DEALING WITH LIABILITY RISKS TO OWNERS OF COMPUTERS USED IN DENIAL OF SERVICE ATTACKS

ROBERT A. BOURQUE AND BLAKE A. BELL
SIMPSON THACHER & BARTLETT LLP

JULY 6, 2000

Robert A. Bourque *is a partner with Simpson Thacher & Bartlett and chair of the firm's technology committee.* ***Blake A. Bell*** *is senior knowledge management counsel with Simpson Thacher.*

Their names sound ominous, almost chilling: "The Ping of Death"; "E-Mail Bombing"; "Flood Attack". The damage they can cause is breathtaking. "They" are all variants of the same thing — so-called "Denial of Service Attacks."

Anyone owning a computer or network connected to the Internet should not ignore the risk that a hacker could take remote control of your computers and misuse them to wage an electronic attack against a third party. Nor should you ignore the risk that you could be sued for the hacker's misuse of your computers in such circumstances.

WHAT IS A DENIAL OF SERVICE ATTACK?

A Denial of Service attack (or DoS attack as it often is called) is a method used to deny legitimate users access to a computer or a network of computers. A Distributed Denial of Service Attack, known as a DDoS attack, typically is performed on a larger scale because many different computers are used at one time to effect the denial of service.[1]

Many DDoS attacks involve remotely accessing other persons' or companies' computers and then instructing those computers to bombard targeted computers, such as computers that host particular Web sites, with fake traffic intended to overwhelm those computers and effectively deny access to them by legitimate users.

To conduct such an attack, a hacker typically uses software tools that are widely and freely available on the Internet. The tools have names such as Trin00, Tribal Flood Network, TFN2K and Stacheldraht.

Using online access, the hacker breaks into inadequately-secured computers intended for use to wage an attack against a third-party's computers. On the inadequately-secured computers, the hacker installs software programs sometimes known as "soldiers" or "slaves." The hacker instructs these programs to respond at a later time to commands that the hacker sends from a remote location using a remote computer connected to the Internet.

To begin an attack, the hacker uses a computer to send commands to the soldier or slave programs instructing them, for example, to flood a third-party's targeted computer, or computer network, with fake traffic. The computers containing the soldier or slave programs — which the hacker misuses to wage the attack — which themselves are victims of the hacker — are sometimes called "zombies". On some occasions, the zombies are instructed by the hacker to use fake — or "spoofed" — Web addresses so that it appears that the data streaming from the zombies is coming from locations other than their actual locations. This can make it even more difficult to track down the culprit.

RECENT DDOS ATTACKS

Perhaps the most widely-reported DDoS attacks that have occurred so far took place on three successive days earlier this year. On February 7, Yahoo.com experienced an assault that shut down the Web site — one of the world's most popular and most heavily-trafficked sites — for more than three hours. The next day, additional assaults were directed at online auction site eBay, online retailer Buy.com, online bookseller Amazon.com and online news service CNN.com. The impact of the attacks was massive. Buy.com's Web site was disrupted for three hours on the very same day the company was going public through an initial public offering of its stock. eBay's and CNN's sites were shut down for nearly two hours and Amazon.com was offline for one hour.

On Wednesday, February 9, the assaults continued. That day, the Web sites of online broker E*Trade and technology information provider ZDNet were attacked. The Federal Bureau of Investigation commenced an investigation almost immediately.[2]

This article will explore some of the liability risks and other risks faced by the owners of computers used in such denial of service attacks — the owners of the so-called "zombies." Such an issue is of particular interest since in most attacks, the responsible hacker will be anonymous and difficult, if not impossible, to identify. Moreover, even if identified, the culprit is likely to be effectively judgment-proof due to the massive losses that can result from such attacks.[3] Thus, the only identifiable "deep pockets" for injured parties to sue may be the owners of networks whose computers are misused to wage such attacks. Commentators have begun to reference the risk of liability in such circumstances as a matter of "downstream liability."[4] This article also will outline some of the steps that could be taken to mitigate the risks associated with such DDoS attacks.

THE FIRST CLAIM FOR "NEGLIGENTLY ALLOWING ONESELF TO BE HACKED" MAY LOOM

No reported downstream liability case appears yet to have been brought. But, if news reports are any indication, a case is being prepared for the Scottish courts as this article is being written. The threatened litigation arises from a June 21 incident in which Web hijackers took over the domain name Nike.com, owned by sports shoe manufacturer Nike, Inc., and redirected visitors who tried to access Nike.com to an anti-Nike Web site operated by a social activist group.[5]

On June 21, FirstNET Online (Management) Limited, owner of FrugalNames, learned that the domain name www.nike.com had been "repointed" to the protesters' Web site hosted on FrugalNames' servers. In a press release, FirstNET reportedly alleged that Nike's technical contacts listed with domain name registrar Network Solutions were outdated and that the company failed to return its calls. FirstNET further alleged in its press release that the re-routed Web site was attracting "additional (and unauthorised) traffic hitting our servers [and] is causing our existing clients' site performance to be undermined. Assuming that this happening is . . . attributed to Nike, Inc., through error or omission, it cannot be overstated that such a breach in their security has a knock-on effect for our company and our clients." Additionally, according to one report, Nike asked FirstNET to redirect traffic back to Nike's servers as an emergency measure so that people typing the Web address Nike.com would see Nike's Web site and not that of the protesters.[6]

After the incident, FirstNET reportedly submitted an invoice to Nike for the services it performed in trying to assist Nike in fending off the hijacking. Nike reportedly refused to pay the invoice.[7]

Now FirstNET Online reportedly "is preparing to sue the shoe maker — for 'allowing' itself to be hacked."[8] FirstNET apparently believes that Nike failed to implement adequate security measures with the administrator of its domain name to prevent unauthorized repointing of the domain name by hackers. Nike denies the allegation and counters that even before the incident it asked the administrator of its domain name to take additional steps to prevent such a hijacking.

FirstNET has suggested that it may bring a proceeding against Nike in a Scottish court. FirstNET reportedly plans to pursue "a claim for compensation for the disruption caused by the enormous amount of traffic generated by 'nike.com'".[9] While the case, of course, would not be a pure downstream liability case involving a DDoS attack, the essence of the claim would be similar — an allegation that Nike negligently allowed itself to be hacked in a way that caused damage to FirstNET.

NEGLIGENCE AS THE BASIS FOR DOWNSTREAM LIABILITY

Some commentators suggest that a lack of attention to computer security usually explains how "slave" or "soldier" software could be inserted on the computers used by a hacker to conduct a DDoS attack. Thus, the argument goes, a negligence theory might best be used to impose liability on the owners of such computers. As one commentator has put it:

> I think there is a straightforward negligence argument . . . People hacked into these computers using known [security] holes in most cases. If you maintain security against known hacker attacks, then it's much more difficult to plant the code that allows your server to be turned into a zombie.[10]

As the argument goes, the plaintiff in a downstream liability lawsuit would be expected to introduce evidence to show that the owners of the "zombies" used in the attack utilized out-

of-date software and/or "inadequately-configured defenses." Testimony would be elicited "that fixes for well-known vulnerabilities have been available for years at [little or] no cost from software manufacturers, security firms, and from volunteers freely exchanging solutions." Additionally, testimony likely would be elicited from computer owners or administrators of any network whose computers were used to mount the attack regarding whether they knew or should have known their network was vulnerable and whether they knew where to obtain the fixes for the vulnerability but failed to do so.[11]

Negligence "is the great, generic catch basin of tort law. As such, 'what is negligence' is almost as difficult to answer as 'what is a tort.'"[12] Each of the elements of the tort of negligence, of course, must be proven — even in the context of a so-called "computer tort." Those elements are: (1) the existence of a legally-cognizable duty; (2) a breach of that duty; (3) proximate cause between the conduct and the resulting injury; and (4) actual loss or damage.[13]

Those commentators who have considered the issue have suggested that one possible defense to a negligence claim against the owner of a computer used in a DDoS attack might revolve around whether the owner owed the injured party a duty to exercise due care. They argue that even when a defendant has acted badly, there can be no tort of negligence absent a showing that the defendant owed a duty of due care to the plaintiff. Or, as Professor William Prosser so eloquently stated in his seminal treatise on the *Law of Torts*, it is possible that "the defendant was negligent, but is not liable because he was under no duty to the plaintiff not to be."[14]

Duty, of course, cannot be addressed meaningfully without considering the concept of proximate cause. Indeed, Professor Prosser concluded that assessment of duty is essentially inseparable from assessment of proximate cause.[15]

Defending downstream liability lawsuits by arguing that the defendant owed no duty of due care to the plaintiff will present difficult and resource-consuming policy questions. Indeed, the parties in such disputes likely will face off precisely as did the majority and the dissenters in *Palsgraf v. Long Island Railroad Co.*[16]

In *Palsgraf*, a passenger being helped aboard a moving train by a railroad employee dropped a package containing fireworks.The package fell onto the tracks and exploded. The concussion dislodged scales standing at a distance from the train. The scales struck a woman. She sued the railroad. A jury found the railroad negligent.

On appeal, Judge Benjamin Cardozo wrote the majority's opinion. He determined that the railroad had no liability in the case because it was not negligent toward the plaintiff. He emphasized that negligence is not based on a duty owed to the world at large, but is founded on the foreseeability of harm to the plaintiff who was injured. The dissenters, in contrast, argued that a duty of due care is owed to the "world at large" to refrain "from those acts which unreasonably threaten the safety of others"even if those others are "outside what would generally be thought the danger zone."

In a downstream liability case, a defendant likely will argue that any "wrong" to the owners of disrupted computer systems is not actionable because it is not a "wrong personal to" them. To hold otherwise, the argument goes, would be to find a duty to the online "world at large."

The plaintiff in a downstream liability case, however, need not adopt the dissent's view in the *Palsgraf* case. Rather, such a plaintiff likely will assert not only that policy considerations justify imposing liability (*see* below), but also that the harm the plaintiff suffered was entirely foreseeable to the defendant particularly given the widespread attention that such attacks have received in the last few years.

In defending such claims and responding to such arguments, however, it would be a mistake for defendants and their counsel to focus solely on whether the defendant owed the plaintiff a duty of due care. For example, there may well be an argument, in appropriate circumstances, that the defendant bears no liability due to plaintiff's own negligence in the matter. As Professor Prosser noted in his treatise:

> There are many situations in which the hypothetical reasonable man would be expected to anticipate and guard against the conduct of others. . . . He is required to realize that there will be a certain amount of negligence in the world. . . . [W]hen the risk becomes a serious one, either because the threatened harm is great, or because there is an especial likelihood that it will occur, reasonable care may demand precautions against 'that occasional negligence which is one of the ordinary incidents of human life and therefore to be anticipated.'"[17]

Unfortunately, DoS attacks arguably have become so common and so widely known that they arguably have risen to the level of "ordinary incidents of human life," at least in the online context. Thus, those who fail to recognize the serious risk of such attacks and themselves fail to take reasonable precautions to ***defend*** against them may have little recourse against the unwitting — though admittedly careless — owners of the computers coopted by a hacker to commit an attack.

Although no cases appear to have addressed this line of defense in the context of liability for a DoS attack, the issue has been touched upon in an arguably analogous context. In *Computer Tool & Engineering, Inc. v. Northern States Power Co.*,[18] a company whose computer equipment was damaged by a power surge sued the local power and telephone companies alleging that their negligence caused a power surge that damaged the company's equipment. The court allowed the jury in the case to consider the plaintiff's own negligence in failing to protect against the power surge. The result was a substantially reduced damage award to the plaintiff. The plaintiff appealed, arguing that the trial court erred in allowing the jury to conduct a comparative negligence analysis. The appellate court affirmed the trial court's decision to allow the jury to consider plaintiff's negligence. According to the court, the matter was properly submitted to the jury because there was evidence that the plaintiff knew that a power surge could damage its equipment and that inexpensive hardware to protect the equipment from such a power surge was available. Yet, according to the court, the plaintiff did

not install such protection despite the fact that it knew of prior irregularities in the power supply.

The decision in *Computer Tool & Engineering* would certainly seem relevant to an analysis of whether and to what extent the owner of a computer or a computer network that is unwittingly used to commit a DoS attack should be held liable for the misuse of its computer system. It would seem unlikely that the party injured in such an attack would be unaware of the risk of such attacks particularly given the widespread media attention such attacks typically receive (witness, for example, the prominent stories that appeared in virtually every major print publication following the February attacks that caught the world's attention earlier this year). And, there are simple (though potentially expensive) techniques available to fend off such attacks. Perhaps the simplest of such techniques — one reportedly used by E*Trade to fend off the attack it faced last February 9 — involves the use of detection software to identify the commencement of a DoS attack followed by the prompt redirection of customer traffic to servers that are not targeted in the attack. There are other defensive techniques as well.[19]

Yet, the decision in *Computer Tool & Engineering* might best be explained by a simple economic analysis of the outcome in the case. In effect, responsibility for the damage was allocated based on the parties' abilities to manage the risk most efficiently. If that is the proper way to read the case, then there is at least an argument that the decision may actually support the imposition of liability on the owners of zombie computers used in DDoS attacks under the theory that they best can manage the risks that lead to such attacks by taking simple and cost-effective precautions to protect their own systems from intrusion by hackers seeking to install slave or soldier software.

Economic allocation of liability in such cases recently was addressed in an article published by Hal R. Varian in *The New York Times* on June 1 of this year.[20] In that article, Varian essentially argued that network operators who own the computer networks within which individual computers are used as zombies should bear the brunt of liability for damages resulting from DoS attacks. According to Varian:

> One reason computer security is so poor in practice is that the liability is so diffuse. Consider the attacks that took place a few months ago, in which computer vandals took over computers on relatively unprotected university networks and used them to shut down Yahoo and other major Web sites. Although the universities found the takeover of their machines a nuisance, they didn't bear the bulk of the costs of the attack on Yahoo. But if [the] universities bore some liability for the damages to third parties, they would have a stronger incentive to make their networks more secure." [21]

Varian, in short, would place liability squarely on the shoulders of the operator of the computer network whose computers were used in the attack and not the individual users of those networked zombie computers because, according to Varian's view, "[t]he average user is essentially clueless about how to prevent his computer from being taken over, so assigning liability to him would be pointless. Assigning liability to the network operator would make more sense."

Varian argues, in effect, that if liability for such attacks were to be better clarified — or, at a minimum, rendered less "diffuse" — by imposing liability on the operators of computer networks whose computers are used in such attacks, networks would have a greater incentive to obtain insurance against the risk. Economically rational insurers, in turn, would have incentives to improve their clients' security practices to reduce or eliminate their own losses. Under such circumstances, Varian argues, computer security in general likely would improve.[22]

While the dispute over whether and how the owners of zombie computers used in such attacks may be held liable for failing to take steps to protect their systems against intrusion continues to rage, there seems to be little dispute regarding whether zombie owners will, some day, find themselves subject to suit for failing to take such precautions.[23] Thus, it would seem prudent for network operators to take steps such as those described at the end of this article to minimize their risk in this regard.

LAWSUITS ARE NOT THE ONLY RISK

Lawsuits, of course, are not the only risks faced by those whose computers are used to conduct DoS attacks. Indeed, companies in heavily regulated industries must be sensitive to and cognizant of the risk that if an intruder misuses their computer systems to conduct such attacks, they may have an obligation to alert government regulators.

For example, banks and certain other financial institutions whose computer networks are infiltrated and used to conduct DoS attacks may have an obligation to report such instances, depending on the computer systems that are infiltrated by the hacker, to the Federal Bureau of Investigation's Computer Crimes Unit and to the Suspicious Activity Reporting System using a Suspicious Activity Report. Indeed, on June 19 of this year, five federal banking agencies and the Financial Crimes Enforcement Network jointly issued revised Suspicious Activity Report Forms. Among many other changes, the revised forms now include reporting requirements for computer intrusions "in recognition of the need to obtain more specific information with regard to computer related suspicious activity". The new report defines a "computer intrusion" that triggers reporting obligations to include "gaining access to a computer system of a financial institution to . . . damage, disable or ***otherwise affect*** critical systems of the institution."[24] Thus, once such institutions learn that their computer systems have been used to wage a DoS attack, they must consider their own obligations to report such activity using the newly-revised Suspicious Activity Report Form.

Of course, another risk faced by those whose computers are used to wage DoS attacks is the substantial expense and diversion of productive resources that most assuredly will follow such an attack as law enforcement investigators and, in some instances, regulators swoop in to investigate the attack and trace it to its source. The impact that such an investigation can have on a business cannot be minimized, particularly in instances where the attack is a high profile attack such as those that occurred last February. As the old saw goes, an ounce of prevention is worth a pound of cure. The remainder of this article will discuss the prevention that should be considered.

MINIMIZING THE RISKS OF LIABILITY

Much can be done to minimize the risks of liability in this context. What follows is a summary of some of the principal steps that firms may wish to consider to reduce their risks of downstream liability in connection with DoS attacks.

- Arrange a computer security audit or risk assessment of the firm's computer systems, perhaps using an independent, third-party auditor, to satisfy yourself that the firm's systems are state-of-the-art and include current software.

- Implement a meaningful security management infrastructure based on state-of-the-art security applications including firewalls, vulnerability scanning, intrusion detection systems and the like.[25]

- Satisfy yourself that appropriate senior technical staff are well-versed in current Internet security issues and instruct them to keep security systems current and reliable.

- Learn more about DDoS attacks and about Internet security in general and encourage your technical staff to do the same.[26]

- Obtain insurance against the liability risk you may face. The insurance community is creating products in this and related areas and you should review your options.[27]

- Establish an Incident Response Team designed to enable senior technical staff with meaningful access to senior management to respond quickly in the event the firm detects a misuse of its systems in connection with a possible DoS attack.

- In the event you discover that an attack is underway using your systems, contemplate temporarily disabling your systems if that is a reasonable option. Contact law enforcement personnel to inform them of the incident.

- In the event that an attack is discovered using your systems, collect and preserve system log information that might be important evidence of the intrusion and misuse of your systems. Collect this data quickly before it is accidentally — or even deliberately — erased.

Finally, it is well and good to take steps to reduce your risk of liability for damages inflicted on others. But, don't lose sight of the fact that your systems may also become the target of an attack directed at bringing down ***your*** computers. Preparation for that possibility is also required.[28]

ENDNOTES

1 *See* Symantec AntiVirus Research Center, *Denial of Service Attack (DoS)* <http://www.symantec.com/avcenter/venc/data/dos.attack.html> (visited June 3, 2000); Jenevra Georgini, *Distributed Denial of Service Attacks*, 16(11) E-COMMERCE 8 (Mar. 2000). For an excellent whitepaper describing DDoS attacks, DDoS tools, and techniques for defending against such attacks, *see* Internet Security Systems, *Distributed Denial of Service Attack Tools* (visited June 24, 2000) <http://documents.iss.net/whitepapers/ddos.pdf>.

2 *See* Jonathan Dube, *Web Under Attack - Five Leading Web Sites Suffer Outages After Coordinated Attacks This Week*, ABCNEWS.COM, Feb. 8, 2000 <http://abcnews.go.com/sections/tech/DailyNews/yahoo000208.html>; Matt Richtel & Sara Robinson, *Several Web Sites Are Attacked on Day After Assault Shut Yahoo*, N.Y. TIMES ON THE WEB, Feb. 9, 2000 <http://www.nytimes.com/library/tech/00/02/biztech/articles/09hack.html>.

3 As one commentator puts it, rather bluntly, "whom would you rather sue: some impecunious wretch sitting in a basement cackling over his latest attack . . . or a real business with assets?" M.E. Kabay, *Distributed Denial-of-Service Attacks, Contributory Negligence and Downstream Liability*, UBIQUITY - AN ACM IT MAGAZINE AND FORUM <http://acm.org/ubiquity/views/m_kabay_1.html> (visited June 21, 2000).

4 *See* M.E. Kabay, *Distributed Denial-of-Service Attacks, Contributory Negligence and Downstream Liability*, UBIQUITY - AN ACM IT MAGAZINE AND FORUM <http://acm.org/ubiquity/views/m_kabay_1.html> (visited June 21, 2000). *See also* Hal R. Varian, *Economic Scene: Liability for Net Vandalism Should Rest With Those That Can Best Manage the Risk*, N.Y. TIMES, June 1, 2000, at C2, col. 1 (available via N.Y. TIMES ON THE WEB at http://www.nytimes.com/library/financial/columns/060100econ-scene.html>); Matthew G. DeVost, *Editorial - Distributed Denial Of Service Attacks Raise Liability Questions*, INFO-SEC.COM (Feb. 11, 2000) <http://www.info-sec.com/denial/00/denial_021100c_j.shtml>; Brad K. Gushiken, *March 20, 2000 - Possible Liability for Owners of Computers Used in "Denial of Service" Attacks*, HAWAIILAWYER.COM (Mar. 20, 2000) <http://www.hawaiilawyer.com/articles/ebiznews.htm>; Loraine Lawson, *Could a DDoS Attack Land You in Court? Experts Say Yes*, ARIZONA STATE UNIV. TECHREPUBLIC (Apr. 5, 2000) <http://phy.asu.edu/computer/security/liable.htm>; Michael D. Scott, *Denial of Service Attacks - A New Threat*, 4(11) CYBERSPACE LAWYER 1 (Glasser LegalWorks Feb. 2000).

5 *See* Bob Sullivan, *Nike.com Hijacked by Protesters*, MSNBC.COM, June 21, 2000 <http://www.msnbc.com/news/423820.asp>; *Nike Says Web Site Was Hacked In Protest of Economic Forum*, WALL ST. J. INTERACTIVE ED., June 22, 2000 <http://interactive.wsj.com/articles/SB961632106181641786.htm> (paid subscription required); Matt Richtel, *Protesters Hack Nike Web Site*, N.Y. TIMES ON THE WEB, June 22,

2000 <http://www.nytimes.com/library/tech/00/06/biztech/articles/22nike.html>; *Hackers Take Over Nike Web Site*, Associated Press special to CNET News.com, June 21, 2000 <http://news.cnet.com/news/0-1007-200-2122747.html>; *ShameOnNike.com* (visited July 5, 2000) <http://www.shameonnike.com/>.

6 *See* David Raikow, New Legal Storm on Net Horizon, special to ZDNet (July 4, 2000) <http://www.zdnet.com/zdnn/stories/comment/0,5859,2597881,00.html>. *See also* Craig Bicknell, *Whom To Sue for Nike.com Hack?*, WIREDNEWS.COM, June 29, 2000 <http://www.wired.com/news/politics/0,1283,37286,00.html> (part 1) and <http://www.wired.com/news/politics/0,1283,37286-2,00.html> (part 2).

7 *Id.*

8 *Id*.

9 *Id.* Additionally, FirstNET reportedly plans to bring a claim that sounds in breach of contract because it "says it provided a service [to Nike] and deserves to be paid." *Id.*

10 Brad K. Gushiken, *March 20, 2000 - Possible Liability for Owners of Computers Used in "Denial of Service" Attacks*, HAWAIILAWYER.COM (Mar. 20, 2000) <http://www.hawaiilawyer.com/articles/ebiznews.htm> (quoting Stewart A. Baker, Esq. of Steptoe & Johnson LLP of Washington, D.C.).

11 *See* M.E. Kabay, *Distributed Denial-of-Service Attacks, Contributory Negligence and Downstream Liability*, UBIQUITY - AN ACM IT MAGAZINE AND FORUM <http://acm.org/ubiquity/views/m_kabay_1.html> (visited June 21, 2000).

12 1 COMPUTER LAW GUIDE (CCH) ¶ 17,601, at 28,501 (1999).

13 William L. Prosser, HANDBOOK OF THE LAW OF TORTS 143 (4th Ed. West Pub. Co. 1971); 1 COMPUTER LAW GUIDE (CCH) ¶ 17,601, at 28,501 (1999).

14 William L. Prosser, HANDBOOK OF THE LAW OF TORTS 143 (4th Ed. West Pub. Co. 1971).

15 *Id.* at 244-45.

16 248 N.Y. 339, 162 N.E. 99 (1928).

17 William L. Prosser, HANDBOOK OF THE LAW OF TORTS 170-71 (4th Ed. West Pub. Co. 1971).

18 453 N.W.2d 569 (Minn. Ct. App. 1990).

19 *See* Rutrell Yasin, *New Defense for DoS Attacks*, CMP'S TECHWEB, May 5, 2000 <http://www.internetwk.com:80/story/INW20000505S0003>; Symantec AntiVirus

Research Center, *Denial of Service Attack (DoS)* (visited June 1, 2000) <http://www.symantec.com/avcenter/venc/data/dos.attack.html>; Internet Security Systems, *Dealing With Internet Attacks* (visited June 1, 2000) <http://www.iss.net/news/denial.php>; Chey Cobb & Stephen Cobb, *Denial of Service* (visited June 1, 2000) <http://www.miora.com/articles/art-scdos.htm>; Cisco Systems, *Defining Strategies To Protect Against TCP SYN Denial of Service Attacks*, July 8, 1999 <http://www.cisco.com/warp/public/707/4.html>; Carnegie Mellon Software Engineering Institute CERT Coordination Center, *Denial of Service Attacks* (visited June 1, 2000) <http://www.cert.org/tech_tips/denial_of_service.html>.

20 Hal R. Varian, *Economic Scene: Liability for Net Vandalism Should Rest With Those That Can Best Manage the Risk*, N.Y. TIMES, June 1, 2000, at C2, col. 1 (available via N.Y. TIMES ON THE WEB at <http://www.nytimes.com/library/financial/columns/060100econ-scene.html>).

21 *Id.*

22 Thus, for example, under Varian's view when an individual computer owner's computer connected to the Internet via a broadband cable connection is misused by a hacker to wage an attack, Varian would urge the courts to hold the cable system network operator liable for the attack rather than the individual computer owner. This makes sense, according to Varian, because the cable system operator is better situated than the "clueless" average computer user to insure against and to take measures to prevent such attacks.

23 The owners of such zombies, of course, likely would have common law claims against the hacker who misused their networks, although once again that would seem to be of little consolation where the damages are large and the hacker is either difficult to identify or effectively judgment proof. If the zombie owner is a financial institution whose systems have been misused, it may have a statutory claim against the hacker as well. The Computer Fraud and Abuse Act, Pub. L. No. 99-474, 100 Stat. 1213 (1986) (codified as amended at 18 U.S.C. § 1030(a)(5) (West 1999)) allows a financial institution victimized by a federal computer crime to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g). *See also* Elizabeth C. Yen, *Counsel's Corner*, 116 BANKING L.J. 403, 403 n.2 (Apr.-May 1999).

24 *Suspicious Activity Report*, FRB FR 2230, FDIC 6710/06, OCC 8010-9 / 8010-1, OTS 1601, NCUA 2362, Treasury TD F 90-22 47 (Revised June 2000) <http://www.treas.gov/fincen/f9022-47-1.pdf> (emphasis added). *See also* Elizabeth C. Yen, *Counsel's Corner*, 116 BANKING L.J. 403, 403 & n.1 (Apr.-May 1999) ("Unauthorized access to or tampering of a bank's computer system . . . may violate 18 U.S.C. Section 1030, a federal computer crime statute, potentially triggering a SAR filing"); *Guidance for Financial Institutions on Reporting Computer-Related Crimes*, FDIC FINANCIAL INSTITUTION

LETTER FIL-124-97 (Dec. 5, 1997)
<http://www.fdic.gov/news/news/financial/1997/fil97124.html#attach>; *Reporting Computer Related Crimes*, COMPTROLLER OF THE CURRENCY AL 97-9 (Nov. 19, 1997)
<http://www.occ.treas.gov/ftp/advisory/97-9.txt>; *Guidance Concerning the Reporting of Computer-Related Crimes by Financial Institutions*, BOARD OF GOV. OF THE FED. RESERVE SYSTEM SR 97-28 (ENF) (Nov. 6, 1997)
<http://www.federalreserve.gov/boarddocs/SRLETTERS/1997/SR9728.HTM>; *Infrastructure Threats from Cyber-Terrorists*, OFFICE OF THE COMPTROLLER OF THE CURRENCY BULLETIN OCC 99-9 (Mar. 5, 1999) (National Banks must "Report significant unauthorized [computer] access attempts to the FBI Computer Crimes Unit unit and the Suspicious Activity Reporting System") <http://www.occ.treas.gov/ftp/bulletin/99-9.txt>..

25 There are products designed to detect use of computers as zombies, some of which are free. *See, e.g., Network Associates Announces On-Line Dectector for Denial of Service Vulnerabilities* (visited June 1, 2000) <http://www.nai.com/dm/dsvjump.asp> (offering a free service called "CyberCop Zombie Scan" which is an "on-line solution to detect if your computer can be used as a jump-point for hackers").

26 The resources on this topic are legion, and many are freely available. *See, e.g., Internet Security Systems X-Force Database* (visited June 24, 2000) <http://xforce.iss.net/>; Internet Security Systems, *Denial of Service Attack Using the TFN2K and Stacheldraht Programs*, ISS Security Alert Advisory 43 (Feb. 9, 2000)
<http://xforce.iss.net/alerts/advise43.php>; Internet Security Systems, *Distributed Denial of Service Attack Tools* (visited June 24, 2000)
<http://documents.iss.net/whitepapers/ddos.pdf>.

27 *See News and Views: E-Commerce Insurance Offered*, 2(4) E-COMMERCE L. REP. 24 (Glasser LegalWorks Feb. 2000); Lorelie S. Masters, *Big Hack Attack: Insurance in the New Millennium*, 2(5) E-COMMERCE L. REP. 21 (Glasser LegalWorks Mar. 2000).

28 Once again, the literature on this topic is extensive and typically freely available. *See, e.g., supra* at n.12.