclusions, we must try to understand all the various perspectives involved in the application of the law to computers.

My second general comment regards potential applications of Fourth and Fifth Amendment rights to computing technology. I believe part of our problems here are a direct result of our successes. Technology has made it possible for

a business to fit equivalents of its filing cabinets, typewriters, printing equipment, mailboxes, telephones, billing department, encryption material, address books, fax machine, customer records, payroll, and more into a small computer system. The result is a greatly heightened vulnerability to fire, theft, sabotage . . . or execution of a search warrant.

As Denning noted, searching millions of bytes of storage for evidence is not a quick or simple task. It is complicated by the many places where information may be stored. Data can be written to blocks on a disk marked as "bad," and added between software-defined disk partitions. Data can be stored offline on other media, such as cassette tapes, which may be mislabelled and stored away from the computer system itself. The data may even be stored in nonvolatile memory of peripheral devices, such as laser printers and autodialers. Someone wishing to conceal computer data from searchers has many options available. Furthermore, a suspect does not even need to hide illicit data on a personal system. The data can be hidden at school, at a place of employment, or on a hobbyist bulletin board system, all without the rightful owner knowing of the act.

If the material is required for a successful investigation and prosecution, it is necessary to obtain it all at once, as computer data is easily destroyed. This usually requires confiscation of everything that can be used as storage, including tapes, printouts, and the I/O devices that may have written them in nonstandard format. (Anyone who has suffered the frustration of transferring diskettes between PCs with misaligned heads should be able to understand this.) Items that may not be recognized by the owners as possible storage places, such as the tapes in an answering machine, may also need to be seized.

After material has been seized, it may require weeks or months of effort to properly search all that has been confiscated. After the search is completed, the system may need to be held for potential use at a trial to be conducted after further investigation is completed. During all this time, the owners are deprived of use of the equipment and may suffer unduly.

I am not convinced that these are instances of over-broad searches that should be prohibited so much as they are instances of undue reliance on the technology. As I suggested earlier, many of these same systems might be completely wiped out by a fire or malicious act because of their centralized nature. Developing mechanisms to allow suspects to get copies of seized media as suggested in the editorial may not, in itself, be enough. I believe that a combination of methods—including stronger requirements on the evidence required to obtain a warrant, better education of law enforcement agents, and perhaps less reliance on computers by users—is also necessary. This problem requires considerably more thought before it can be solved.

My third comment regards Denning's implication that First Amendment rights naturally extend (or should extend) to computer communications. I am very hesitant to endorse such a position without qualification. I certainly believe that freedom of expression is a precious right to be protected. At the same time, I am concerned about the limits of such expression, because what we *express* with computers has so many new and unforeseen dimensions. Would sending a computer virus or worm (not the source code—the executable) through electronic mail be protected as a form of expression? Should the use of other people's computers and networks for the propagation of bulletin boards and mail be something that could not be regulated? Would instigating an

"We reveal and report on what is happening, but we are not a how-to magazine for hackers. Our subscribers range from 10-year-olds to secret service agents worldwide."

EMMANUEL GOLDSTEIN
**Editor**
*2600 Magazine*
**(A hackers' quarterly)**

"The computer underground is a marginally deviant subculture. It's not as sophisticated, not as conspiratorial as once thought; and it's not full of antisocial sociopaths as once described."

GORDON MEYER
**Coeditor**
*Computer Underground Digest*

email flood that causes a machine to crash be a protected form of expression? Is it perhaps naive to speak of First Amendment rights when we are referring to communications that potentially cross our national boundaries into countries that have different traditions of individual rights?

My ambivalence on this issue is tinged with real alarm at incidents such as the attempted banning of Usenet newsgroups at Stanford University, the University of Waterloo, and other institutions. I believe the increased incidence of efforts to ban books, movies, telecasts, and artwork viewed as obscene, racist, blasphemous, or otherwise contrary to the narrow interests of some individuals should not be allowed to creep further into the realm of computer communications. At the same time, I believe we should be cautious that we do not end up with a situation where disruptive and destructive behavior on the networks is (accidentally or otherwise) given constitutional protection. Neither do I think we want a future where computer users in the U.S. are prohibited from connecting to international networks because local (U.S.) law protects them as they ignore international law and custom.

My last comment to Denning's thought-provoking editorial is directed to her conclusion that simple unauthorized computer intrusions should not be considered serious (i.e., considered as a misdemeanor). Here, I must disagree. Although I believe that the computer operators should bear some responsibility if they have not followed reasonable security precautions, I do not believe a reduction in charges is the way to do it, for it does not directly impact them as intended. Instead, it rewards the perpetrators of the illegal acts, possibly because of an accident or oversight. For instance, I would not expect that criminal charges would be reduced if someone illegally entered my house because I forgot to lock the door one night.

A better method would be more analogous to what happens in cases of car theft: car thieves do not receive a lesser charge if the keys are left in the ignition; however, the owner may find that his or her insurance provides reduced or no recovery in such cases. Breaking into a computer is wrong, and is not something that is done accidently —the intruder must actively seek entry.

Likewise, the lack of appreciable damage should not be grounds to reduce a charge, although it should certainly be considered as a mitigating circumstance during sentencing. Considerable damage has been caused by people who were "just looking around" on others' systems. Furthermore, for the victim, it is often impossible to tell what has actually occurred during such an incident, and recovery must often be performed as if a more substantial attack had been made. To the victim, any break-in is likely to result in considerable effort. Furthermore, reducing the charges because of minimal actual damage fails to take into account intent and ability—intruders apprehended immediately after breaking in may not yet have had an opportunity to cause damage, nor should they be given the opportunity to do so.

In closing, I second the comment in Denning's conclusion about the necessity of bringing these discussions into classrooms and professional forums. The editorial raises some very important issues that we need to continue to discuss and consider. The computing profession, as represented by such organizations as the ACM, should be helping to guide the development of fair and just laws, not merely reacting to cases like that of *Craig Neidorf* and *Steve Jackson Games*.

EUGENE SPAFFORD
*Assistant Professor*
*Purdue University*
*W. Lafayette, Ind.*

My comments on Denning's editorial come from three different perspectives: as chair of the ACM Committee on Scientific Freedom and Human Rights (SFHR), as a person who studies the field of secure systems, and as a private citizen.

There are four issues that are addressed in the editorial: (1) Should electronic publications be accorded the same [First Amendment] protection as printed ones? (2) Should the government be constrained in what can be seized for evidence? (3) Should the operators of electronic bulletin boards be held accountable for what is published on the boards? (4) Should there be a range of offenses for electronic "breaking and entering"? There is another, overriding issue that the editorial addresses: (5) How can we, as computer scientists, deal with the *hacker hysteria* that seems to be sweeping through the law enforcement agencies in this country?

Let us start with (5). The SFHR has historically been concerned with issues of discrimination against computer scientists, especially where the discrimination was based on one hysteria or another sweeping a country. Hacker hysteria is difficult to counter, because there are real crimes being committed, and in some cases the hackers themselves attempt to justify the crimes in the name of freedom of information. The SFHR has not been formally polled on this issue, but our general approach has always been that the laws of a country, and the commonly accepted rules on the humane treatment of individuals, must not be swept aside by some hysteria. In the case of hacker hysteria, the problem partially arises from the discovery by the media and others that the growth of computer technology has left us all vulnerable in mysterious ways to technologically induced

failures. At Denning's panel discussion on the hacker culture at the 13th National Computer Security Conference (Oct. 1990), an audience member stood with tears on his face as he described his son in intensive care and his fear that some hacker could change the automatic monitoring system on the computer that was keeping his son alive. We are using computers, networks of computers, in situations that are very scary, and the idea that someone can cause harm to happen is dreadful. The answer that a panelist gave the man—that no responsible hospital would or should allow outside access to that computer, is not enough to reduce the scare, and did not satisfy the man. What can we do to help calm this hysteria, and to be certain that human rights and scientific freedom are not swept away by it?

Denning's editorial is an excellent example of what we can do. We can focus on the facts of the situations, and refuse to participate in the hysteria. The four issues raised relate precisely to the facts of the situations: (1) Should electronic publications be accorded the same protection as printed ones? If computer scientists are to be given the same rights as everyone else, the answer to this question clearly must be "yes." (2) Should the government be constrained in what can be seized for evidence? Again, computer scientists must be allowed to continue their work, even when accused of a crime. There need to be clear constraints on what is seized for evidence, and for how long. (3) Should the operators of electronic bulletin boards be held accountable for what is published? To reduce the free exchange of information on electronic bulletin boards is not in the service of democracy. Is the telephone company liable for what is said over telephone lines? No.

The question of a range of offenses for electronic breaking and entering (4) needs to be expanded upon. Many of the hackers are boys who are using hacking as previous generations used peeping-tomism or minor trespassing: for the sense of adventure, to satisfy curiosity, etc. In the suburb in which I live, I once had the experience of a local teenage boy breaking into our house and doing various nondestructive things. When the police were called, they did not take the invasion of privacy very seriously: no man-hunt, no breaking down doors, they didn't even dust for fingerprints. Yet I experienced precisely the same feeling of invasion as I did when someone broke into a computer I was using at work. I do not condone either case: I simply say they are the same. Each action that can cause harm if your computer is broken into can be translated into an action that can cause harm if your home is broken into. So having a range of offenses, comparable to the range of offenses that exist for breaking into homes makes sense: walking into a house that is not locked is still a crime, but less of a crime than breaking down a wall and destroying everything in sight; and the most severe situation is one in which property is stolen or people are hurt. These ranges need to be built into the laws.

As one who studies security issues, I must say that this hysteria is truly misplaced. It continues to be reported that those who do the most harm to systems are those who have a right to use those systems: the hospital maintenance person is more likely than a hacker is to load the wrong program and cause a problem. Security features must be appropriately viewed, of course; to do less is irresponsible. But also we need to understand how to assure the correct functioning of this technology.

PAULA HAWTHORN
*Chair*
*ACM Committee on Scientific Freedom and Human Rights*
*San Jose, Calif.*

The *Neidorf* case demonstrates the need to view the recent spate of prosecutions against computer hackers with some skepticism. The government pressed its charges against Craig Neidorf on all fronts. Spurious allegations were made in the national press as well as the courtroom. Without good legal assistance and the help of computer experts, Neidorf might well have gone to jail based on charges that should never have been brought. This case should make clear to both prosecutors and the public that fear and ignorance provide a weak foundation for a criminal indictment.

Computer-related crime is likely to be a growing problem in this country. More valuable information will be stored in computer systems and more financial transactions will occur on computer networks. Investigating and prosecuting these cases will pose new challenges for the law enforcement community, the courts, and the legislators. As Denning's editorial shows, computer scientists will also have an important responsibility in helping to sort out complex technical questions.

At the same time, both professionally trained computer scientists and the public should be wary of any prosecutions directed toward the exchange of digital information, as opposed to acts of destruction or theft. The tendency in some quarters to view information itself as a threat is at odds with the First Amendment and our system of open government. This is not a technical matter; it is a reflection of a system of government that is intended to promote the exchange of information and the protection of individual liberty.

Our laws draw a clear line between words that may cause harm and acts that result in actual harm. If we did not make such a distinction, the shelves of many libraries

and the racks of many newsstands would be left bare. Mystery novels and history books might well be restricted because some passages describe criminal acts, or other passages recount acts of espionage. Computer scientists should be particularly cautious about government efforts to restrict the exchange of information because of the importance of the free flow of information to computer networking and technical innovation.

Recognizing the right of Craig Neidorf to publish *Phrack* is not an endorsement of the views expressed in *Phrack*. It is for each person to decide whether *Phrack's* editorial policies are appropriate or responsible. However, it is not the government's role to make such a judgement, and its heavy-handed efforts to silence *Phrack* were potentially as threatening to a new generation of electronic publishers as they were to Craig Neidorf.

As a matter of legal precedence, the *Neidorf* case is not significant. No legal issues were adjudicated and no new law was established. But the case has helped to raise important questions about the prosecution of computer crime and the importance of digital networks for the exchange of information. These issues require further exploration and the best efforts of all who are interested in the future development of digital information systems.

MARC ROTENBERG
*Director*
*Computer Professionals for Social Responsibility*
*Washington, D.C.*

If the Electronic Frontier Foundation wants a speechwriter like President Bush's, Dorothy Denning is the ideal candidate. Her article offers a "kinder, gentler" perspective on the dynamic which involves young computer enthusiasts, law enforcement, and computer security professionals. Mildly, sweetly, she reports little that she did not personally experience, and thus suggests much more than she states.

A master of understatement, she notes without comment that the Secret Service secretly videotaped Craig Neidorf and others drinking beer and eating pizza. This investigation, if that is what is was, occurred through a two-way mirror for 15 hours, at SummerCon '88 in St. Louis.

Why, concerned citizens and taxpayers will want to ask (perhaps with greater anger than Denning demonstrates), would professional law enforcement personnel go to such lengths? Demonstrating the eternal verity of the cliche that a little knowledge is a dangerous thing, the agents had apparently taken as gospel the announcement that The Phoenix Project would begin at this conference. The announcement, Denning tells us, stated the goal of a community where "Knowledge is the key to the future and it is FREE." Clearly, this was probable cause to suspect a devilish conspiracy was afoot!

Without this piece of historical perspective, we might be tempted to echo the optimistic view of law enforcement suggested by John Barlow in his now classic "Crime and Puzzlement." Barlow seems to believe that law enforcement officers investigating computer crime are nothing more than a bunch of blunderers, needing little more than technological training to return to the path of righteousness and respect for the American way. Somehow, I find it hard to agree.

I have read the search warrant which eventuated in the seizure of large quantities of computers, print and computer media from Steve Jackson Games in Austin, Tex. I have read a number of the briefs in the *Craig Neidorf* case. Frankly, I find the seizure at Steve Jackson Games unconscionable. At best, prosecuting Craig Neidorf for republishing material wrongly alleged to be valuable proprietary information was enormously stupid. Could these two cases be the consummation of two years of investigation? It seems to me that what we have here is more than technological time lag.

I suggest we are looking at "paranoia a deux." This is a unique dance in which each participant draws strength and support to the extent it can portray the other as frighteningly strong and unprincipled. Its most potent current manifestation is the posturing between Sadaam Hussein and George Bush. Closer to home, the suggestion of a war against computer crime evokes similar passions.

Those symbolizing the establishment (i.e., law enforcement) and those symbolizing the antiestablishment (i.e., the "dreaded hackers") can alternately deify and villify each other, neither group showing much interest in its relation to society as a whole.

Aside from the restraint that makes her observations so palatable, Denning's article is refreshingly commonsensical. Understand those whom you would pursue and punish, she tells us.

Consider the extensive resources devoted to the investigation now commonly called Operation Sun Devil. How much money does it take to justify a two-year surveillance extensive enough to involve spying on pizza parties and violating legitimate businesses' constitutional rights? How much fear of hacking was required to *sell* this expense to the higher-ups in the Secret Service, and various state and federal prosecutors' offices. It required more fear, I believe, than any documentation of Operation Sun Devil has yet shown. Instead, what I see looks more like a case of inadequate reflection.

In fact, lashing out at hackers with an operation as mammoth as Operation Sun Devil is like throwing a brick at a mirror. Like it or

not—and clearly there are many in law enforcement who do not—Craig Neidorf, Steve Jackson, and those who fancifully call themselves the Legion of Doom, are saying no more than rock star Boy George: Before his fall from the public eye, the cross-dressed dandy sang persuasively, pouting into the camera, "I'm the boy you made me." *Hackers* reflect social values: technological competence and impatience with the property claims of others. We continue to reward wizardry and ignore ethical behavior. Is it surprising when our young people get our message?

I hope many of Denning's colleagues will join her research. Confronted by a new form of social action, we need to be more reflective, and not simply try to destroy our reflections.

J.J. BUCK BLOOMBECKER
*Director*
*National Center for*
*Computer Crime Data*
*Santa Cruz, Calif.*

I concur with Denning's suggestion that unauthorized access to a computer should not be a felony—but this does not go far enough. The concept of justice is that only actions that unjustly harm other people should be crimes. Unauthorized access in itself harms no one, and thus should not be a crime at all.

Security measures are precautions—one method of preventing various actions (including some such as destruction of data) that we can agree are crimes. However, breaking security does not imply such actions.

The harmless failure of a precaution may raise concern regarding its effectiveness, and may suggest that modifications are needed to reduce future risk; but it is not in itself a problem demanding a remedy. In this situation, the means (security) have failed, but the desired end (avoiding harm) has been achieved anyway. Punishing unauthorized access confuses means with ends.

Unauthorized access is sometimes compared with trespassing. They are similar in some respects, but this does not imply they must be judged alike. We do not, for example, have laws against unauthorized use of a typewriter.

In addition, the analogy with trespassing fails to support the proposed laws. To treat unauthorized access as "computer trespassing" would suggest a penalty comparable to that for real trespassing. In Massachusetts, this is one night in jail—worth avoiding, but not a serious matter. The Massachusetts state legislature, with this analogy in mind, rejected a computer crime bill several years ago because the proposed penalties seemed disproportionately severe.

Certain activities—while not harmful in themselves—are prohibited because they are considered clear evidence of intent to commit a real crime. Unauthorized access is not such evidence because most security breakers do no harm and intend none.

A breach of security may put a person in a position to commit a crime. Some would transfer the seriousness of these potential crimes to the act of security-breaking itself; but this would be inflicting punishment for crimes that have not been committed.

Serious potential crime situations occur frequently in everyday life. For example, whenever two strangers pass on a street, one could attack the other. This suggests punishing the crime of unauthorized presence on the street. Earlier this year a black man was arrested for being in Wellesley, Mass. The police applied the reasoning that blacks were unlikely to be authorized users, and concluded he must have been a criminal. This became a scandal because the man was famous; otherwise it would not have attracted attention.

Ultimately, laws against unauthorized access (or unauthorized anything) reflect the urge to control the actions of other people—a spirit of regimentation, in which the greatest crime is disobedience. This spirit is incompatible with a free society.

But what about the practical need for such laws? Carefully maintained computer security is effectively impossible for casual visitors to break. It is superfluous to prosecute offenses than can more easily be prevented.

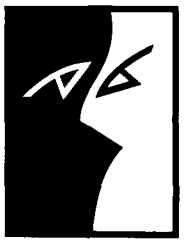
However, criminalization does cause practical difficulties for computer systems where strict security is not intended.

Many adolescent crackers are obsessed with security-breaking which they think of as a hobby and a challenge. They face a temptation to do harmful things, but most of them resist it. When they visit a system, it is important to communicate with them, to encourage them to use their skills in a useful fashion.

However, when unauthorized access is a crime, crackers are understandably afraid of communicating with anyone who might perhaps be planning to betray them to the police. Even if we have no such intention, there is no convincing way we can reassure them.

This inability to communicate has the paradoxical effect of increasing the likelihood that crackers will harden and move to actual crime—the opposite of what criminalization is supposed to accomplish.

RICHARD STALLMAN
*Founder*
*GNU Project*
*Cambridge, Mass.*



# Denning's Rebuttal

The electronic media have given us new paradigms for communicating, publishing, and conducting business. My colleagues' comments demonstrate significant disagreement on the interpretation of these paradigms, and they make clear these issues are not going to be solved merely by better computer security or law enforcement. Dialogue is essential, and the points of disagreement show where that dialogue is most needed.

I would like to comment on four areas in which there is no clear agreement: whether there is a "hacker crackdown"; whether unauthorized entry alone is damaging; what penalties are appropriate when security is lax; and how young people who break into systems or allegedly aid and abet crime should be treated.

With respect to the crackdown, I agree with Parker that law enforcers are not taking disciplinary action on illegal hacking as a result of fear generated by well-publicized incidents, as I incorrectly suggested in the opening paragraphs of my article. Neither are they attempting to stamp out legal hacking or throw a small group of high-tech, antiauthoritarian teenagers in jail in order to enhance security, as suggested by Levy. Rather, law enforcers are responding to crimes reported by companies whose losses were sufficiently great to justify prosecution. Operation Sun Devil was the result of extensive credit card and toll fraud, and not a fear of hacking as BloomBecker states. I do not see what Hawthorn calls "hacker hysteria" in the law enforcement community. Instead, I see an honest effort to be more responsive to computer crimes which have taken place.

I also agree with Parker that the outcry over computer seizures and indictments has been prompted by only a few incidents—mainly the *Neidorf* and *Steven Jackson* cases.

Neither of these cases was part of Sun Devil. I chose to write about the *Neidorf* case because there are important lessons to be learned from it and issues to be discussed.

I agree with Parker that we should support law enforcers, but I disagree with his view that we should not raise concerns when we see shortcomings. Doing so generates the opportunity for a different outcome in the future.

The small number of complaints should not obliterate the fact that most hacking cases have been handled well. Law enforcers typically show considerable respect for civil liberties and an understanding of juvenile delinquency. There is a wide spectrum of hackers and hacking cases, each requiring different treatment. From what I have observed, law enforcers are savvy to those differences.

The second area of disagreement is whether unauthorized entry into a computer system is in itself damaging. When Stallman says that unauthorized access that does no harm should not be considered a crime, he takes the position that it is not damaging. His view reflects his fundamental belief that all generally useful information, including computer software, should be in the public domain. He says that most people who have gained access to his system have not damaged files or disrupted service. He believes that most young people break in for the challenge and to learn rather than to cause harm. Parker's use of the term "malicious hacker" to denote any person who enters a system without authorization shows a contrary view—that unauthorized entry is in itself harmful. Parker's view reflects his observation of many cases where intruders disrupted service, stole trade secrets and credit reports, read private email, ran up huge phone bills, and modified files. Spafford also points out that considerable damage has been caused by people who were "just looking around." Even when there is no explicit damage, an intrusion is disruptive because steps must be taken to remove the intruder and restore the system to a protected state.

Since many hackers do not see unauthorized access as harmful, we need to educate young people about the costs of their actions on organizations and why, as Parker points out, unauthorized access is regarded as a violation of the rights and property of others. At the same time, I agree with Stallman that we must be careful that we do not punish people for actions they could have committed, but had no intention of committing.

The role of computers in society has changed dramatically from the early days of computing. Organizations now use computers to support life-critical functions, keep track of sensitive information, and manage business operations. In such environments, unauthorized access cannot be tolerated, and so it is reasonable that our values and laws reflect that. Computer trespassing is now regarded as blatant rejection of social values.

The third area of disagreement is what penalties are appropriate when security is lax. I agree with Parker that a felony conviction is appropriate when extensive damage was intended or performed, regardless of whether the system was adequately protected. Moreover, I see merit in his position to treat an offense according to the intent of the perpetrator and seriousness of the act, rather than according to the vulnerability of the victim. At the same time, system administrators who permit lax security are culpable for their own negligence.

The fourth area of disagreement is how we should treat young people who break into systems or publish magazines like *Phrack* that allegedly promote criminal activity. Parker calls them our adversaries and suggests that I have given aid and comfort to our adversaries. I believe that it is our responsibility as adults to help bring young people into the community as responsible citizens. Many young people break the law or encourage others to do so at some time in their lives. Most of them grow up to become responsible adults. While we should not approve of all their actions, treating them as our adversaries is, in my view, likely to alienate them and push them into a lifestyle of crime. ◻

*—Dorothy E. Denning*

**CR Categories and Subject Descriptors:** K.4.1 [**Computers and Society**]: Public Policy Issues—*privacy, regulation;* K.4.2 [**Computers and Society**]: Social Issues—*abuse and crime involving computers;* K.5.0 [**Legal Aspects of Computing**]: General

**General Terms:** Legal Aspects, Security

**Additional Key Words and Phrases:** Computer crime, constitutional rights, electronic publication, enhanced 911 system, hacking

**About the Author**

**DOROTHY E. DENNING** is a member of the research staff at Digital Equipment Corporation's Systems Research Center where she researches computer security and computer crimes committed by young people. Before joining Digital, she served as a senior staff scientist at SRI and as an associate professor of computer science at Purdue University. **Author's Present Address:** Digital Equipment Corporation, Systems Research Center, 130 Lytton Ave., Palo Alto, CA 94301, denning@src.dec.com.