12

Legal Considerations

> The law may not be the most precisely sharpened instrument with which to strike back at a hacker for damages. . . , but sometimes blunt instruments do an adequate job.
>
> —PAMELA SAMUELSON

Thus far, we have dealt primarily with technical matters. But there are legal concerns as well. For example, a certain level of security may be legally required. On the other hand, your ability to monitor certain kinds of activities may be restricted. Also, should you ever wish—or need—to prosecute, your logs may not be admissible in court. All of these matters must be considered when devising a security policy.

Obviously, computer law is a large field. We don't claim to cover it all; that would be material for an entire book. Instead, we restrict our focus to areas of concern to a security administrator: what constitutes illegal use of a computer, what you can and can't do to detect or monitor it, the status of any evidence you may collect, and your exposure to civil liability suits in event of a security problem.

Our advice should be taken with a certain quantity of salt. For one thing, we are not lawyers. For another, our comments are based primarily on U.S. federal law; individual state laws can and do vary, as we have noted in a few instances. Besides, non-U.S. law is likely to be completely different. A general overview of that aspect can be found in [Sieber, 1986], although its age is starting to show.

Finally, computer crime law is a new field. The statutes are quite recent, and there is little case law for guidance. Interpretations may change, perhaps radically, in the future. Indeed, the laws themselves may change, as legislators react to newer threats.

12.1 Computer Crime Statutes

The primary U.S. federal law against computer crime is the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, which was used to prosecute Robert Morris[1] in the famous Internet Worm case [Spafford, 1989a, 1989b; Eichin and Rochlis, 1989; Rochlis and Eichin, 1989]. It proscribes a number of forms of computer crime, including illegally obtaining classified information and obtaining financial information from a bank or credit-card issuer's computer.

Other subsections are more generally applicable, but are restricted in very important ways. For example, it is illegal to connect to a U.S. federal agency's computer if and only if you have no legitimate access to other computers belonging to that agency. The drafters of the law envisioned that intradepartmental computer abuse was best dealt with by administrative sanctions, rather than by criminal law. Furthermore, your access to such a computer must "affect" the government's use of that computer for the activity to be illegal under this statute.

Simply connecting to, or even using, a *Federal interest computer* is *not* illegal under this statute, unless your activities are part of a larger fraudulent scheme, cause more than $1,000 of damage, tamper with medical records, or interfere with authorized use of the computer. A "Federal interest computer," incidentally, is a government computer, a financial institution's computer, or two or more computers involved in the offense, if they are located in different states.

Trafficking in stolen passwords is also barred by this act and by 18 U.S.C. § 1029. Again, the law contains qualifications; not all stolen passwords will leave someone liable under these acts.

Messages stored on a "a facility through which an electronic communication service is provided"[2] are protected by the *Electronic Communications Privacy Act* (*ECPA*). In this case, simply reading messages without proper authorization (or, of course, tampering with them, or blocking access to them) is illegal. As discussed later, this protection does not apply to ordinary corporate or university machines; the intent is to provide similar protections to users of public mail services as are provided to telephone callers.

Depending on the circumstances, other U.S. federal statutes may apply. The law against theft of federal property[3] is broad enough to cover some cases of illegal computer use, for example [Gemignani, 1989]. Other possibilities include the laws against mail fraud,[4] wire fraud,[5] and possibly even the law against false statements.[6]

Often, state law is more stringent. For example, under California law,[7] someone can be convicted who "knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network." No evidence of damage or maliciousness is necessary, though the penalties are more severe if such has occurred. The statute also provides for civil damages, including specifically "any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data

[1] *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991).

[2] Electronic Communications Privacy Act, 18 U.S.C. § 2701(a)(1).

[3] 18 U.S.C. § 641.

[4] 18 U.S.C. § 1341.

[5] 18 U.S.C. § 1343.

[6] 18 U.S.C. § 1001.

[7] California Penal Code § 502(c)(7).

A Very Brief Introduction to Legal Notation

> Pope moved that we strike from the State's brief and appendix a selection from the Year Book of 1484 written in Medieval Latin and references thereto. The State provided no translation and conceded a total lack of knowledge of what it meant. The motion is granted.
>
> —*Pope v. State of Maryland*, 284 Md. 309, 396 A.2d 1054 (1979)

Because this chapter deals with legal matters, we have used standard legal notation for references to cases and statutes. The full set of rules is rather complex; indeed, the notation is the subject of entire books [BB, 1991]. We are using a simplified version of it. Our citations are of the form

Common name, volume work page (year).

The key part is the triple "volume work page." That is, the particular reference is part of some series of books that may encompass hundreds of volumes. Works cited here include the *Federal Reporter*, *Second Series* (F.2d), the *Atlantic Reporter*, *Second Series* (A.2d), and the *Federal Supplement* (F. Supp). The particular case in each book is the one that begins on the specified page. That is, the physical form is authoritative, rather than some indirect notation involving a case serial number. If a case is reported in more than one work, several of these triples can appear. The parenthetical giving the year of the decision sometimes includes the name of a court, if that is not implicit in the name of the book.

For statutes, the format is similar, but the "volume" refers to a "Title" of the law, and the page number is replaced by a section number. Thus,

18 U.S.C. § 2510

refers to section 2510 of Title 18 of the *United States Code* (U.S.C.). Full citations often include in parentheses the year the law was last amended; we have omitted it.

was or was not altered, damaged, or deleted by the access."[8] That is, in the event of an intrusion you may be able to recover the costs of checking for damage, even if none has actually occurred.

12.2 Log Files as Evidence

Unlike the material in the following sections, the question of how computer printouts can be admitted as evidence has been extensively studied. This is not surprising, given the ubiquity of computers in business. Still, security logs present some unique questions.

The basic problems are technical in nature. First, and most obvious, forging computer logs is trivial. The same commands that let us obscure the names of attacking sites for this book would let us insert any names we wished in our logs, including yours. Second, even assuming an absence of malice on our part, computer systems have a less-than-sterling reputation for reliability. The hardware is almost certainly working properly; the software, though, is another matter entirely. Is your logging software correct? Can you prove it in court?

The legal strictures mirror these two points. First, computer records are not normally admissible as evidence *per se*; rather, they must meet various criteria to be admitted at all. That is, appropriate testimony must be presented to show that the logs are accurate, intact, etc. Second, the records must be authenticated. We will discuss each of these issues in turn.

To start with, computer records are legally classified as *hearsay*. That is, they are not the oral testimony of a witness. In general, hearsay testimony is not admissible in court under the *Federal Rules of Evidence*.[9] However, there are a number of exceptions that are often applicable to computer-generated output.

The most important such exception covers *business records*:[10]

> Records of regularly conducted activity — A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. The term "business" as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.

Quite a lot is covered by that mouthful; we will dissect it piece by piece.

First of all, the logs must be created reasonably contemporaneously with the event. Information gathered at some remove does not qualify. Second, the information must be recorded by someone with knowledge of the event. In this case, the recording is being done by a program; the record therefore reflects the *a priori* knowledge of the programmer and system administrator.

[8] California Penal Code § 502(e)(1).

[9] Fed. R. Evid. 802.

[10] Fed. R. Evid. 803(6).

The most important proviso is that the logs must be kept as a regular business practice, in furtherance of the business. Random compilations of data are not admissible. Similarly, logs instituted after an incident has commenced do not qualify under the business records exception; they do not reflect the customary practice of your organization. On the other hand, if you start keeping regular logs *now*, you will be able to use them as evidence later.

It is also helpful from a legal perspective if you actually make some use of your own information. Doing so, and being able to prove it, demonstrates your own faith in its correctness: if you actually rely on it for your own purposes, it is more likely to be accurate. In our case, we use the mail logs for normal postmaster duties, and we regularly follow up on all apparent security incidents. This track record—scrupulously logged, and whose accuracy is implicitly recognized by the positive responses we have received from system administrators around the world—would be potent testimony to the general integrity of our traces if they were challenged in court.

The business records exception goes on to note that a "custodian or other qualified witness" must testify to all of the previous conditions, and to the accuracy and integrity of the logs. This process is known as *authentication*.[11] The custodian need not be the programmer who wrote the logging software; however, he or she must be able to offer testimony on what sort of system is used, where the relevant software came from, how and when the records are produced, etc. It is also necessary to offer testimony as to the reliability and integrity of the hardware and software platform used, including the logging software.[12] A record of failures, or of security breaches on the machine creating the logs, will tend to impeach the evidence. The point cannot be stressed too highly in this context: if you are claiming that a machine has been penetrated, log entries from after that point are inherently suspect. Log files accumulated on a still-secure machine, as recommended in Section 4.7, are much more valuable, though the generation process might still be viewed with a jaundiced eye.

Anything that tends to increase the apparent validity of your records will help. Thus, output from commercial software is more valuable as evidence than output from homegrown software. You would do far better to persuade your vendor to improve logging than to add your own, though the latter is better than nothing. If nothing else, your own logs will help protect you, even if a judge does not like them for fear they've been tampered with:

> The integrity of the report-generated program, operating system, and computer system cannot be ensured on a practical basis. . . . [T]otal trust must be placed in the technologists and vendors who designed, implemented, and maintain the products. The more widely used a product is and the more reputable the vendor, the greater the likelihood of its integrity; nevertheless, it takes only one individual with sufficient skills, knowledge, and access to secretly modify it [Nat, 1979].

Similarly, logs kept on a WORM device are obviously less vulnerable to charges of tampering. In high-threat environments, it might be useful to use a digital timestamping service (i.e., [Haber and Stornetta, 1991a, 1991b], as described in Section 13.1.8). Files obtained from the other party—say, through search warrants or the *discovery* process in a civil suit—are also admissible as evidence.

[11] Fed. R. Evid. 901.

[12] Fed. R. Evid. 901(b)(9).

An exception to the hearsay rule[13] provides that any statements made by opponents and damaging to them are admissible.

This cuts both ways: in a civil lawsuit against the alleged hackers, anything in your own records that would tend to exculpate the defendants can be used against you. Your own logging and monitoring software must be made available to them, to permit them to attack the credibility of the records. But under certain circumstances, if you can show that the relevant programs are *trade secrets*, you may be allowed to keep them secret, or disclose them to the defense only under a confidentiality order [Arkin *et al.*, 1992].

If a stored file itself is at issue—say, a program that an intruder has altered, or the text of an uploaded Trojan horse—it may be introduced as evidence without running afoul of the hearsay rule [Arkin *et al.*, 1992; Bender, 1992]. The file itself *is* the evidence; you are not trying to use its contents as testimony as to other facts. But such files must still be authenticated in the usual way.

In all cases, the original copies of any files are preferred. However, duplicates are admissible unless there is substantial doubt as to their authenticity.[14] For these purposes, a printout of a disk or tape record is considered to be an original copy,[15] unless and until judges and jurors come equipped with SCSI interfaces.

As always, other jurisdictions have their own interpretations. For example, the computer crime statute in Iowa explicitly permits printouts to be used as evidence in such cases, the normal rules of evidence notwithstanding.[16]

The hearsay notion is a creation of English common law, and as such applies primarily in the U.K. and former British colonies, such as the United States and Australia. It does not apply in *Continental law* countries [Sieber, 1986]. The courts there will accept computer records as evidence without bars to its admissibility; however, they are free to evaluate its reliability and worth, as they will with any other form of evidence (as, of course, will U.S. and British courts).

12.3 Is Monitoring Legal?

You have your monitors in place, you notice an incident and call the police, and an arrest and civil suit result. That is, you are arrested and you are sued, not the intruder. Improbable? Perhaps, but it is not a ridiculous scenario. There are indeed some risks stemming from both U.S. federal and state laws. In particular, the ECPA imposes some limits on the sorts of monitoring that can be done. These may apply to the scenario we have described, though we caution you that there is little case law in this field. The U.S. Department of Justice has noted the ambiguity of the law with respect to keystroke monitoring in a formal advisory; see the box on page 203.

The basic restrictions are set forth in various portions of the ECPA: 18 U.S.C. §§ 3121–3127, 18 U.S.C. §§ 2510–2521, and 18 U.S.C. §§ 2701–2711. These laws govern pen registers,[17]

[13] Fed. R. Evid. 801(d)(2).

[14] Fed. R. Evid. 1003.

[15] Fed. R. Evid. 1001(3).

[16] Iowa Code § 716A.16.

[17] A *pen register* is a device for recording the number dialed from a phone. The same statute also restricts the use of *trap and trace device*s; these provide the number of the calling party.

Dept. of Justice Advice on Keystroke Logging (From CERT Advisory CA-92:19, December 7, 1992)

The legality of such monitoring is governed by 18 U.S.C. section 2510 et seq. That statute was last amended in 1986, years before the words “virus” and “worm” became part of our everyday vocabulary. Therefore, not surprisingly, the statute does not directly address the propriety of keystroke monitoring by system administrators.

Attorneys for the Department have engaged in a review of the statute and its legislative history. We believe that such keystroke monitoring of intruders may be defensible under the statute. However, the statute does not expressly authorize such monitoring. Moreover, no court has yet had an opportunity to rule on this issue. If the courts were to decide that such monitoring is improper, it would potentially give rise to both criminal and civil liability for system administrators. Therefore, absent clear guidance from the courts, we believe it is advisable for system administrators who will be engaged in such monitoring to give notice to those who would be subject to monitoring that, by using the system, they are expressly consenting to such monitoring. Since it is important that unauthorized intruders be given notice, some form of banner notice at the time of signing on to the system is required. Simply providing written notice in advance to only authorized users will not be sufficient to place outside hackers on notice.

An agency’s banner should give clear and unequivocal notice to intruders that by signing onto the system they are expressly consenting to such monitoring. The banner should also indicate to authorized users that they may be monitored during the effort to monitor the intruder (e.g., if a hacker is downloading a user’s file, keystroke monitoring will intercept both the hacker’s download command and the authorized user’s file). We also understand that system administrators may in some cases monitor authorized users in the course of routine system maintenance. If this is the case, the banner should indicate this fact. An example of an appropriate banner might be as follows:

> This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel.
>
> In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored.
>
> Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

Each site using this suggested banner should tailor it to their precise needs. Any questions should be directed to your organization’s legal counsel.

wiretapping, and access to computer storage devices, respectively.

Generally, the law prohibits surveillance without a court order. However, there are a number of exceptions. For example, U.S. federal law[18] specifically permits a party to a communication to record it; thus, it is generally permissible for a party to a *talk* session to keep a transcript of it. But this right may be limited under certain circumstances. Some states require the consent of both parties to a communication before recording may take place; obviously, explicit consent is not generally available from hackers.

There appears to have been just one court case involving keystroke monitoring.[19] Unfortunately, it antedates the ECPA, so some of the reasoning no longer applies. (The pre-ECPA statute barred interceptions of oral communications and was silent on data taps.) But the final conclusions of the judges are still enlightening.

In this case, Seidlitz, a former employee of Optimum Systems, Inc. (OSI), used a supervisor's account to dial in to the company computer and download the source code to some valuable software. The login was noticed, a keystroke monitor (the *MILTEN Spy* function) enabled, and phone traces performed. Based on that evidence, the FBI executed a search warrant on Seidlitz's house and office. Various incriminating printouts were found, and Seidlitz was convicted on assorted charges.

In his appeal, he argued, among other things, that the keystroke monitor constituted an illegal wiretap. The Court of Appeals disagreed. They noted that (a) one party to the call consented to the monitoring, and (b) it was not an improper search under the Fourth Amendment, since the monitoring was performed by private individuals, and not at the request of law enforcement agencies. The court further noted that though they did not rule on the question, they had "serious reservations" about any expectation of privacy during the intrusion (their footnote 20). They went on to say (page 159):

> While we base our affirmance of the denial of the suppression motion upon our consideration of the statutory and constitutional arguments advanced by the appellant, and addressed by the court below, we think it appropriate to observe that we discern a certain speciousness which infects all of the illegal surveillance contentions made by the defendant with respect to the evidence which was obtained through use of the Milten Spy. Unlike the typical telephone user who employs the telephone merely as a convenience to converse with other persons over distances, Seidlitz used the telephone to tamper with and manipulate a machine which was owned by others, located on their premises, and obviously not intended for his use. Unlike the party to a personal telephone call who may have little reason to suspect that his words are being covertly recorded, Seidlitz, a computer expert, undoubtedly was aware that by their very nature the computers would record the data he sent and received, and that OSI, also expert in the use of computers, could detect such exchanges if alerted to the presence of an intruder. In this sense the use by the witness below of the term "intruder" to describe an unauthorized user of the computers is aptly applied to the defendant, since by telephonic signal he in fact intruded or trespassed upon the

[18] 18 U.S.C. § 2511(2)(d).

[19] *United States v. Seidlitz,* 589 F.2d 152 (4th Cir. 1978).

> physical property of OSI as effectively as if he had broken into the Rockville facility and instructed the computers from one of the terminals directly wired to the machines. Under these circumstances, having been "caught with his hand in the cookie jar", we seriously doubt that he is entitled to raise either statutory or constitutional objections to the evidence.

The Seidlitz case involved a private computer. Computing and electronic communications service providers are more limited in their right to monitor user activity. Just as phone company personnel may not, in general, listen to your calls, employees of a public electronic mail service may not read your messages, whether in transit[20] or stored.[21]

Some examination can be necessary, of course. It is quite permissible to look at stored files if such a look is necessary to provide the desired service.[22] Thus, a system administrator who attempts manual routing of wedged mail files is not liable under this statute. Similarly, system administrators are permitted to protect their own property. Examination of fraudulent messages is quite permissible, if the intent of the messages is to defraud the service provider.[23] But random monitoring to detect such behavior is prohibited, at least for communications providers.[24] (Even when random monitoring is not prohibited by law, it is, in our firm opinion, quite unethical. Electronic mail deserves the maximum amount of privacy possible.)

Assuming that you have legally monitored an attempted intrusion, you are somewhat limited in what you can do with the information. In particular, you may neither disclose the contents of the intercepted message[25] nor even "use"[26] the information, except internally in the usual course of your job.[27] This would seem to rule out sharing the information with such organizations as CERT.

The situation with respect to private organizations looking at stored files is somewhat murkier. Most companies assert ownership of their computers and of all files stored thereon; Hernandez concludes that that gives them the right to audit even electronic mail messages [Hernandez, 1988, pp. 39–41]. Indeed, he quotes a participant in the legislative drafting process as saying that that was the intent. Again, state law or non-U.S. law may differ. California state law bars employers from monitoring employees' telephone calls, though in one case (the Epson electronic mail case) a judge held that only voice conversations were protected, not computer messages [Rose, 1991].

To be extremely picky about the law, it is not even clear if logging the source of network connections is legal in all states.[28] Is such a log equivalent to a prohibited trap and trace device? The law defines such a device as follows:[29]

[20] 18 U.S.C. § 2511.

[21] 18 U.S.C. § 2702.

[22] 18 U.S.C. § 2702(b)(5).

[23] 18 U.S.C. §§ 2511(2)(a)(i) , 2702(b)(5).

[24] 18 U.S.C. § 2511(2)(a)(i).

[25] 18 U.S.C. § 2511(1)(c).

[26] 18 U.S.C. § 2511(1)(d).

[27] 18 U.S.C. § 2511(2)(a)(i).

[28] U.S. federal law permits providers of electronic communications services to record service initiation or completion to protect themselves from fraud or abusive use of their services (18 U.S.C. § 2511(2)(h)(ii)).

[29] 18 U.S.C. § 3127(4).

> [T]he term *trap and trace device* means a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted.

That would certainly seem to describe a source address logger.

To be sure, the underlying data network—TCP/IP—will not work without knowing the source of the call. Indeed, certain applications, such as FTP, will not work without knowing it. But there is no requirement in the protocol that that information be logged. Consider the following excerpts from a Pennsylvania Supreme Court ruling barring *Caller*ID*:[30]

> Even if the Caller*ID service were solely a function of the telephone company—which it almost certainly is not—we agree with the Commonwealth Court that the service still violates the wiretap law, because it is being used for unlimited purposes without the "consent" of *each* of the users of the telephone service. . . . "Even though the language of the federal law and 1988 amendments to the Wiretap Act are nearly the same, by not changing the 'all party consent rule,' it is clear that the General Assembly meant that any part of the communication, including phone number identification, should have the consent of all parties prior to it being trapped and traced." 576 A.2d at 93.
>
> We agree. None of the parties relying upon the exception in Section 5771(b) provides a satisfactory explanation of why the "user" as it appears in Section 5771(b)(2) must refer only to the Caller*ID customer, rather than the calling party, or both the called and calling parties. No one disputes that the definition of "user" in the Wiretap Act includes "any person or entity" who uses the telephone network. 18 P.C.S. § 5702. It is also obvious that when a Caller*ID device is employed, two "users" of the telephone network are involved—the called party *and* the calling party. It is the caller whose number is being trapped and traced and whose privacy is being jeopardized, and whose "consent" would therefore be particularly relevant. . . . The two-party consent rule has long been established in Pennsylvania as a means of protecting privacy rights. . . .

That decision could easily be read as barring network caller logging as well, at least in Pennsylvania or other states with similar laws.

12.4 Tort Liability Considerations

42 Several aspects of computer security work carry liability implications. Having too little security can be a negligent act, under long-standing doctrine. Conversely, knowingly permitting a hacker to use your system, even for the purpose of monitoring his or her activities, may expose you to lawsuits from any other parties attacked via your machine.

It helps to understand what liability is, legally speaking. In most cases, tort liability arises if someone has some duty to be careful, but engages in some insufficiently careful behavior that results in harm to others. Keeton *et al*. put it this way [Keeton *et al.*, 1984, § 31]:

[30] *Barasch et al. v. Bell Telephone of Pennsylvania et al.*, 529 Pa. 523, 605 A.2d 1198 (1992).

> The standard of conduct imposed by the law is an external one, based upon what society demands generally of its members, rather than upon the actor's personal morality or individual sense of right and wrong. A failure to conform to the standard is negligence, therefore, even if it is due to clumsiness, stupidity, forgetfulness, an excitable temperament, or even sheer ignorance. An honest blunder, or a mistaken belief that no damage will result, may absolve the actor from moral blame, but the harm to others is still as great, and the actor's individual standards must give way in this area of the law to those of the public. In other words, society may require of a person not to be awkward or a fool.

It could be argued that a site on a network is not obliged to meet some standard of behavior towards other such sites. That may be so; as far as we know, there is no case law on that subject. But the analogies are sufficiently strong to other areas where negligence has been found that prudence seems indicated.

The next point turns on what constitutes a "reasonable" level of care. The courts have held that even if certain precautions are not customary in the industry, they may nevertheless be found necessary to shield other parties from harm. Indeed, even if no one in an industry takes certain precautions, a court might still find fault with someone who omits them. Nycum [1983] notes that the ruling in the *T.J. Hooper* case[31] may be relevant to computer security issues. In that case, a barge loaded with coal sank in a storm. As was common custom then, the tugboat was not equipped with a radio receiver that would have let its crew receive a storm warning. The tugboat line was held to be responsible:

> Indeed in most cases reasonable prudence is in face common prudence; but strictly it is never its measure; a whole calling may have unduly lagged in the adoption of new and available devices. It may never set its own tests, however persuasive be its usages. Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission. . . . But here there was no custom at all as to receiving sets; some had them, some did not; the most that can be urged is that they had not yet become general. Certainly in such a case we need not pause; when some have thought a device necessary, at least we may say that they were right, and the others too slack. . . . We hold [against] the tugs therefore because [if] they had been properly equipped, they would have got the Arlington [weather] reports. The injury was a direct consequence of this unseaworthiness.

This ruling is extremely important in the field of liability law; it is quite likely that a court would hold that applied to computer-related losses, too.

The types of risks being run go beyond the obvious. A university, for example, is obligated to keep student information confidential, up to and including (under certain circumstances) phone numbers and the height and weight of athletic team members.[32] While private suits for damages are not permitted under this statute, the school's negligence could certainly be used as evidence in other proceedings arising under this law.

[31] *T.J. Hooper*, 60 F.2d 737 (2d Cir. 1932).

[32] Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g(b).

In a similar vein, assorted statutes require various government agencies to keep certain information confidential. One[33] requires that the U.S. government

> establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. . . .

Injured parties may seek relief under 5 U.S.C. § 552a(g)(4), though monetary damages may be sought only if the failure was intentional.

In the private sector, the *Foreign Corrupt Practices Act*[34] contains a provision requiring a good system of internal accounting controls in many companies. If a company's computer systems are sufficiently insecure that unauthorized individuals could dispose of assets, or erase audit trails of questionable transactions, both the company and the individuals responsible for those computer systems could face prosecution [Gemignani, 1989]. Similarly, a disgruntled shareholder would have grounds for filing a suit against the management team that permitted this.

Credit bureaus are required to "follow reasonable procedures to assure maximum possible accuracy of the information" they distribute.[35] If they are negligent in their security measures and someone introduces false information, they could be sued for damages.[36] If they are aware of the security problems but decide not to correct them, a court could interpret that as "willful noncompliance" with the act, and impose punitive damages as well.[37]

There is even the risk of being sued for libel, if an intruder masquerades as a legitimate user and defames someone via mail or netnews. Kahn [1989, note 110] notes that the system operator's degree of liability rests in part on the security measures taken to prevent such abuses. If a court held, following the *T.J. Hooper* case, that strong security measures should have been taken, the outcome could be painful.

If you are attempting to monitor an ongoing intrusion, à la *The Cuckoo's Egg* [Stoll, 1989, 1988] or the Berferd incident, the liability considerations are somewhat different. In this case, you are not merely negligent, you are knowingly harboring a wild and dangerous beast.[38] If that beast should decide to use your system as a lair when attacking other systems, you stand a considerable risk. Again quoting Keeton *et al*. [Keeton *et al.*, 1984, § 34]:

> The amount of care demanded by the standard of reasonable conduct must be in proportion to the apparent risk. As the danger becomes greater, the actor is required to exercise caution commensurate with it. Those who deal with instrumentalities that are known to be dangerous, such as high tension electricity, gas, explosives,

[33] 5 U.S.C. § 552a(e)(10).

[34] Foreign Corrupt Practices Act, 15 U.S.C. § 78m.

[35] Credit Card Fraud Act, 15 U.S.C. § 1681e(b).

[36] 15 U.S.C. § 1681o.

[37] 15 U.S.C. § 1681n.

[38] In *Cowden v. Bear Country, Inc.*, 382 F. Supp. 1321 (D.S.D.1974), the court ruled that the operator of a drive-through animal park is required to exercise a high degree of care against injury to visitors.

> elevators, or wild animals, must exercise a great amount of care because the risk is great. They may be required to take every reasonable precaution suggested by experience or prudence. [footnotes omitted]

There was a stronger ruling in an English case that has influenced American common law.[39] The owner of a reservoir that flooded a working mine via abandoned mine tunnels was held liable, even though he was unaware of the existence of the tunnels. Nevertheless, he harbored something dangerous, so he had to bear the associated risks. The analogy between interconnected mine tunnels and a computer network is eerily suggestive.

To be sure, a lawsuit filed against you would be quite unfair. Without exception, *every* system administrator we have spoken with would prefer that you left your door open, so that the intruders' activities with respect to other machines can be monitored. It is, after all, much easier to clean up a system when you know what has been changed. Without such knowledge, you really need to reload your system from the distribution media.

It is also worth noting that if you close your doors, the attackers will not suddenly return to the primordial ooze. As we noted earlier, Berferd did not vanish; he simply switched to a Swedish site. For that matter, he first started using our bait machine when he learned that Stanford had been monitoring him. A plausible defense would be that you are not in any way sheltering the hackers; rather, you *are* taking affirmative action to minimize any danger to your neighbors, precisely by leaving your machine open *and* monitoring their activities. But we do not know if a jury would believe you.

Speaking personally, we have no doubts that such surveillance is helpful to the network community at large. But check with your lawyers first.

[39] *Rylands v. Fletcher*, [1865] 3 H.&C. 774, 159 Eng. Rep. 737.