Possible Vicarious Liability for Computer Users in the USA?

Table of Contents

Disclaimer

This essay is a suggestion for new law in the USA. This essay does *not* describe the current law of liability for users of computers in the USA.

This essay is intended only to present general information about an interesting topic in law and is *not* legal advice for your specific problem. See my disclaimer at http://www.rbs2.com/disclaim.htm .

1. The Problems

This essay discusses the potential liability of an owner of a computer for harm caused to someone, as a result of propagation of malicious computer programs, denial-of-service attacks on websites, or spam e-mail from the owner's computer, without the knowledge of the owner.

malicious computer programs

Anyone who uses e-mail is well aware of the recurring epidemics of so-called "computer viruses"[1] that are commonly spread by e-mail. Users who click on an attachment in e-mail are at risk for being infected with a virus.

The fact that some malicious programs continue to propagate for months, even years, after anti-virus programs have been updated to detect a specific malicious program shows that some users of computers are either (1) not running anti-virus software, (2) not updating the virus definitions in their anti-virus software, or (3) continuing to use a machine that is infected by a virus.

My essay, *Examples of Malicious Computer Programs,* posted on the Internet at http://www.rbs2.com/cvirus.htm , reviews the history of some early computer viruses, the immense harm caused by viruses, and makes the point that, in May 2002, despite the existence of more than 60,000 known computer viruses, the authors of *only five* viruses had been arrested, prosecuted, and sentenced for their crime.

denial of service attacks

Computer criminals can install malicious software on computers, which makes those computers function as "zombies" in a denial-of-service attack on a website.[2] The zombie computers send out a series of pings to the website, thus overloading the website and making the website unavailable to legitimate users. The resulting unavailability of the website is certainly harmful to the owner of the website and may also be harmful to people who need access to that website. The denial-of-service attacks are unknown to the owners of the zombie computers. The owner of a zombie computer typically never gave permission for the computer criminal to

[1] For simplicity, I use the word "virus" in this essay to refer to any malicious computer program, including computer worms, Trojan horse programs, and true computer viruses. For the purposes of this essay it is not necessary to distinguish a worm from a virus.

[2] David Dittrich, *Distributed Denial of Service Attacks/Tools,* http://staff.washington.edu/dittrich/misc/ddos/ (large collection of relevant links); anonymous, *Denial of Service Attack,* http://securityresponse.symantec.com/avcenter/venc/data/dos.attack.html ; Ronald B. Standler, *Computer Crime,* (2002) http://www.rbs2.com/ccrime.htm#anchor111666 .

access that zombie computer.

spam e-mail

In mid-2003, it was realized that some unsolicited commercial e-mail (commonly called "spam") was coming, not from computers operated by spammers, but from innocent computers that had been hijacked by means of a backdoor installed by a computer worm. The use of worms to install backdoors for spammers apparently began on 9 January 2003 with the Sobig.A worm, which could install the Trojan horse program Backdoor.Lala.[3] The MyDoom[4] worm that was discovered on 26 Jan 2004 and the Bagle[5] worms that was discovered between 27 February 2004 and 29 March 2004 were other epidemics of malicious programs that installed backdoors for spammers. By mid-2004, the majority of spam e-mail was coming from such innocent computers. For example, one newspaper reported:

> Spammers are notoriously tough to track, since they use a wide- and ever-expanding range of tricks and tactics to disguise their identities, including open proxies, third-party computers through which spammers route their mass mailings.
>
> Many of the open proxies are, in fact, spawning spam without their users' knowledge, since they've been previously compromised by worm and virus writers to create a backdoor, by which the hackers can operate the system. Last week's wave of Bagle worms, for instance, all had a backdoor component that installed on infected computers.
>
> The prime use for such proxies is to send spam, according to Mark Sunner, the chief technology officer of U.K.-based MessageLabs, which specializes in filtering enterprise messaging for spam and viruses.
>
> "Sixty to seventy percent of the spam we're trapping is coming from open proxies," Sunner said. "And there's doubt in my mind that spammers are bankrolling people who can write viruses, people who may have not been writing them before, to create a vast array of proxies."

Gregg Keizer, "CAN-SPAM Violators Are Tough To Track," *Information Week,* 10 Mar 2004.

[3] For information on Backdoor.Lala, see http://securityresponse.symantec.com/avcenter/venc/data/backdoor.lala.html .

[4] See http://www.symantec.com/avcenter/venc/data/w32.mydoom.a@mm.html , which reports that the MyDoom worm "sets up a backdoor into the system by opening TCP ports 3127 through 3198, which can potentially allow an attacker to connect to the computer and use it as a proxy to gain access to its network resources."

[5] See http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.c@mm.html for the C variant of the Bagle worm, which is called Beagle by Symantec. The C variant creates a backdoor on an infected computer by opening port 2745. The E, F, G, H, I, J and K variants of Bagle also create a backdoor on port 2745. Other variants of the Bagle worm use a different port.

A good overview of the early history and terse technical details of this problem is given in an article at a computer security company's website:

> In January 2003, the Win32 virus "Sobig.a" appeared on the scene. It was a virus that would download a specially modified proxy server and run it on infected machines. The proxy server would run hidden on the infected systems, listening on completely non-standard ports and logging none of the traffic passing through it. This is what the spammers had always needed, and it was handed to them by a virus. We may never know if the author of the Sobig.a is actually one of the spammers or was paid by a spammer to write the virus.
> The best we can do is to analyze the system the virus uses to install the proxy servers and undermine its ability to remain hidden on the Internet by sharing that information.

LURHQ Threat Intelligence Group, "Sobig.a and the Spam You Receive Today – LURHQ," 17 Mar 2003, http://www.lurhq.com/sobig.html .

2. Legal Analogies

In March 2004, when I searched the Westlaw database of reported court opinions in the USA, I found no reported case on the liability of a computer owner for misuse of his computer by a hacker. When attorneys are faced with a new problem, they look for analogies in well-settled areas of law. The following situations are analogous to the computer owner who connects a computer to the Internet without current anti-virus software and without a software firewall.

leaving keys in unlocked, unattended car

In a different area of law, consider the driver of an automobile who parks that automobile and leaves the doors unlocked and leaves the keys in the ignition switch. If the car is stolen and used to commit a crime (e.g., vehicular homicide), the driver who left the keys in the ignition can be liable for damage caused by the thief of the automobile. The following states, among others, permit tort liability against the driver who leaves the key in an *un*attended vehicle, especially if there is a high risk that the vehicle will be stolen:

- *Vadala v. Henkels & McCoy, Inc.,* 397 A.2d 1381 (Del.Super. 1979);
- *Ross v. Hartman,* 139 F.2d 14 (App.D.C. 1943), *cert.den.,* 321 U.S. 790 (1944);
  Gaither v. Myers, 404 F.2d 216 , 220-23 (D.C.Cir. 1968);
- *Vining v. Avis Rent-A-Car Systems, Inc.,* 354 So.2d 54 (Fla. 1977);
  Hendeles v. Sanford Auto Auction, Inc., 364 So.2d 467 (Fla. 1978);
- *Davis v. Thornton,* 180 N.W.2d 11 (Mich. 1970);
- *Illinois Farmers Ins. Co. v. Tapemark Co.,* 273 N.W.2d 630, 635-38 (Minn. 1978);
- *Hill v. Yaskin,* 380 A.2d 1107 (N.J. 1977);
- *Herrera v. Quality Pontiac,* 73 P.3d 181, 2003-NMSC-018 (N.M. 2003);
  Richardson v. Carnegie Library Restaurant, Inc., 763 P.2d 1153, 1164-66 (N.M. 1988) (collecting cases, but unable to reach a majority decision);
- *Justus v. Wood,* 348 S.W.2d 332 (Tenn. 1961);
  McClenahan v. Cooley, 806 S.W.2d 767 (Tenn. 1991).

There are several reasons that make this a reasonable rule of law:

1. Leaving the keys in the ignition switch is a negligent act that easily enabled a criminal to steal the automobile — leaving the keys in the ignition switch was the first event in a chain of events that eventually produced an injury.
2. It is foreseeable that car thieves are often either incompetent or reckless drivers.[6] If the driver of a stolen car is chased by police, the probability of an accident is increased.
3. Many states have statutes prohibiting leaving the key in a motor vehicle that is both unlocked *and* unattended. It is a general rule of law that violation of a statute that was intended to protect a class of people constitutes negligence, which can be the proximate cause of injury. Restatement (Second) of Torts § 286 (1965).
4. The owner of a dangerous item, such as an automobile, has a duty to prevent foreseeable harm(s) with that item.[7] See also Restatement (Second) of Torts § 297-98.
5. An additional reason for this rule of law is that can be difficult to prove the identity of hit-and-run drivers of stolen automobiles, so by making the driver who leaves the keys in the ignition switch liable in tort, society provides a way to compensate innocent victims of *un*identified hit-and-run drivers.

Automobile theft is harmful to society in two ways: (1) stolen cars are much more likely to be involved in accidents, which cause injury to people and property, and (2) stolen cars that are either damaged or not recovered must be reimbursed by insurance, which increases the cost of purchasing insurance. Several courts have cited U.S. Department of Justice statistics on stolen automobiles:

> On March 1, 1968, the Attorney General of the United States and nineteen responsible organizations, including national associations of mayors, police chiefs, district attorneys, municipal law officers, launched the National Auto Theft Prevention Campaign in a nationwide effort to reduce automobile theft. ....
>
> The data distributed by the Campaign include the estimate that in 1966 more than a million cars were stolen nationally and that about 24% of the stolen vehicles were involved in accidents. The theft problem is acute in the District of Columbia where, during 1967, there were over 13,000 auto thefts, an increase over 1966 of 30%[,] as opposed to a national rise of 17%. The accident rate for stolen cars is estimated to be approximately 200 times the normal

[6] Many car thieves are young people who are either inexperienced, or even unlicensed, drivers. In the year 1975, stolen cars were 47 times more likely to be involved in an accident. *Hill v. Yaskin,* 380 A.2d 1107, 1110 (N.J. 1977). Also see *Justus v. Wood,* 348 S.W.2d 332, 338 (Tenn. 1961) ("It is common knowledge that a person possessed of the characteristics which would cause him to thus steal an automobile is a person who is irresponsible and totally devoid of regard for the rights and safety of others who might be using the street at the same time....").

[7] *Vining v. Avis Rent-A-Car Systems, Inc.,* 354 So.2d 54, 56 (Fla. 1977)("The owner of a dangerous instrumentality must exercise due care to ensure that such a danger does not occur."). *Prosser and Keeton on Torts,* § 73, at page 524 of the Student Edition, (5th ed. 1984) says this dangerous instrumentality approach is unique to Florida, but also calling it a "simple but sweeping approach".

> accident rate. And in the District of Columbia, 85% of the thieves do not possess operator's permits. A study has disclosed that of the total cars stolen, the key had been left in either the ignition or in the car in 42.3% of the cases.
>
> Moreover, the authorities point out that auto theft is to a large extent a crime of opportunity, unusually inviting to young people, and is often the first major episode in a criminal career. The data reveal that 70% of the District of Columbia auto thefts are by offenders under the age of 21. [eight footnotes omitted]

Gaither v. Myers, 404 F.2d 216, 222-23 (D.C.Cir. 1968).
cited in:

- *Davis v. Thornton,* 180 N.W.2d 11, 14 (Mich. 1970);
- *Zinck v. Whelan,* 294 A.2d 727, 731-32 (N.J.Super.A.D. 1972);
- *Dix v. Motor Market, Inc.,* 540 S.W.2d 927, 935 (Mo.App. 1976)(Stewart, J., dissenting);
- *Herrera v. Quality Pontiac,* 73 P.3d 181, 185 (N.M. 2003)(citing unnamed expert).

It is commonly accepted that removing the key and then locking unattended vehicles is beneficial not only to the driver and owner of the vehicle (e.g., by avoiding the inconvenience of a stolen vehicle), but also is beneficial to society in avoiding injury to innocent victims of recklessly operated stolen vehicles, and also by avoiding crime (i.e., theft of vehicles is "a crime of opportunity").

some states reject this liability

However, this rule of tort liability for drivers who leave the keys in an unlocked vehicle does *not* apply to all states in the USA. The following states do not recognize this rule of liability:

- *Richards v. Stanley,* 271 P.2d 23 (Calif. 1954); but see *Hergenrether v. East,* 393 P.2d 164, (Calif. 1964) and *Palma v. U.S. Industrial Fasteners, Inc.,* 681 P.2d 893, 901-03 (Calif. 1984);
- *Galbraith v. Levin,* 81 N.E.2d 560 (Mass. 1948);
  Poskus v. Lombardo's of Randolph, Inc., 670 N.E.2d 383 (Mass. 1996);
- *Manchenton v. Auto Leasing Corp.,* 605 A.2d 208, 212 (N.H. 1992)(State statute only prohibits leaving key in vehicle parked on "ways", *not* applicable to vehicles parked on private property);
- *Wilson v. Harrington,* 56 N.Y.S.2d 157 (N.Y.A.D. 3 Dept. 1945),
  aff'd without opinion, 65 N.E.2d 101 (N.Y. 1946);
- *Liney v. Chestnut Motors, Inc.,* 218 A.2d 336 (Penn. 1966);
- *Keefe v. McArdle,* 280 A.2d 328 (R.I. 1971).

A common reason for holding that there is *no* liability is that the stealing of a car is an intervening act that breaks the chain of causation.

compulsory immunization

Most states have a statute requiring that children receive certain immunizations (e.g., poliomyelitis, measles, mumps, rubella, diphtheria, pertussis, tetanus, etc.) before they are permitted to attend school. The reason for requiring everyone to be immunized is to protect the health of the pupils,[8] by preventing epidemics of contagious diseases amongst pupils in one classroom, or in one school. Waivers of the required immunization can be obtained if the immunization is medically contraindicated for one patient (e.g., a pupil who is allergic to a component of the vaccine) or sometimes if the parents have a religious objection.[9] If *most* of the pupils are immunized, then there may be so-called "herd immunity" that prevents epidemics, despite the presence of a few *un*immunized individuals. Furthermore, during an epidemic, a school can prohibit unimmunized pupils from attending.[10]

Similarly, a state statute requiring all adults to be vaccinated against smallpox was held to be a valid exercise of the police power, to protect the public health. *Commonwealth of Massachusetts v. Pear,* 66 N.E. 719 (Mass. 1903), *aff'd sub nom. Jacobson v. Commonwealth of Massachusetts,* 197 U.S. 11 (U.S. 1905). There are many other reported cases on this topic, but *Jacobson* is still the controlling law in the USA.

[8] Such a compulsory vaccination statute is a valid exercise of the police power of the state. *Zucht v. King,* 225 S.W. 267 (Tex.Civ.App. 1920), *writ dismissed,* 260 U.S. 174 (U.S. 1922).

[9] See, e.g., *Anderson v. State,* 65 S.E.2d 848 (Ga.App. 1951)(compulsory education); *Davis v. State,* 451 A.2d 107 (Md. 1982)(establishment clause); *Dalli v. Board of Ed.,* 267 N.E.2d 219 (Mass. 1971)(religious exception void); *Commonwealth of Massachusetts. v. Green,* 168 N.E. 101 (Mass. 1929)(no religious exception); *Brown v. Stone,* 378 So.2d 218 (Miss. 1979) (no religious exception), *cert. den.* 449 U.S. 887 (U.S. 1980); *Board of Ed. of Mountain Lakes v. Maas,* 152 A.2d 394 (N.J.Super.A.D. 1959)(no religious exception), *aff'd without opinion,* 158 A.2d 330 (N.J. 1960), *cert. den.,* 363 U.S. 843 (1960); *State of Ohio ex rel. Dunham v. Board of Ed. of City School Dist. of Cincinnati,* 96 N.E.2d 413 (Ohio 1951)(no religious exception), *cert. den.,* 341 U.S. 915 (U.S. 1951); *Itz v. Penick,* 493 S.W.2d 506 (Tex. 1973)(immunization statute is valid); *Jones ex rel. Jones v. State Dept. of Health,* 18 P.3d 1189 (Wyo. 2001)(medical contraindication); *In re LePage,* 18 P.3d 1177 (Wyo. 2001)(religious objection).

[10] *Maack v. School Dist. of Lincoln,* 491 N.W.2d 341 (Neb. 1992).

livestock as chattel

Another analogy that makes some sense to me is the tort liability of an owner for the acts of his/her livestock (e.g., cows, sheep, etc.). It is well-established law that the owner of livestock, which are not dangerous animals and are not wild animals, is liable for foreseeable harms caused by those animals. Restatement (Second) of Torts §§ 504, 515, 518 (1977). Like a cow, the computer is a chattel (i.e., thing) that can not be liable in tort. And, like a cow, a computer has no intelligence and no sense of moral responsibility.

A case in Maine in 1857 held that there were two circumstances in which the owner of livestock was liable for harms caused by those livestock:

1. If domestic animals, such as oxen and horses, injure any one, ... *if they are rightfully in the place where they do the mischief,* the owner of such animals is not liable for such injury, unless he knew that they were accustomed to do mischief....
2. The owner of domestic animals, *if they are wrongfully in the place where* they do any mischief, is liable for it, though he had no notice that they had been accustomed to do so before....

Decker v. Gammon, 44 Me. 322, 327-29 (1857) [emphasis in original],
quoted in *Byram v. Main,* 523 A.2d 1387, 1389 (Me. 1987).

Furthermore, statutes in many states impose strict liability (i.e., liability with neither fault nor negligence) on the owner of livestock or dogs. See, e.g., *Corey v. Smith,* 120 N.E.2d 410, 411-12 (Ind. 1954); *Madrid v. Zenchiku Land and Livestock,* 51 P.3d 1137 (Mont. 2002); *Restatement (Second) of Torts* § 509, comment f (1977).

A few recent cases on the topic of liability for livestock include:

- *Williams v. Goodwin,* 116 Cal.Rptr. 200, 204-08 (Cal.App. 3 Dist. 1974);
- *Thompson v. Lee,* 402 N.E.2d 1309, 1311-13 (Ind.App. 1 Dist. 1980);
- *Sybesma v. Sybesma,* 534 N.W.2d 355 (S.D. 1995).

3. Application to Computers

Applying this automobile analogy to use of computers, I believe that connecting an *un*protected[11] computer to the Internet is a negligent act. It is foreseeable that an unprotected computer that is connected to the Internet will eventually be infected with malicious computer programs, which can then cause harm to others: either by sending copies of malicious programs, by being a zombie computer in a distributed denial-of-service attack, or by being a relay for spam e-mail. In my opinion, the owner or operator of an *un*protected computer should be liable in tort for damage(s) caused by misuse of his/her computer by others.

Unprotected computers that are connected to the Internet with a static IP address (e.g., broadband connection, not a modem on a voice-grade telephone line) are at greater risk for access via a backdoor, since the criminal who accesses this computer has the convenience of a constant IP address.

Like hit-and-run drivers of stolen cars, the identities of writers of computer viruses and anonymous senders of spam are difficult to identify, which means that control of viruses and spam must focus on protecting everyone's computer.

Like stolen automobiles, infection by malicious programs is a crime of opportunity. Just as leaving the keys in an *un*locked, *un*attended vehicle makes the vehicle more likely to be stolen, connecting an *un*protected computer to the Internet makes the computer more likely to be infected by a computer virus, worm, or backdoor access program.

Some people, particularly those who are not knowledgeable about computers, may whine that it is "too difficult" to install and update anti-virus software. However, modern anti-virus software is easy to install and update. Some modern anti-virus programs automatically update themselves when the computer is both on and connected to the Internet.

Another objection is that anti-virus software is too expensive. When I was writing the early drafts of this essay in March 2003, an initial copy of anti-virus software for Windows on CD-ROM cost approximately US$ 50 and provides free online updates for one year. After the first year, a renewal subscription to online updates for this software costs approximately US$ 15/year. Firewall software costs approximately US$50. Such costs are not burdensomely expensive: the annual fee is less than what states charge for licensing automobiles.

[11] ”Protected" means running *both* current anti-virus software *and* current firewall software. On 32-bit Microsoft Windows operating systems, anti-virus software needs to be updated at least weekly, because of the large number of new malicious programs targeted at those operating systems. For computers running a version of either the Apple or Linux operating systems, anti-virus software might be current if updated once every two months.

What happens when a plaintiff sues a defendant for sending a virus to the plaintiff, when neither the plaintiff nor the defendant had anti-virus software on their computers? I suggest that in such a situation the plaintiff and the defendant are equally blameworthy for not having anti-virus software, and equally innocent[12] in being unaware of good computing practices, hence there should be no recovery for the plaintiff. An analogy to law in some states shows that a landowner who erected no fence around his property can not recover from trespass of another's livestock.[13] As a general principle of torts, *both* the plaintiff *and* the defendant are held to a standard of reasonably prudent conduct, and they must *both* take measures to avoid foreseeable harms. It is most common in tort cases to discuss the negligence of the defendant, but the plaintiff can also be found to have failed to exercise appropriate care (e.g., contributory negligence, comparative fault, etc.) or to have voluntarily assumed the risk of harm.

4. Vicarious Liability for Computer Owners

The above discussion concentrates on the negligence of the computer owner in not having current anti-virus software and not having a software firewall on the owner's computer. There is another legal theory that might make the owner liable: because the owner has legal control over the computer, the owner might be *vicariously liable* for any misuse of the computer that is either unauthorized or unknown to the owner.

The law of vicarious liability is well developed in the context that an employer is liable for the acts or omissions of the employer's employees in the scope of their employment.[14] Further, there is considerable federal case law on vicarious liability for copyright infringement.[15]

However, my search of the Westlaw databases on 28 March 2004 found no reported cases in the USA involving vicarious liability for use of a computer.

[12] I assume that the defendant did not know that his computer was infected with a virus and spewing copies of that virus.

[13] *Selby v. Bullock,* 287 So.2d 18, 21 (Fla. 1973) ("Cows know little of strict liability but do respect barbed wire."); *Maguire v. Yanke,* 590 P.2d 85, 88-93 (Idaho 1978). Also see, Restatement (Second) of Torts § 504(4).

[14] *Prosser and Keeton on Torts,* §§ 69-70, (5th ed. 1984); Restatement (Second) of Agency § 219 (1958).

[15] See, e.g., *Sony Corp. of America v. Universal City Studios, Inc.,* 464 U.S. 417, 435-442 (U.S. 1984); *A&M Records, Inc. v. Napster, Inc.,* 114 F.Supp.2d 896 (N.D.Cal. 2000), *aff'd in part,* 239 F.3d 1004 (9th Cir. 2001), *aff'd after injunction modified,* 284 F.3d 1091 (9th Cir. 2002); *Burdick v. Koerner,* 988 F.Supp. 1206, 1209-1210 (E.D.Wis. 1998); *Microsoft Corp. v. Grey Computer,* 910 F.Supp. 1077, 1090-91 (D.Md. 1995).

In a related subject area, hackers dialed the toll-free telephone number for Jiffy Lube Corporation, then dialed additional telephone numbers that allowed the hackers to make free long-distance calls to anyone. A court ordered Jiffy Lube to pay AT&T for such unauthorized long-distance calls. *American Tel. & Tel. Co. v. Jiffy Lube Intern., Inc.,* 813 F.Supp. 1164 (D.Md. 1993). The same liability was later found in *American Tel. and Tel. Co. v. United Research Laboratories, Inc.,* 1994 WL 623566 (E.D.Pa. 1994)("The unfortunate fact of the matter is that while URL is an innocent victim of the criminal actions of unknown third parties, it bears the risk of loss under the law."); *American Message Centers v. F.C.C.,* 50 F.3d 35 (D.C.Cir. 1995); *AT & T Corp. v. Community Health Group,* 931 F.Supp. 719 (S.D.Cal. 1995) and in *AT&T Corp. v. Fleming & Berkley,* 1997 WL 737661 (9th Cir. 1997). Parents of a child who used a home computer to attempt to hack telephone company's computers were ordered by a trial court to pay the telephone company $33,720 (plus reimburse the company for almost $14,000 of attorney's fees), despite a state statute limiting liability of parents to $10,000 for torts of their children, because the telephone company relied on a liquidated damages clause in their tariff. An appellate court reversed the damage award and remanded for proof of actual damages. *Thrifty-Tel, Inc. v. Bezenek,* 54 Cal.Rptr.2d 468 (Cal.App. 4 Dist. 1996). The final result in *Bezenek* is not reported in the Westlaw database. The cases mentioned in this paragraph were decided on contract principles (i.e., a tariff), not by applying vicarious tort liability, however the judges did not find the contract *un*conscionable or invalid for any other reason.

Again, making an analogy to automobiles, a car rental company is responsible for paying the parking files incurred by its customers, although the car rental company had no control over the illegal conduct of its customers. *City of Chicago v. Hertz Commercial Leasing Corp.,* 349 N.E.2d 902 (Ill.App. 1 Dist. 1976), *aff'd,* 375 N.E.2d 1285 (Ill. 1978), *cert. den.,* 439 U.S. 929 (U.S. 1978). This is an example of vicarious liability for a minor criminal offense, *not* tort liability.

5. Conclusion

In March 2004, when this essay was first written, there appears to be no reported case for tort liability for owners of computers in the USA for misuse of their computer by *un*known or *un*authorized persons. Common forms of such misuse include propagation of malicious computer programs, being a zombie computer in a distributed denial-of-service attack on a website, or sending spam e-mail from the owner's computer. This essay suggests new law in the USA, following legal principles accepted in other subject areas of law. There are two ways that such liability could be found by a court:

1. because it was negligent of the owner not to maintain current anti-virus software and a software firewall on the owner's computer, and such negligence might be proximate cause of injury to an innocent victim
2. because the owner of the computer might be vicariously liable for the misuse of the owner's computer by unknown hackers or unknown spammers.

While one can quibble about the applicability of the analogies (e.g., either vehicular homicide or death from smallpox is different from damage to property), the fundamental purpose of tort law is to give a victim financial compensation for negligent, reckless, or intentional conduct that causes harm to the victim. Running a computer without current anti-virus software and without firewall software is certainly poor computing practice (i.e., negligence), and it is an interesting question whether such poor computing practice might also be the proximate cause of harm to someone else.

A statute requiring computer owners to run current anti-virus software and a software firewall on each computer that is connected to the Internet would be beneficial to society by motivating many computer owners to run these security programs. And if nearly every computer connected to the Internet had current anti-virus software and a software firewall, those two programs would help prevent the spread of malicious computer programs, prevent distributed denial-of-service attacks on websites, and would prevent spammers from using innocent computers to send spam e-mail. Incidentally, such a statute could also make it easier for plaintiffs' attorneys to prove negligence in tort litigation, thus helping to compensate innocent victims. However, I believe that negligence could be proved without such a statute.[16]

The real problem here is that the technology in malicious computer programs is advancing very rapidly, so that articles on computer viruses that are only five years old now seem quaintly antique. However, it takes law tens of years to adapt to new technology.[17] At the rate that computer technology is advancing, the law will never catch up, so the only solution to problems of computer crime is with more technology (e.g., anti-virus software and firewall software).
In my opinion, the law should require that people use such appropriate technology to prevent harm to society.

[16] It is negligent to operate a computer that is connected to the Internet without current anti-virus software and firewall software, just as it is negligent to drive a car with defective brakes. In both cases, it is foreseeable that someone will be injured.

[17] Ronald B. Standler, *Response of Law to New Technology,* (1997) http://www.rbs2.com/lt.htm .

This document is at **www.rbs2.com/cvicarious.pdf**
My most recent search for court cases on this topic was in March 2004
created 11 March 2004, revised 17 Apr 2004

go to my essay, *Tips for Avoiding Computer Crime,* at http://www.rbs2.com/cvict.htm , which I began in May 1999 to explain the need for good computing practices, including anti-virus software and software firewalls, to people.

return to my homepage at http://www.rbs2.com/