legally speaking

Can Hackers Be Sued for Damages Caused by Computer Viruses?

The law can be a rather blunt instrument with which to attack a hacker whose virus has caused damage in a computer system. Among the kinds of damage that can be caused by computer viruses are the following: destroyed programs or data, lost computing time, the cost of system cleanup, and the cost of installing new security measures to guard against a recurrence of the virus, just to name a few. The more extensive and expensive the damage is, the more appealing (at least initially) will be the prospect of a lawsuit to seek compensation for the losses incurred. But even when the damage done is considerable, sometimes it may not be worthwhile to bring a lawsuit against the hacker whose virus has damaged the system. Careful thought should be given to making a realistic appraisal of the chances for a meaningful, beneficial outcome to the case before a lawsuit is filed.

This appraisal must take into account the significant legal-theory and practical difficulties with bringing a lawsuit as a way of dealing with the harm caused by a hacker's virus. This column will discuss both kinds of difficulties. A brief synopsis of each type of problem may be helpful before going into detail about each. The legal theory problem is essentially this: There may not yet be a law on the books or clearly applicable legal precedents that can readily be used to establish a right to legal relief in computer virus situations. The law has lots of experience with lawsuits claiming a right to compensation for damage to persons or to tangible property. But questions may arise if someone seeks to adapt or extend legal rules to the more intangible nature of electronically stored information. The practical difficulties with using the law to get some remedy for harm caused by a hacker's virus can be even more daunting than the legal theory problems. Chief among the practical difficulties is the fact that the lawsuit alone can cost more than can ever be recovered from the hacker-defendant.

To understand the nature of the legal theory problems with suing a hacker for damage caused by his or her virus, it may help to understand a few basic things about how the law works. One is that the law has often evolved to deal with new situations, and evolution of this sort is more likely when fairness seems to require it. Another is that the law generally recognizes only already established categories of legal claims, and each of the categories of legal claims has its own particular pattern to it, which must be matched in order to win a lawsuit based on it. While judges are sometimes willing to stretch the legal category a little to reach a fair result, they are rarely willing to create entirely new categories of law or stretch an existing category to the breaking point. Because of this, much of what lawyers do is pattern-matching and arguing by analogy: taking a given set of facts relevant to a client's circumstances, sorting through various possible categories of legal claims to determine which of them might apply to the facts at hand, and then developing arguments to show that this case matches the pattern of this legal category or is analogous to it.

Whenever there is no specific law passed by the legislature to deal with a specific issue, such as damages caused by computer viruses, lawyers look to more general categories of legal claims to try to find one that matches a particular client's situation. "Tort" is the name used by lawyers to refer to a category of lawsuits that aim to get money damages to compensate an injured party for harm caused by another person's wrongful conduct. Some torts are intentional (libel, for example, or fraud). Some are unintentional. (Negligence is a good example of this type of lawsuit.) The harm caused by the wrongful conduct may be to the victim's person (as where someone's negligence causes the victim to break a leg) or property (as where a negligent driver smashes into another car, causing it to be "totaled"), or may be more purely economic losses (as where the victim has to incur the expense of renting another car after his or her car has been destroyed by a negligent driver). In general, tort law permits a victim to recover money damages for all three types of injuries so long as they are reasonably foreseeable by the person who causes them. (Some economic losses, however, are too remote to be recoverable.)

Among the categories of traditional torts that might be worth considering as the basis of a lawsuit seeking compensation for losses

caused by a computer virus is the law of trespass. Though we ordinarily think of trespass in connection with unlawful entry onto another's land, the tort of trespass applies to more situations than this. Intentional interference with someone's use of his or her property can be a trespass as well. A potential problem with the use of trespass for computer virus situations, however, might be in persuading a judge to conceive of a virus as a physical invasion of a computer system. A defendant might argue that he or she was in another state and never came anywhere near the plaintiff's computer system to show that the trespass pattern had not been established. The plaintiff would have to counter by arguing that the virus physically invaded the system, and was an extension of the defendant who was responsible for planting it.

Another tort to consider would be the law of conversion. Someone who unlawfully "converts" someone else's property to his or her own use in a manner that interferes with the ability of the rightful owner to make use of it can be sued for damages by the rightful owner. (Conversion is the tort pattern that can be used to recover damages for theft; *theft* itself is more of a criminal law term.) As with trespass, the law of conversion is more used to dealing with interferences with use of tangible items of property, such as a car. But there would seem to be a good argument that when a virus ties up the computing resources of a firm or university, it is even more a conversion of the computing facility than if some component of the system (such as a terminal) was physically removed from the premises.

Even if a claim, such as conversion, could be established to get damages for lost computer time, that wouldn't necessarily cover all of the kinds of losses that might have been caused by the virus. Suppose, for example, that a virus invaded individual accounts in a computer system and sent out libelous messages masquerading as messages from the account's owner or exposed on a computer bulletin board all of the account owner's computer mail messages. Libel would be a separate tort for a separate kind of injury. Similarly, a claim might be made for invasion of privacy and intentional misrepresentation to get damages for injuries resulting from these aspects of the virus as well.

So far we have been talking mostly about intentional torts. A hacker might think that he or she could not be found liable for an intentional tort because he or she did not intend to cause the specific harm that resulted from the virus, but that is not how tort law works. All that is generally necessary to establish an intentional tort is that the person intended to do the conduct that caused the harm, and that the harm was of a sort that the person knew or should have known would be reasonably certain to happen as a consequence of his or her actions. Still, some hackers might think that if the harm from their viruses was accidental, as when an "experiment" goes awry, they might not be legally responsible for the harm. That is not so. The law of negligence allows victims of accidental injury to sue to obtain compensation for losses caused by another's negligence.

The law of negligence allows victims of accidental injury to sue to obtain compensation for losses caused by another's negligence.

Negligence might be a more difficult legal claim to win in a computer virus case because it may be unclear exactly who had what responsibilities toward whom under the circumstances. In general, someone can be sued for damages resulting from negligence when he or she has a duty to act in accordance with a standard of care appropriate to the circumstances, and fails to act in accordance with that standard of care in a particular situation. Standards of care are often not codified anywhere, but depend on an assessment of what a reasonable person would do in the same set of circumstances. A programmer, for example, would seem to have a duty to act with reasonable care in writing programs to run on a computing system and a duty not to impose unreasonable risks of harm on others by his or her programming. But the owner of the computing system would also have a duty of care to create reasonable safeguards against unauthorized access to the computing system or to some parts of the computer system because the penchant of hackers to seek unauthorized entry is well-known in the computing community. The focus in a negligence lawsuit, then, might not be just on what the hacker did, but on what the injured party did to guard against injury of this sort.

Sometimes legislatures pass special laws to deal with new situations such as computer viruses. If a legislature was to consider passing a law to provide remedies for damages caused by computer viruses, there would be a number of different kinds of approaches it could take to formulate such a law. It is a tricker task than one might initially suppose to draft a law with a fine enough mesh to catch the fish one is seeking to catch without creating a mesh so fine that one catches too many other fish, including many that one doesn't want to catch.

Different legislative approaches have different pros and cons. Probably the best of these approaches, from a plaintiff's standpoint, would be that which focuses on unauthorized entry or abuse of access privileges because it limits the issue of wrongful conduct by the defendant to access privileges, something that may be relatively easy to prove. Intentional disruption of normal functioning would be a somewhat more demanding standard, but would still reach a wide array of virus-related conduct. A law requiring proof of

damage to data or programs would, again from a plaintiff's standpoint, be less desirable because it would have stiffer proof requirements and would not reach viruses that merely disrupted functioning without destroying data or programs. The problem of crafting the right law to cover the right problem (and only the right problem) is yet another aspect of the legal theory problems posed by computer viruses.

Apart from the difficulties with fitting computer virus situations in existing legal categories or devising new legal categories to reach computer viruses, there are a set of practical difficulties that should be considered before undertaking legal pursuit of hackers whose viruses cause damage to computer systems.

Perhaps the most important set of practical difficulties with suing a hacker for virus damages is that which concerns the legal remedy one can realistically get if one wins. That is, even if a lawyer is able to identify an appropriate legal claim that can be effectively maintained against a hacker, and even assuming the lawyer can surmount the considerable evidentiary problems that might be associated with winning such a lawsuit, the critically important question which must be answered before any lawsuit is begun is what will one realistically be able to recover if one wins.

There are three sets of issues of concern here. One set relates to the costs of bringing and prosecuting the lawsuit. Lawsuits don't come cheap (and not all of the expenses are due to high attorney fees). Another relates to the amount of damages or other cost recoveries that can be obtained if one wins the lawsuit. It's fairly rare to be able to get an award of attorney's fees or punitive damages, for example, but a lawsuit becomes more attractive as an option if these remedies are available. Also, where the virus has spread to a number of different computer systems on a network, for example, the collective damage done by the hacker may be substantial, but the damage to any one entity within the network system may be sufficiently small that, again, it may not be economically feasible to maintain individual lawsuits and the collectivity may not have sufficiently uniform interests to support a single lawsuit on behalf of all network members.

But the third and most significant concern will most often be the ability of the defendant to write a good check to pay the damages that might be awarded in a judgment. Having a judgment for one million dollars won't do you any good if it cost you $10,000 to get it and the defendant's only asset is a used computer with a market value of $500. In such an instance, you might as well have cut your losses and not brought the lawsuit in the first place. Lawyers refer to defendants of this sort as "judgment-proof."

While these comments might suggest that no lawsuit should ever be brought against a young hacker unless he or she has recently come into a major inheritance, it is worth pointing out the law does allow someone who has obtained a judgment against another person to renew the judgment periodically to await "executing" on it until the hacker has gotten a well-paying job or some other major asset which can be seized to satisfy the judgment. If one has enough patience and enough confidence in the hacker's future (or a strong enough desire for revenge against the hacker), there may be a way to get some compensation eventually from the defendant.

Proof problems may also plague any effort to bring a successful lawsuit for damages against a computer hacker. Few lawsuits are easy to prove, but those that involve live witnesses and paper records are likely to be easier than those involving a shadowy trail of electronic signals through a computer system, especially when an effort is made to disguise the identity of the person responsible for the virus and the guilty person has not confessed his or her responsibility. Log files, for example, are constantly truncated or overwritten, so that whatever evidence might once have existed with which to track down who was logged onto a system when the virus was planted may have ceased to exist.

Causation issues too can become very murky when part of the damage is due to an unexpected way in which the virus program interacted with some other parts of the system. And even proving the extent of damages can be difficult. If the system crashes as a result of the virus, it may be possible to estimate the value of the lost computing time. If specific programs with an established market value are destroyed, the value of the program may be easy to prove. But much of the damage caused by a virus may be more elusive to establish. Can one, for example, recover damages for economic losses attributable to delayed processing, for lost accounts receivable when computerized data files are erased and no backup paper record was kept of the transactions? Or can one recover for the cost of designing new security procedures so that the system is better protected against viruses of this sort? All in all, proof issues can be especially vexing in a computer virus case.

In thinking about the role of the law in dealing with computer virus situations, it is worth considering whether hackers are the sorts of people likely to be deterred from computer virus activities by fear of lawsuits for money damages. Criminal prosecution is likely to be a more powerful legal deterrent to a hacker than a civil suit is. But even criminal liability may be sufficiently remote a prospect that a hacker would be unlikely to forego an experiment involving a virus because of it. In some cases, the prospect of criminal liability may even add zest to the risk-taking that is involved in putting a virus in a system.

Probably more important than new laws or criminal prosecutions in deterring hackers from virus-related conduct would be a stronger and more effective ethical code among computer professional and better internal policies at private firms, universities, and governmental institutions to regulate usage of computing resources. If hackers cannot win the admiration of their colleagues when they succeed at their clever stunts, they may be less likely to do them in the first place.

And if owners of computer facilities make clear (and vigorously enforce) rules about what is acceptable and unacceptable conduct when using the system, this too may cut down on the incidence of virus experiments.

Still, if these measures do not succeed in stopping all computer viruses, there is probably a way to use the law to seek some remedy for damages caused by a hacker's virus. The law may not be the most precisely sharpened instrument with which to strike back at a hacker for damages caused by computer viruses, but sometimes blunt instruments do an adequate job, and sometimes lawsuits for damages from viruses will be worth the effort of bringing them.

Pamela Samuelson
Visiting Professor
Emory Law School
Atlanta, Ga.

Viruses and Criminal Law

Harry the Hacker broke into the telephone company computer and planted a virus that he expected would paralyze all telephone communications in the United States. Harry's efforts, however, came to naught. Not only did he make a programming error that made the virus dormant until 2089 instead of 1989, but he was also unaware that the telephone company's computer was driven by a set of preprogrammed instructions that were isolated from the effects of the virus. An alert computer security officer, aided by automated audits and alarm systems, detected and defused Harry's logic bomb.

A hypothetical situation, yes, but not one outside the realm of possibility. Let us suppose that Harry bragged about his feat to some friends in a bar, and a phone company employee who overheard the conversation reported the incident to the police and gave them Harry's name and address. Would Harry be guilty of a crime? Even if Harry had committed a crime, what is the likelihood that he could be convicted.

Before attempting to answer these questions, we must first know what a crime is. A crime is an act that society, through its laws, has declared to be so serious a threat to the public order and welfare that it will punish anyone who commits the act. An act is made criminal by being declared to be a crime in a duly enacted statute. The statute must be clear enough to give reasonable notice as to what is prohibited and must also prescribe a punishment for taking the action.

The elements of the crime must be spelled out in the statute. In successful prosecution, the accused must have performed acts that demonstrate the simultaneous presence of all of the elements of the crime. Thus, if the statute specifies that one must destroy data to have committed an alleged crime, but the act destroyed no data, then one cannot be convicted of that crime. If the act destroyed only student records of a university, but the statute defines the crime only for a financial institution, then one cannot be convicted under the statute.

All states now have criminal statutes that specifically address certain forms of computer abuse. Many misdeeds in which the computer is either the instrument or object of the illicit act can be prosecuted as more traditional forms of crime, such as stealing or malicious mischief. Because we cannot consider all possible state and federal statutes under which Harry might be prosecuted, we will examine Harry's action only in terms of the federal computer crime statute.

The United States Criminal Code, title 18, section 1030(a)(3), defines as criminal the intentional, unauthorized access to a computer used exclusively by the federal government, or any other computer used by the government when such conduct affects the government's use. The same statute, in section 1030(a)(5)(A), also defines as criminal the intentional and unauthorized access to two or more computers in different states, and conduct that alters or destroys information and causes loss to one or more parties of a value of at least $1000.

If the phone company computer that Harry illicitly entered was not used by the federal government, Harry cannot be charged with a criminal act under section 1030(a)(3). If Harry accesses two computers in different states, and his action alters information, and it causes loss to someone of a value of at least $1000, then he can be charged under section 1030(a)(5)(A). However, whether these conditions have been satisfied may be open to question.

Suppose, for example, that Harry plants his logic bomb on a single machine, and that after Harry has disconnected, the program that he loaded transfers a virus to other computers in other states. Has Harry accessed those computers? The law is not clear. Suppose Harry's act does not directly alter information, but merely replicates itself to other computers on the network, eventually overwhelming their processing capabilities as in the case of the Internet virus on November 2, 1988. Information may be lost, but can that loss be directly attributed to Harry's action in a way that satisfies the statute? Once again, the answer is not clear-cut.

And what of the $1000 required by the statute as an element of the crime? How is the loss measured? Is it the cost of reconstructing any files that were destroyed? Is it the market value of files that were destroyed? How do we determine these values, and what if there were adequate backups so that the files

could be restored at minimal expense and with no loss of data? Should the criminal benefit from good operating procedures on an attacked computer? Should the salaries of computer personnel, who would have been paid anyway, be included for the time they spend to bring the system up again? If one thousand users each suffer a loss of one dollar, can one aggregate these small losses to a loss sufficiently large to be able to invoke the statute? The statute itself gives us noguidance so the courts will have to decide these questions.

No doubt many readers consider questions such as these to be nitpicky. Many citizens already are certain that guilty parties often use subtle legal distinctions and deft procedural maneuvers to avoid the penalities for their offenses. "If someone does something wrong, he or she should be punished and not be permitted to hide behind legal technicalities," so say many. But the law must be the shield of the innocent as well as a weapon against the malefactor. If police were free to invent crimes at will, or a judge could interpret the criminal statutes to punish anyone who displeased him or her, then we would face a greater danger to our rights and freedoms than computer viruses. We cannot defend our social order by undermining the very foundations on which it is built.

The difficulties in convicting Harry of a crime, however, go beyond the questions of whether he has simultaneously satisfied each condition of some crime with which he can be charged. There remain the issues of prosecutorial discretion and the rules of evidence.

Prosecutors have almost absolute discretion concerning what criminal actions they will prosecute. That a prosecutor can refuse to charge someone with a crime, even someone against whom an airtight case exists, comes as a shock to many citizens who assume that once the evidence exists that someone has committed a crime, that person will be arrested and tried.

There are many reasons why a prosecutor may pass up the chance to nail a felon. One is that the caseload of the prosecutor's office is tremendous, and the prosecutor must choose the criminals who pose the greatest danger to society. Because computer crimes are often directed against businesses rather than persons and usually carry no threat of bodily injury, they are often seen as low priority cases by prosecutors. Even computer professionals themselves do not seem to think that computer crime is very serious. In a 1984 survey by the American Bar Association, respondents rated computer crime as the third least significant category of illicit activity, with only shoplifting and illegal immigration being lower. With such attitudes among those responsible for computer security, who can blame prosecutors for turning their attention to crimes the public considers to be more worthy of law enforcement's limited resources?

Underlying the assessment of priority is a general lack of understanding about computers among prosecutors. Thus, a prosecutor would have to spend an unusual amount of time to prepare a computer crime case as opposed to a case that dealt with a more traditional, and hence better understood, mode of crime. Moreover, even if the prosecutor is quite knowledgeable about computers, few judges and even fewer jurors are. The presentation of the case, therefore, will be more difficult and time consuming, and the outcome less predictable. I am familiar with a case that took hundreds of hours to prepare and resulted in a conviction, but the judge sentenced the convicted criminal to pay only a small fine and serve two years probation. With such a result, one cannot be surprised that prosecutors ignore computer criminals when there are so many felons that courts obviously consider more worthwhile.

Suppose, for the sake of argument, that we have a prosecutor who is willing to seek an indictment against Harry and bring him to trial. Even then, computer-related crimes can pose special evidentiary problems. Remember that to convict Harry, the prosecutor must convince a jury beyond a reasonable doubt that Harry committed an act in which all of the elements of the crime were found simultaneously. The elements of the crime cannot be found to exist in the abstract; they must be found to apply specifically to Harry.

Apart from having to prove that the act caused the requisite amount of damage and that the computers used were those specified by the statute, the prosecutor would have to show that Harry committed the act and that he did so intentionally and without authorization. Because Harry was using someone else's account number and password, tying Harry to the crime might be difficult unless unusual surveillance was in place. A gunman and his weapon must be physically present at the teller's window to rob the bank, but a computer criminal may be thousands of miles away from the computer that is attacked. A burglar must physically enter a house to carry off the loot and may, therefore, be observed by a witness; moreover, it is generally assumed that someone carrying a television set out of a darkened house in the middle of the night is up to no good. By contrast, a computer criminal can work in isolation and secrecy, and few, if any, of those who happen to observe are likely to know what he is doing.

The evidence that ties the computer criminal to the crime, therefore, is often largely circumstantial; what is placed before the jury is not eyewitness testimony, but evidence

Even if the prosecutor is quite knowledgeable about computers, few judges and even fewer jurors are. The presentation of the case, therefore, will be more difficult and time consuming, and the outcome less predictable.

from which the facts can only be reasonably inferred. Although convictions on the basis of circumstantial evidence alone are possible, they are often harder to obtain.

Adding to the prosecutor's difficulties in getting convincing evidence about Harry's acts are the unsettled constitutional issues associated with gathering that evidence. Does Harry have a reasonable expectation that his computer files are private? If so, then a search warrant must be obtained before they can be searched and seized. If Harry's files are enciphered, then must Harry furnish the key to decryption, or would he be protected from having to do so by his Fifth Amendment right against self-incrimination? The evidence that would convict Harry won't do the prosecutor much good if it is thrown out as having been obtained by impermissible means.

In the face of these difficulties, some have introduced bills into Congress and into some state legislatures that prohibit planting a virus in a computer system. But drafting a responsible computer crime bill is no easy task for legislators. The first effort at federal computer crime has proscribed, and even imposed heavy penalties for, standard computing practices. It did not clearly define what acts were forbidden. It was so broad that one could have been convicted of a computer crime for stealing a digital watch, and it did not cover nonelectronic computers. The bill was never enacted.

If we want a statute that targets persons who disrupt computer systems by planting viruses, then what do we look for in judging the value of proposed legislation?

Is the proposed statute broad enough to cover activity that should be prohibited but narrow enough not to unduly interfere with legitimate computer activity? Would an expert be able to circumvent the statute by designing a harmful program that would not be covered by the statute? Does the proposed statute clearly define the act that will be punished so as to give clear notice to a reasonable person? Does the act distinguish between intentional acts and innocent programming errors? Does the statute unreasonably interfere with the free flow of information? Does it raise a First Amendment free speech problem? These and other questions must be considered in developing any new computer crime legislation.

Where do I personally stand with regard to legislation against viruses, logic bombs, and other forms of computer abuse? It is not enough to say I am against conduct that destroys valuable property and interferes with the legitimate flow of information. The resolution of legal issues invariably involves the weighing of competing interests, e.g., permitting the free flow of information v. safe-guarding a system against attack. Even now, existing criminal statues and civil remedies are powerful weapons to deter and punish persons who tamper with computer systems. I believe that new legislation should be drawn with great care and adopted only after an open discussion of its merits by informed computer professionals and users.

The odds are that Harry the Hacker will never be charged with a crime, or, if charged, will get off with a light sentence. And that is the way it will remain unless and until society judges computer crimes, be they planting viruses or stealing money, to be a sufficiently serious threat to the public welfare to warrant more stringent and careful treatment. If such a time comes, one can only hope that computing professionals and societies such as the ACM will actively assist legislatures and law enforcement officials in dealing with the problem in an intelligent and technologically competent manner.

Michael Gemignani
Senior Vice President and Provost
University of Houston at Clear Lake
Houston, TX 77059