COMPUTER SECURITY PUBLICATIONS: INFORMATION ECONOMICS, SHIFTING LIABILITY AND THE FIRST AMENDMENT

ETHAN PRESTON* & JOHN LOFTON**

> Society increasingly depends upon technological means of controlling access to digital files and systems, whether they are military computers, bank records, academic records, copyrighted works or something else entirely. There are far too many who, given any opportunity, will bypass those security measures, some for the sheer joy of doing it, some for innocuous reasons, and others for more malevolent purposes. Given the virtually instantaneous and worldwide dissemination widely available via the Internet, the only rational assumption is that once a computer program capable of bypassing such an access control system is disseminated, it will be used.[1]

I. INTRODUCTION

From July through August 2001, a malicious computer program swept across the Internet. The program propagated itself by infecting at first a few computers, and then using those computers to find and

* B.A., University of Texas at Austin, 1998. J.D., Georgetown University Law Center, 2001. This author would like to thank John Litwinski, Leonard Sanchez and M. Eliza Stewart for their insightful comments and support.

** B.A., University of Texas at Austin, 1998. J.D., Boalt Hall School of Law, May 2002.

1. *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 451-52 (2d Cir. 2001) (quoting), *aff'g, Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 331 (S.D.N.Y. 2000).

exploit still more vulnerable computers. The program's name was Code Red. It is estimated that Code Red would infect nearly a million computers and would cause an estimated 2.4 billion dollars in damage before it ran its course.[2]

Code Red's story began on June 18, 2001, when a computer security firm, named eEye, announced on its Web page that it had discovered a vulnerability in Microsoft's Internet Information Server (IIS).[3] The eEye firm found that the portion of IIS was vulnerable to a carefully crafted data input, called a buffer overflow.[4] A buffer overflow functions by inputting more data than a vulnerable program anticipates.[5] The buffer overflow then overwrites portions of the program in the computer's memory, or RAM.[6] Because the program only reserves memory space for the anticipated data, the extra input "overflows" into memory reserved for the program, overwriting portions of the vulnerable program's code.[7] After processing the anticipated input in the reserved space in the memory, the computer then interprets the unanticipated overflow as part of the original, vulnerable program.[8] The end result is that if a buffer overflow is properly constructed, it may be used to gain control over the

2. *See* H.R. Subcomm. on Govt. Efficiency, Fin. Mgt., & Intergovt. Rel., Comm. on Govt. Reform, *Hearings on "What Can Be Done to Reduce the Threats Posed by Computer Viruses and Worms to the Workings of Government*," 107th Cong. (Aug. 29, 2001) (citing U.S. Gen. Acctg. Off. Chief Technologist Keith A. Rhodes' statement: *Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures* 4 (available at <http://www.gao.gov/new.items/d011073.pdf> (accessed Oct. 1, 2002)).

3. eEye, *All Versions of Microsoft Internet Information Services Remote Buffer Overflow (SYSTEM Level Access)* [¶ 3] (June 18, 2001) <http://www.eeye.com/html/Research/Advisories/AD20010618.html > (accessed Oct. 7, 2002); George V. Hulme, *Full Disclosure—Are Security Software Vendors Trying to Keep Systems Safe From Threats Such as Code Red, or Are They More Worried About Self-Promotion?* [¶ 5] (Aug. 6, 2001) <http://www.informationweek.com/story/IWK20010803S0020> (accessed Oct. 7, 2002)).

4. eEye, *supra* n. 3, at [¶ 3].

5. Bruce Schneier, *Secrets & Lies: Digital Security in a Networked World* 207-09 (John Wiley & Sons, Inc. 2000) (detailing a more lucid discussion of buffer overflows).

6. *Id*.

7. *Id*.

8. *See* Hal Berghel, *The Code Red Worm* [¶¶ 5, 17] (Dec. 1, 2001) <http://www.acm.org/~hlb/index2.html> (citing a more precise account of the exact vulnerability in IIS can be obtained) (accessed Oct. 1, 2002).

computer.[9] Notably, eEye did not actually release this buffer overflow, though it said it would at some future date.[10]

On the same day eEye announced its discovery to a specialized e-mail list, named BugTraq,[11] Microsoft released a small program that would eliminate this vulnerability by prior arrangement.[12] BugTraq is an e-mail journal on computer security and computer security vulnerabilities with around 40,000 readers.[13] BugTraq is a respected publication on computer security vulnerabilities. Its prominence is roughly analogous to that of the *New England Journal of Medicine* with respect to public health and medicine.[14] Three days after eEye announced its discovery, someone using the pseudonym "HighSpeed Junkie" independently released the actual buffer overflow needed to exploit the vulnerability of a public Web site.[15]

The first of Code Red exploitations began July 12, 2001 with reports of the attacks appearing the next day.[16] Code Red was a worm that used the vulnerability in IIS to gain control of a target machine.[17]

9. Schneier, *supra* n. 5, at 207.

10. *See* eEye*, supra* n. 3, at [¶ 25].

11. E-mail from Marc Maiffert, eEye's chief hacking officer, to BugTraq, *All Versions of Microsoft Internet Information Services, Remote Buffer Overflow (SYSTEM Level Access)* [¶ 3] (June 18, 2001) (copy on file with *Whittier Law Review*).

12. Microsoft, *Microsoft Security Bulletin MS01-033; Unchecked Buffer in Index Server ISAPI Extension Could Enable Web Server Compromise* (June 18, 2001) <http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/bulletin/ms01-033.asp> (accessed Oct. 7, 2002).

13. Brian McWilliams, "*Happy Hacker" Drops a Bomb on Security Experts* [¶ 14] (Oct. 1, 2001) (copy on file with *Whittier Law Review*).

14. *See* Insecure.Org, *Insecure Mailing List Archive: Must-Read Security Lists* <http://lists.insecure.org/#bugtraq> (accessed Oct. 1, 2002).

15. Brian McWilliams, *Attack Program Exploits New Microsoft Bug*, Newsbytes [¶2] (July 3, 2001) (copy on file with *Whittier Law Review*); Thomas C. Greene, *IIS Worm Made to Packet Whitehouse.gov* [¶2] (July 19, 2001) <http://www.theregister.co.uk/content/4/20474.html> (accessed Oct. 1, 2002).

16. Berghel, *supra* n. 8, at [¶ 16]; CAIDA, *CAIDA Analysis of Code-Red: Code-Red Worms: A Global Threat* (last updated June 14, 2002) <http://www.caida.org/analysis/security/code-red/ > (accessed Oct. 1, 2002).

17. Berghel, *supra* n. 8, at [¶ 4];

> Worms . . . run as autonomous, standalone programs. Worms achieve their malevolence without need of unsuspecting host programs for either infection or propagation. Passive worms propagate with data transmissions, such as e-mail, as in the case of the VBS/AnnaKournikova spamming worm that used Visual Basic to exploit a hole in Microsoft Outlook to replicate itself to everyone in the host computer's e-mail address book. . . .

Once in control, Code Red would replace the computer's Web page, set the computer to scan for other computers with the same vulnerability, and infect them.[18] Code Red set the computers to flood the White House home page with data, making it inaccessible on prearranged dates.[19] Code Red was supposed to scan random blocks of IP addresses, but a flaw in its design restricted its growth.[20] Nevertheless, Code Red infected over 12,000 computers by July 18.[21]

On July 19, 2001 a second version of Code Red (CRv2) was first sighted.[22] While the previous version of Code Red scanned only limited sections of the Internet, CRv2 scanned for vulnerable computers all across the Internet.[23] The CRv2 rate of infection was dramatically higher than the first version of Code Red. An estimated 359,000 computers were infected 14 hours after the first sighting of CRv2.[24] This second version generated such severe problems that on July 30, Microsoft and the FBI National Infrastructure Protection Center held a press conference urging the application of Microsoft's patch and describing the disinfection procedure for Code Red.[25]

Around August 4, 2001 a new and entirely different version of Code Red was discovered.[26] Because it exploited the same vulnerability, it was named Code Red II. However, Code Red II was significantly more dangerous than the prior versions because it created a "back door" into the computer, allowing unauthorized parties to control an infected computer.[27] It also scanned the Internet for other vulnerable computers, but did not announce its presence to the

> Active worms, on the other hand, exploit security weaknesses in networking and operating systems software to aggressively gain entry into computer systems.

Berghel, *supra* n. 8, at [¶¶ 9-10].

18. CAIDA, *supra* n. 16.

19. Berghel, *supra* n. 8, at [¶ 18]; CAIDA, *supra* n. 16.

20. *See* CAIDA, *supra* n. 16.

21. Robert Lemos, *"Code Red" Worm Claims 12,000 Servers* [¶¶ 1-2] (July 18, 2001) <http://news.com.com/2100-1001-270170.html?legacy=cnet> (accessed Oct. 1, 2002).

22. CAIDA, *supra* n. 16.

23. *See* Berghel, *supra* n. 8, at [¶ 19]; CAIDA, *supra* n. 16.

24. Berghel, *supra* n. 8, at [¶ 18]; CAIDA, *supra* n. 16.

25. *See* Berghel, *supra* n. 8, at [¶¶ 1-6].

26. Berghel, *supra* n. 8, at [¶ 28]; CAIDA, *supra* n. 16.

27. Berghel, *supra* n. 8, at [¶ 28]; CAIDA, *supra* n. 16.

computer's owner by replacing the computer's Web page.[28] By focusing on computers in the same network (presumably with the same software and same vulnerabilities), Code Red II propagated more efficiently.[29] However, computers infected with Code Red II broadcast the fact that they had been "back doored" by scanning for additional vulnerable computers.[30] Individuals capable of receiving and identifying Code Red II scans could use that information to break into the Code Red II-infected computers that had scanned them.[31] Malicious system administrators, prepared to identify Code Red II scans, would receive lists of computers that could be taken over with trivial effort.[32] Code Red II-infected computers could then be used to facilitate further attacks on still other computers.[33] Code Red II will greatly damage the state of Internet security for some time to come.

The Code Red worms are notable not only for the costs they generated and the number of computers they infected, but for the debate they provoked.[34] Every party involved sought to lay blame at

28. CAIDA, *supra* n. 16.

29. *See* Berghel, *supra* n. 8, at [¶ 28]; CAIDA, *supra* n. 16.

30. *See* Berghel, *supra* n. 8, at [¶ 20]; CAIDA, *supra* n. 16.

31. *See* Bruce Schneier, *Crypto-Gram Newsletter: Code Red Worm* [¶ 17] (Aug. 15, 2001) <http://www.counterpane.com/crypto-gram-0108.html> (accessed Oct. 1, 2002).

32. *Id*.

33. *Id*.

> Code Red's infection mechanism causes insecure computers to identify themselves to the Internet, and this feature can be profitably exploited. My network is regularly probed by Code Red-infected computers, trying to infect me. I can easily generate a list of those computers and their IP addresses. This is a list of computers vulnerable to the particular IIS exploit that Code Red uses. If I wanted to, I could attack every computer on that list and install whatever Trojan or back door I wanted. I don't have to scan the network; vulnerable computers are continuously coming to me and identifying themselves. How many hackers are piggybacking on Code Red in this manner?

Id.

34. The 1988 Morris Worm achieved a high level of penetration across the Internet, nearly 10 percent of the computers on the Internet at the time (but only around 6,000 computers). *See* e-mail from Mea Culpa to BugTraq, *[ISN] 10th Anniversary of the Internet Worm* [¶¶ 1, 5] (Nov. 4, 1998) <http://lists.jammed.com/ISN/1998/11/0015.html> (accessed Oct. 1, 2002). In terms of damage, the Code Red programs pale in comparison to the ILOVEYOU virus. The ILOVEYOU attacked 14 federal agencies, and the networks of major corporations like Microsoft and Dow Jones and caused losses upward of $10 billion. *See Computer Virus Hit 14 Agencies*, Chi. Trib. C1 (May 10, 2000); Rob Kaiser & Tom McCann, '*Love' Ain't Grand: New E-Mail Bug Wreaks Havoc*, Chi. Trib. N1 (May 5, 2000); Dirk Beveridge, *Filipinos*

another's feet. The eEye firm faulted Microsoft for promoting IIS, an unsafe product, and those network administrators who failed to diligently patch their computers.[35] Richard Smith, the director of the Privacy Foundation, criticized eEye for releasing information about the vulnerability in IIS, arguing that eEye's publications indirectly caused the release of Code Red.[36] Other commentators and journalists joined Smith in condemning eEye's actions.[37] As the furor died down, the moderator of the BugTraq list defended eEye.[38] Code Red, he stated, exploited the IIS vulnerability in a "more sophisticated" fashion than eEye described, so there was no indication that eEye's publication helped Code Red's author.[39] Each of the parties involved, not to mention the clearly guilty author of Code Red and the malicious individuals who took advantage of it, could have done more to prevent some of Code Red's damage. The question of liability for the Code Red worm represents the ethical and legal uncertainty surrounding computer security vulnerabilities and corresponding computer security publications.

The modern world relies on computer security and increasingly finds that it cannot be taken for granted. Computers control much of modern society's infrastructure and computer failure can have

Ambivalent Toward Love Bug Notoriety [¶¶ 1, 2] (May 15, 2000) <http://www.detnews.com/2000/technology/0005/15/technology-55541.htm> (accessed Oct. 1, 2002).

35. Steven Bonisteel, *Code Red Worm Reveals Flaws in Network Stewardship* [¶¶ 13, 20-24, 35-37] (July 31, 2001) (on file with *Whittier Law Review*); Hulme, *supra* n. 3, at [¶¶ 14-16, 18].

36. E-mail from Richard M. Smith, CTO, Privacy Foundation, to BugTraq, *Can We Afford Full Disclosure of Security Holes?* [¶ 13] (Aug. 10, 2001) (on file with *Whittier Law Review*); *see* Hulme, *supra* n. 3, at [¶ 12].

37. *See* Dan Verton, *Security Experts Question Release of Code Red Worm's Exploit Data* (July 20, 2001) <http://www.computerworld.com/securitytopics/security/story/0,10801,62453,00.html> (accessed Oct. 7, 2002); Russ Cooper, *A Call for Responsible Disclosure in Internet Security* (Aug. 13, 2001) <http://www.nwfusion.com/columnists/2001/0813cooper.html> (accessed Oct. 1, 2002); Thomas C. Greene, *Internet Survives Code Red* (July 20, 2001) <http://www.theregister.co.uk/content/4/20546.html> (accessed Oct. 1, 2002); Hulme, *supra* n. 3, at [¶ 12].

38. Elias Levy, *Full Disclosure is a Necessary Evil* [¶¶ 6-8] (Aug. 16, 2001) (on file with *Whittier Law Review*); Steve Steinke, *Code Red: The Rorschach Test*, Network Magazine 16 (Oct. 5, 2001) (available at [¶ 3] <http://www.networkmagazine.com/article/NMG20011003S0007/> (accessed Oct. 1, 2002)).

39. Levy, *supra* n. 38, at [¶ 6].

disastrous consequences.[40] Many computer failures can be ascribed to computer security failures.[41] The rate of reported computer security incidents has risen over 3,000 percent since 1988.[42] There is reason to believe that computer security incidents are massively under reported as well.[43] Even vaunted institutions, like the federal government, discover that their computer security is substandard. The General Accounting Office has found computer security vulnerabilities in the Department of Commerce,[44] the Department of Defense,[45] the

40. "International air traffic control relies on linked computer nets, as do such diverse, and critical functions as telephone operations, emergency response, medical record management, oil distribution, municipal sewage treatment, electrical generation, and railway switching." Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 Colum. J. Transnational L. 885, 866 (1999); *see id*. at 892-93 (citing potential consequences for computer failure including train crashes, power outages, massive traffic jams and extensive water pipe ruptures); Peter G. Neumann, *Computer Related Risks*, 12-93 (ACM Press/Addison Wesley 1995) (discussing computer-related safety risks to communications systems, space systems, defense systems, civil aircraft, trains, ships, robotics, medical systems and electrical power).

41. Neumann, *supra* n. 40, at 96-118, 181-203.

42. *See* Computer Emerg. Response Team, *CERT/CC Statistics 1988-2002* (last updated July 18, 2002) <http://www.cert.org/stats/cert_stats.html> (accessed Oct. 1, 2002) (citing six incidents in 1988; 132 in 1989; 252 in 1990; 406 in 1991; 773 in 1992; 1,334 in 1993; 2,340 in 1994; 2,412 in 1995; 2,573 in 1996; 2,134 in 1997; 3,734 in 1998; 9,859 in 1999; 21,756 in 2000; 52,658 in 2001 and 43,136 incidents in the first two quarters of 2002).

43. Security violations may not be reported because the costs of lost confidence from public reporting outweigh the benefits, or because they are simply not detected. *See* Stevan D. Mitchell & Elizabeth A. Banker, *Private Intrusion Response*, 11 Harv. J.L. & Tech. 699, 704 n. 10 (1998) (assuming that an estimation of one in ten security violations is detected and, of those, one in ten is reported to police); *id*. at 708 n. 16 (noting that "Computer Security Institute [estimates] 17% of detected intrusions are reported" and "[p]revious FBI estimates have been at 11%," while Department of Defense estimates range from 12% to 0.7%). "Reliable statistics remain elusive owing to definitional ambiguities, methodological inconsistencies, and limited reporting. Investigators have conveyed anecdotally their sense that the volume of potentially criminal incidents is increasing." *Id*. at 701 n. 3 (citing Sharon Walsh & Robert O'Harrow Jr., *Trying to Keep a Lock on Company Secrets*, Wash. Post D1 (Feb. 17, 1998) (comments of then-FBI Section Chief William Perez)).

44. U.S. Gen. Acctg. Off., *Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk* 1 (Aug. 13, 2001) (available at <http://www.gao.gov/new.items/d01751.pdf> (accessed Oct. 1, 2002)).

45. U.S. Gen. Acctg. Off., *Information Security: Challenges to Improving DOD's Incident Response Capabilities* 7-9 (Mar. 29, 2001) (available at <http://www.gao.gov/new.items/d01341.pdf> (accessed Oct. 1, 2002)).

Department of the Interior,[46] the Internal Revenue Service,[47] the Environmental Protection Agency,[48] and the Department of Energy.[49] Managing computer security is swiftly becoming as important and as difficult a task as managing the computers themselves.

Computer security publications have a major impact on the state of computer security on the Internet. The proliferation of publications providing information about vulnerabilities and programs that exploit vulnerabilities has enlarged the population of computer users capable of successfully breaching computer security. Scott Charney, the former head of the Department of Justice's Computer Crime and Intellectual Property Section stated, "[t]he advent of automated hacker tools allows many novices to do advanced hacking."[50] Another computer security professional recently estimated that 500 to 1,000 individuals have the knowledge and talent to discover security vulnerabilities, while 5,000 individuals can exploit those discoveries independently.[51] By this expert's estimate, as many as 100,000

46. U.S. Gen. Acctg. Off., *Information Security: Weak Controls Place Interior's Financial and Other Data at Risk* 1 (July 3, 2001) (available at http://www.gao.gov/new.items/d01615.pdf> (accessed Oct. 7, 2002). Most recently, the Department of the Interior's computer system was disconnected from the Internet pursuant to a court order; a special master had found that Interior's security did not effectively protect funds in the Indian Trust system. *Cobell v. Norton*, 2001 WL 1555296 at 45 (D.D.C. Dec. 6, 2001) (reporting on Alan L. Balaran's *Report and Recommendation of the Special Master Regarding the Security of Trust Data at the Department of the Interior* (Nov. 14, 2001) (available at <http://www.indiantrust.com/documents/2001.12.04_BALARAN.pdf> (accessed Oct. 7, 2002)).

47. U.S. Gen. Acctg. Off., *Information Security: IRS Electronic Filing Systems* 2 (Feb. 16, 2001) (available at <http://www.gao.gov/new.items/d01306.pdf> (accessed Oct. 7, 2002)).

48. U.S. Gen. Acctg. Off., *Information Security: Fundamental Weaknesses Place EPA Data and Operations at Risk* 4 (July 6, 2000) (available at <http://www.gao.gov/new.items/ai00215.pdf> (accessed Oct. 7, 2002)).

49. U.S. Gen. Acctg. Off., *Information Security: Vulnerabilities in DOE's Systems for Unclassifed Civilian Research* 2 (June 9, 2000) (available at <http://www.gao.gov/new.items/ai00140.pdf> (accessed Oct. 7, 2002).

50. Wendy R. Leibowitz, *Cracking Cybercrimes*, Natl. L.J. A15 (Feb. 15, 1999); *see* Laura Accinelli, *Hacking Ain't What it Used to Be,* L.A. Times E1 (July 24, 1997) (discussing a "generation gap" between older hackers, who were forced to do research for themselves, and younger hackers, who have a variety of tools available to them).

51. Vernon Loeb, *Back Channels: The Intelligence Community; CIA Document Release Disappoints Scholar*, Wash. Post A23 (Dec. 13, 1999) (quoting Ira Winkler of the Internet Security Advisors Group, updating estimates he made in 1997). In 1997,

individuals use automated hacker tools for attacking computers.[52] As discussed below, computer security publications correlate closely with attacks on computer security.

Given their critical role in the state of Internet security described above, restrictions or regulations on computer security publications could have a dramatic impact in reducing computer crime. Restricting computer security publications might place the tools of computer crime out of the reach of the vast majority of perpetrators. It would follow, therefore, that computer security publications should be a potential subject for regulation. Yet, they are not. Legal commentators have not directly addressed computer security publications. This dearth of legal commentary is surprising, because there is much legal commentary on the assignment of liability optimal to promoting Internet security.[53] Assuming that liability is most efficiently placed on the actor most able to exert control over Internet security, commentators have focused on three parties: computer criminals themselves;[54] the owners and

Winkler estimated that fewer than 200 individuals found computer vulnerabilities, 1,000 could independently exploit those vulnerabilities and 35,000 to 50,000 relied on published, automated attacks. *Id*.

52. *Id*.

53. *See e.g.* Eric J. Bakewell et al., *Computer Crimes*, 38 Am. Crim. L. Rev. 481 (2001); Robin A. Brooks, *Deterring the Spread of Viruses Online: Can Tort Law Tighten the 'Net'?*, 17 Rev. Litig. 343 (1998); Mary M. Calkins, Student Author, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 Geo. L.J. 171 (2000); Scott Charney & Kent Alexander, *Computer Crime*, 45 Emory L.J. 931 (1996); Sarah Faulkner, *Invasion of the Information Snatchers: Creating Liability for Corporations with Vulnerable Computer Networks*, 18 John Marshall J. Computer & Info. L. 1019 (2000); Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. Pa. L. Rev. 1003 (2001); Michael Lee et al., *Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal*, 14 Berkeley Tech. L.J. 839 (1999); Michael Edmund O'Neill, *Old Crimes in New Bottles: Sanctioning Cybercrime*, 9 Geo. Mason L. Rev. 237 (2000); Ethan Preston, *Finding Fences in Cyberspace: Privacy and Open Access on the Internet*, 6 J. Tech. L. & Policy 3 (2001) (available at <http://dogwood.circa.ufl.edu/~techlaw/vol6/Preston.html> (accessed Oct. 7, 2002)); Eric J. Sinrod & William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 Santa Clara Computer & High Tech. L.J. 177 (2000); Michael A. Sussmann, *The Critical Challenges From International High-Tech and Computer-Related Crime at the Millennium*, 9 Duke J. Comp. & Intl. L. 451 (1999); Mitchell & Banker, *supra* n. 43, at 699; Schmitt, *supra* n. 40, at 885.

54. *See e.g.* Calkins, *supra* n. 53; Katyal, *supra* n. 53; O'Neill, *supra* n. 53.

operators of negligently insecure systems that are used to attack others;[55] and software vendors whose products are insecure.[56]

The fundamental problem recognized by legal commentary is that perpetrators of computer crime are not only difficult to identify; they are difficult to apprehend and prosecute or sue. Although computer criminals are obviously in the best position to control or prevent attacks, enforcing regulations against them has proved problematic.[57] Nevertheless, some commentators maintain that perpetrator liability must remain a bedrock strategy of maintaining computer security.[58]

Other commentary focuses on shifting liability to another party that has the capability to prevent computer security breaches or mitigate the harm caused. These comments emphasize the low costs of committing computer crime and encourage strategies of raising its costs.[59] One strategy would assign liability to computer owners whose negligently insecure property serves as an attractive intermediary for computer criminals.[60] Another strategy assigns liability to computer software vendors whose negligently insecure products provide computer criminals opportunities to violate computer security.[61] Both of these strategies place liability on actors with indirect control over Internet security; computer owners can secure their computers and software vendors can secure their products to the indirect benefit of all Internet users.[62] Another innovative proposal is to place liability on Internet service providers that permit their users to attack computer security elsewhere.[63] The efficiency of forcing Internet service providers to exercise control over their users is questionable, however,

55. *See* Faulkner*, supra* n. 53; David L. Gripman, *The Doors Are Locked but the Thieves and Vandals Are Still Getting In: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem*, 16 John Marshall J. Computer & Info. L. 167 (1997).

56. Brooks, *supra* n. 53, at 346; Calkins, *supra* n. 53, at 214 n. 209.

57. *See* Mitchell & Banker, *supra* n. 43, at 704 n. 10, 708 nn. 14-16 (discussing the difficulty in identifying, apprehending and prosecuting computer criminals).

58. *See* Charney & Alexander, *supra* n. 53; Sussmann, *supra* n. 53.

59. *See* Calkins, *supra* n. 53; Katyal, *supra* n. 53; O'Neill, *supra* n. 53.

60. *See* Faulkner, *supra* n. 53; Gripman, *supra* n. 55.

61. *See* Brooks, *supra* n. 53.

62. *See* Katyal, *supra* n. 53 (suggesting, in particular, several innovative strategies for raising the cost of computer crime).

63. *Id*. at 1095-101; Lee, *supra* n. 53, at 874-79.

it would likely be extremely costly and intrude on the privacy of the ISP's users.[64]

The paucity of commentary on computer security publications does not correspond with the potential gains to Internet security of restricting computer security publications. As the opening epigraph states, "the only rational assumption is that once a computer program capable of bypassing . . . an access control system is disseminated [via the Internet], it will be used."[65] By substantially controlling the publication of security vulnerabilities, publishers have a measurable degree of control over and responsibility for their exploitation. If liability is to be placed on the parties that can minimize the costs of computer crime, then computer security publications are logical targets for regulation.

Nevertheless, this article argues that the legal system should extend liability to computer security publishers only with extraordinary caution. This caution springs from the recognition of computer security publications' dual nature. At the same time that public disclosure of vulnerabilities unavoidably facilitates the exploitation of computer security vulnerabilities, the correction and elimination of those same vulnerabilities requires their discovery and disclosure. Computer security publications provide long-term benefits as vulnerabilities are corrected and better products reach the market. Computer owners and operators who are aware of a potential vulnerability can take steps to fix it, while they are powerless to fix an unknown vulnerability.

While this analysis is largely economic, regulation of any form of speech is subject to the First Amendment. As an essential political right, freedom of speech is protected for more than mere economic considerations. Political rights do not hinge on their economic value. Still, the limits of First Amendment protection from liability will likely reflect the balance between a publication's utility for exploitation and its potential for correction of vulnerabilities, as well as, the context of the publication and the intent of the publisher. The debate over computer security publications can be stated in terms of whether a specific rule of liability for publications will generate a net gain or a

64. *See* Katyal, *supra* n. 53, at 1098; Lee, *supra* n. 53, at 877-79 (noting that ISP-based solutions are likely to be undemocratic).

65. *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 331 (S.D.N.Y. 2001).

net loss in security, by permitting more exploitations or more corrections of a vulnerability than would otherwise occur.

In an efficient market for computer security, consumers must receive accurate information about the security associated with various services and products. Unless carefully managed, liability for computer security publications could seriously distort the market for computer security. Litigation could be used to effectively chill computer security publications, and it is unlikely that the parties bringing suit would have the best interests of the market at heart. In particular, the legal system must account for the possibility that software vendors and computer service providers might use litigation to suppress negative information about their products or services and shift liability for security lapses from themselves. The legal system should only extend liability to computer security publishers with an awareness of the vital role computer security publications play in helping the development of security and providing the market with computer security information.

Section II expounds on the role computer security publications, especially disclosures of computer security vulnerabilities, play in the development of security. It describes the life-cycle of vulnerability exploitation and the part computer security publications play in that cycle. Section II also describes the supply of and demand for computer security publications and the economic effect of publishing computer code. Finally, Section II develops criteria for distinguishing between different types of computer security publications.

Section III describes the nature and limits of First Amendment protection for computer security publications and examines the standards of applicable First Amendment jurisprudence. In this context, certain theories of liability merit discussion. Computer security publications are vulnerable to theories of aiding and abetting and conspiracy, as well as, negligence and liability under the Digital Millennium Copyright Act (DMCA).

Finally, Section IV outlines the economic risks of liability-shifting. Powerful institutions with the resources to sustain meritless litigation can suppress even speech putatively protected under the First Amendment. Software vendors and computer service providers have incentives to suppress computer security publications and shift liability

away from themselves.[66] The possibility that software vendors and computer service providers will shift liability for computer security lapses onto computer security publishers, must be recognized as a serious threat to a healthy market for computer security. If computer security publications are suppressed, the long-term consequences for computer security will be deleterious.

II. THEORY OF COMPUTER SECURITY AND INFORMATION ECONOMICS

The first portion of this section provides relevant definitions. The second portion discusses a recent statistical analysis of the relationship between the disclosure of vulnerabilities, related computer security publication and the number of recorded attacks on the vulnerabilities.[67] William A. Arbaugh, William L. Fithen and John McHugh's study, *Windows of Vulnerability*, sets out the life-cycle between discovery, disclosure, exploitation and eventual elimination of computer security vulnerabilities.[68] Naturally, computer security publications have varying degrees of utility for correcting or exploiting vulnerabilities. Publications' explicitness is useful in both correcting and exploiting vulnerabilities, while automating exploitation can only promote exploitation. Arbaugh, Fithen and McHugh's statistical analysis bears this out. The last portion of Section II outlines the arguments that support and oppose full disclosure of vulnerabilities. This is a particularly vibrant and developed debate in the computer security professional community.[69]

A. *DEFINITIONS, TERMS OF ART AND OTHER THROAT-CLEARINGS*

This article employs terms of art, the meanings of which may not be fully apparent outside of the computer security context. Moreover,

66. *See* William A. Arbaugh et al., *Windows of Vulnerability: A Case Study Analysis* 52 (Dec. 2000) <http://www.cs.umd.edu/~waa/pubs/Windows_of_Vulnerability.pdf> (accessed Oct. 2, 2002).

67. *Id*.

68. *Id*. at 53-54.

69. *See* U. of Oulu, Finland Secure Programming Group, *Vulnerability Disclosure Publications and Discussion Tracking* (Aug. 21, 2002) <http://www.ee.oulu.fi/research/ouspg/sage/disclosure-tracking/> (containing many links and other references regarding this debate as maintained by the University of Oulu Secure Programming Group (in Finland)) (accessed Oct. 1, 2002).

the authors have adopted idiosyncratic meanings for other terms used in the article. In particular, legal professionals may be unfamiliar with the precise meaning of some of the words in this article as they are used in the computer security context. It is therefore worthwhile to provide more precise definitions.

At the root of this article's analysis are the concepts of "vulnerability" and "computer security publication." A computer security "vulnerability" refers to:

> [A] weakness that a person can exploit to accomplish something that is not authorized or intended as legitimate use of a network or system. When a vulnerability is exploited to compromise the security of systems or information on those systems, the result is a security incident. Vulnerabilities may be caused by engineering or design errors, or faulty implementation.[70]

As used in this article, the term "computer security publication" refers to any written expression that describes, demonstrates or fixes a vulnerability in any component of a computer system. The article purposely adopts an extremely broad meaning to include a wide array of situations. Computer security publications can come in the form of natural language publications (meaning English or the like), source code or binary code. This article's definition of computer security publication covers advisories from the FBI or vendors, posts to BugTraq, patches, proof-of-concept code which demonstrates vulnerabilities, malicious viruses and anything in between.

Universal City Studios, Inc. v. Reimerdes provided a very cogent definition of the terms "source code" and "binary code":

> Some highly skilled human beings can reduce data and instructions to strings of 1's and 0's and thus program computers to perform complex tasks by inputting commands and data in that form. But it would be inconvenient, inefficient and, for most people, probably impossible to do so. In consequence, computer science has developed programming languages. These languages, like other written languages, employ symbols and syntax to convey meaning. The text of programs written in these languages is referred to as source code. And whether directly or through the medium of another program, the sets of instructions written in

70. Thomas A. Longstaff et al., *Security of the Internet* [¶ 55] (Feb. 1998) <http://www.cert.org/encyc_article/tocencyc.html> (accessed Oct. 1, 2002).

> programming languages—the source code—ultimately are translated into machine "readable" strings of 1's and 0's, known in the computer world as object code, which typically are executable by the computer.[71]

Source code is typically compiled or converted from a text document to object code (also known as binary code). While source code is an efficient form of communication, and binary code is fully functional and can be executed by computers, the court in *Reimerdes* correctly notes that these definitions do not entirely distinguish them from each other.[72] The legal implications of the distinction are addressed in Section III.

Another distinction between types of computer code is particularly important to this article: exploits and patches. An exploit is a code that exploits a vulnerability and compromises a computer system's security.[73] Often, exploits yield an unauthorized degree of access of a computer system. A patch is code that eliminates or corrects a vulnerability.[74] For the purposes of this article, computer security publications may include patches or exploits.

B. *THE LIFE-CYCLE OF A VULNERABILITY*

Windows of Vulnerability is a statistical study examining the relationship between computer security publications and computer security violations.[75] First, the article sets up the six phases of the life-cycle of a vulnerability.[76] The birth phase describes the creation and incorporation of the vulnerability in a software product that is publicly

71. 111 F. Supp. 2d 294, 306 (S.D.N.Y. 2000).

72. *Id*. (stating that the distinction is further blurred by scripting or interpreted languages, such as Perl, where the source code is executed by an interpreter).

73. *See* searchSecurity.com, *Exploit-a searchSecurity Definitions* (May 20, 2001) <http://searchsecurity.techtarget.com/sdefinition/0,,sid14_gci553536,00.html> (accessed Oct. 4, 2002).

74. *See* Whatis.com, *Patch-a Whatis Definition* (July 31, 2001) <http://whatis.techtarget.com/defnition/0,289893,sid9_gci212753,00.html> (accessed Oct. 4, 2002).

75. *See* Arbaugh, *supra* n. 66, at 52, 55.

76. *Id*. at 53-55; *see* Bruce Schneier, *Crypto-Gram Newsletter: Full Disclosure and the Window of Exposure* [¶¶ 3-5] (Sept. 15, 2000) <http://www.counterpane.com/crypto-gram-0009.html> (accessed Oct. 1, 2002) (describing a very similar description of the life-cycle of vulnerabilities).

deployed.[77] The discovery phase is straightforward; the vulnerability is found and public (or semi-public) disclosure of information about the vulnerability is made.[78] *Windows of Vulnerability* suggested that disclosure is limited to, at most, special interest publications.[79] The correction phase begins when someone issues a patch to correct the vulnerability.[80] The ability of issuing a patch is restricted to the software vendor or developer.[81] The industry practice of commercial software vendors is to retain the source code of the software, while publishing only binary code.[82] The investment in research for creating an effective patch to many (if not most) vulnerabilities without the source code is prohibitive.[83] In the publicity phase, the vulnerability is widely publicized on a "large scale once the disclosure is out of control."[84] The definition of computer security publication laid forth in this article encompasses both disclosure and publication. One of the most important phases is scripting; someone creates an exploit that is simple to use and does not require an understanding of the underlying principles of the exploitation of the vulnerability.[85] This is an imprecise and relative definition: "this phase applies to any simplification of intrusion techniques that exploit the vulnerability, such as cracker 'cookbooks' or detailed descriptions on how to exploit the vulnerability."[86] The crucial factor is that the scripting or automation lowers the skill level and background knowledge required to exploit the vulnerability, while "dramatically increas[ing] the size of the population that can exploit systems with that vulnerability."[87] The article's definition of computer security publications also covers scripting or automation. Finally, vulnerabilities enter a death phase,

77. *See* Arbaugh, *supra* n. 66, at 53.
78. *See id*.
79. *Id*.
80. *Id*. at 54.
81. *Id*.
82. *See e.g.* OpenBSD Projects, *Binary Patches for OpenBSD* [¶¶ 2-3] (Aug. 20, 2002) <http://www.openbsd.org.mx/~santana/binpatch.html> (accessed Oct. 4, 2002)
83. *Id*.
84. Arbaugh, *supra* n. 66, at 54.
85. *See id*.
86. *Id*.
87. *Id*.

where the number of systems that retain that vulnerability "shrinks to insignificance."[88]

Attrition of vulnerabilities comes from two sources. System administrators apply patches and retire the vulnerable software product.[89] On the other hand, vulnerabilities lose significance because computer security violators lose interest in exploiting that particular vulnerability.[90] Birth, discovery and disclosure must always occur in sequence because they are causally related.[91] However, disclosure can trigger publication, automated exploitation of the vulnerability and correction.[92] The death of a vulnerability depends greatly on how widespread the vulnerability is, how quickly it is fixed, how widely its existence is publicized and how widely it is exploited.[93] These factors have some interrelation that may extend or shorten the life of a vulnerability.

C. *THE ECONOMICS OF INFORMATION: COMPUTER SECURITY PUBLICATIONS AND WINDOWS OF VULNERABILITY*

Windows of Vulnerability addressed a "great debate" between those who would restrict computer security publications and disclosure of vulnerability and those who advocate the most widespread disclosure of vulnerability discoveries possible.[94] The implications of this article's epigraph are central to that debate; publication of code that circumvents any kind of computer security on the Internet will result in people circumventing that security.[95] The remaining question is whether a particular regulation of computer security publications generates a net gain or a net loss in computer security. This subsection offers criteria which distinguish between publications' utility for licit and illicit purposes. These criteria are important because a publication's utility for illicit purposes will likely correlate with its hostile reception in the legal system.

88. *Id*.
89. *Id.* at 54-55.
90. *Id*.
91. *Id.* at 55.
92. *Id.* at 52, 55.
93. *Id.*at 56, 57.
94. *Id*. at 57.
95. *University City Studios, Inc. v. Corely*, 273 F.3d 429, 451-52 (2d Cir. 2001).

1. *Full-Disclosure and Limited-Disclosure*

Some computer security professionals have adopted a posture of full-disclosure towards computer security vulnerabilities.[96] The philosophy behind full-disclosure posits that the maximum disclosure of details regarding discovered vulnerabilities provides the best environment for security over the long-term.[97] The primary force behind full-disclosure has been frustration with the responsiveness of vendors in issuing patches.[98] Before the development of full-disclosure, publication of vulnerabilities would be suppressed until vendors issued a patch.[99] Computer security professionals' frustration grew with the perception that vendors were dilatory in developing patches without any pressure of vulnerabilities' public disclosure.[100] The publicity generated by full-disclosure prompts vendors to create patches faster and system administrators to install patches faster.[101]

96. Brian Bergstein, *Microsoft: Shhhhh!*, Chattanooga Times/Chattanooga Free Press C1 (Nov. 17, 2001).

97. Bruce Schneier, *Crypto-Gram Newsletter: Full Disclosure* [¶ 9-13] (Nov. 15, 2001) <http://www.counterpane.com/crypto-gram-0111.html> (accessed Oct. 4, 2002); Hulme, *supra* n. 3; Bergstein, *supra* n. 96.

98. Schneier, *supra* n. 97, at [¶ 11].

99. *Id*. at [¶ 9].

100. *Id.* at [¶ 10];

> During the early years of computers and networks, bug secrecy was the norm. When users and researchers found vulnerabilities in a software product, they would quietly alert the vendor. In theory, the vendor would then fix the vulnerability. After CERT was founded in 1988, it became a clearinghouse for vulnerabilities. People would send newly discovered vulnerabilities to CERT. CERT would then verify them, alert the vendors, and publish the details (and the fix) once the fix was available.
>
> The problem with this system is that the vendors didn't have any motivation to fix vulnerabilities. CERT wouldn't publish until there was a fix, so there was no urgency. It was easier to keep the vulnerabilities secret. There were incidents of vendors threatening researchers if they made their findings public, and smear campaigns against researchers who announced the existence of vulnerabilities (even if they omitted details). And so many vulnerabilities remained unfixed for years.
>
> The full disclosure movement was born out of frustration with this process.

Id. at [¶¶ at 9-11].

101. Schneier, *supra* n. 5, at 339-40;

> Since a window [of vulnerability] remains open until the vendor patches the vulnerability and the network administrator installs the patches, the faster the vendor can issue the patch the faster the window starts closing. To spur vendors to patch faster, full-disclosure proponents publish vulnerabilities far and wide. Ideally, the vendor will distribute the patch before any automatic

The full-disclosure movement has developed sophisticated policies and procedures regarding giving notice to the vendor before public disclosure.[102]

Conversely, limited-disclosure proponents argue security vulnerabilities cannot be avoided and their discovery and disclosure should be managed.[103] Scott Culp, manager of the Microsoft Security Response Center, described full-disclosure as "information anarchy."[104] Limited-disclosure proponents argue that unrestricted computer security publication promotes the development and use of exploits faster than it promotes the development and installation of patches.[105] In the eyes of limited-disclosure proponents, exploit publishers "incite and encourage cybercrime," even though their "hands are clean because they, themselves, never actually" commit computer crime.[106] In particular, limited-disclosure proponents argue that full-disclosure greatly increases the population capable of computer crime.[107] Limited-disclosure proponents argue that full-disclosure does not actually *force* vendors to issue patches or administrators to install patches.[108] Because neither vendors or users

attack tools are written. But writing such tools can only hasten the patches. Schneier, *supra* n. 76, at [¶ 10].

102. Even within the full-disclosure movement, there is great variation. CERT, for instance, does not release exploits, while the RFPolicy and @stake's policy have no such stricture. *See* Rain Forest Puppy, *Full Disclosure Policy (RFPolicy) v2.0* [¶ 10 (A)-(G)] (Oct. 17, 2000) <http://www.wiretrip.net/rfp/policy.html> (accessed Oct. 4, 2002); Computer Emerg. Response Team, *The CERT/CC Vulnerability Disclosure Policy* [¶¶ 1-5] (Oct. 2000) <http://www.kb.cert.org/vuls/html/disclosure.html> (accessed Oct. 4, 2002); @stake Research Labs, *@stake Security Vulnerability Reporting Policy* (last updated June 5, 2002) <http://www.atstake.com/research/policy/index.html> (accessed Oct. 4, 2002).

103. Scott Culp, *It's Time to End Information Anarchy* [¶ 4] (Oct. 2001) <http://www.microsoft.com/technet/columns/security/essays/noarch.asp> (accessed Oct. 4, 2002).

104. *Id.*

105. *Id*. at [¶¶ 5-9].

106. Marcus J. Ranum, *Have A Cocktail: Computer Security Today* n. 2 (2000) <http://www.ranum.com/usenix/ranum-elx-cocktail.pdf> (accessed Oct. 4, 2002).

107. *See id*. at [¶¶ 8-9]; Culp, *supra* n. 103, at [¶ 15] ("[T]he state of affairs today allows even relative novices to build highly destructive malware. It's simply indefensible for the security community to continue arming cybercriminals. We can at least raise the bar."). Malware is techno-jargon for malicious software. Berghel, *supra* n. 8, at [¶ 7].

108. Culp, *supra* n. 103, at [¶¶ 6-8].

can be instantly responsive to computer security publications, full-disclosure merely makes users vulnerable.[109] Limited-disclosure proponents posit that arguing that users and vendors should be more responsive essentially blames the victim.[110] Culp argued that ethical culpability lies with computer security publishers that enable attacks rather than the vendors of insecure products and users who fail to diligently apply patches.

> [R]egardless of . . . the form of a patch . . . , an administrator doesn't need to know how a vulnerability works in order to understand how to protect against it, any more than a person needs to know how to cause a headache in order to take an aspirin.
>
> *Likewise, if information anarchy is intended to spur users into defending their systems, the worms themselves conclusively show that it fails to do this.* Long before the worms were built, vendors had delivered security patches that eliminated the vulnerabilities. . . . Yet when these worms tore through the user community, it was clear that few people had applied these fixes. . . .
>
> *[I]f the current methods for protecting systems are ineffective, it makes it doubly important that we handle potentially destructive information with care*. . . .
>
> *At the end of the day, a vendor's paramount responsibility is to its customers, not to a self-described security community. If openly addressing vulnerabilities inevitably leads to those vulnerabilities being exploited, vendors will have no choice but to find other ways to protect their customers*.[111]

To full-disclosure advocates, the implications of Culp's piece essentially threaten to respond to uncontrolled disclosure practices with more secrecy. A full-disclosure deconstruction might condense Culp's position to arguing that vendors obligations are foremost to their customers, rather than to self-selected security publishers. Culp reasons that it is better suppress security issues and weaken demand for

109. *See* Marcus J. Ranum, *The Network Police Blotter* [¶ 6] (Oct. 2000) <http://ranum.com/usenix/ranum_5_temp.pdf> (accessed Oct. 4, 2002); Culp, *supra* n. 103, at [¶¶ 7-8].

110. Ranum, *supra* n. 109, at [¶¶ 13-14].

111. Culp, *supra* n. 103, at [¶¶ 7-10] (emphasis added by author).

security than to increase the demand for security by calling attention to security issues.[112]

However, limited-disclosure proponents may effectively accuse many full-disclosure proponents of conflicts of interest. Some of those who advocate full-disclosure may also seek to maliciously attack computer security.[113] Computer security publishers whose actions degrade the state of security may also sell security solutions. The consequent purchase of those solutions perpetuates insecurity by rewarding a business model that propagates computer insecurity. At their worst, full disclosure practices can degenerate into self-promotion and extortion.[114]

2. *The Demand for Computer Security Publications and the Window of Vulnerability*

A maxim of the full-disclosure philosophy is that there is no security through obscurity. Security through obscurity means that the security of the system depends on the secrecy of the system's details. By restricting computer security publications, this strategy seeks to raise the costs of computer crime.[115] This strategy is controversial. Full-disclosure proponents believe that the discovery (and consequent elimination) of vulnerabilities creates better security than relying on the obscurity of vulnerabilities to prevent their discovery at all.[116] Full-disclosure proponents are skeptical of the assumption that, if

112. Culp, *supra* n. 103, at [¶¶11-13].

113. *See* Ranum, *supra* n. 109, at [¶ 9].

114. *See* Hulme, *supra* n. 3; *see e.g.* U.S. Dept. of J., *Three Kazak Men Arrested in London for Hacking into Bloomberg L.P.'s Computer System* [¶ 4] (Aug. 14, 2000) <http://www.usdoj.gov:80/criminal/cybercrime/bloomberg.htm> [hereinafter U.S. Dept. of J., *Three Kazak Men*] (accessed Oct. 4, 2002) (After breaking into Bloomberg's computer system, one of a number of computer criminals demanded "Bloomberg pay him $200,000 in exchange for providing information to Bloomberg concerning how [he] was able to infiltrate Bloomberg's computer system."); U.S. Dept. of J., *Russian Computer Hacker Indicted in California for Breaking into Computer Systems and Extorting Victim Companies* [¶ 1] (June 20, 2001) <http://www.usdoj.gov:80/criminal/cybercrime/ivanovIndict2.htm> [hereinafter U.S. Dept. of J., *Russian Computer Hacker*] (accessed Oct. 4, 2002) (Having gained illegal computer access and stolen financial files, a Russian computer criminal "attempt[ed] to extort payments from the victim companies for 'computer security services.' ").

115. Schneier, *supra* n. 97, at [¶ 16].

116. Bruce Perens, *Why Security-Through-Obscurity Won't Work* [¶ 5] (1998) <http://slashdot.org/article.pl?sid=980720/0819202> (accessed Oct. 4, 2002).

information about vulnerabilities is suppressed, no independent discovery or exploitation of the vulnerability will occur.[117] Even limitations on disclosure cannot ensure that vulnerability information will be used beneficially, in part because it is impossible to predict how the information will be used.[118] History underscores this point. One computer security group issued an advisory to the BugTraq mailing list, announcing that it had developed and deliberately withheld an exploit of an undiscovered vulnerability, but it had spread outside of the group's limited distribution and into malicious hands.[119] Six days later, someone posted a copy of the exploit's source code to BugTraq (despite copyright notices in the source code forbidding precisely that action).[120] After public arguments, controversy and the threat of a lawsuit, the exploit was removed from the BugTraq archives.[121]

If there is no security through obscurity, it is because exploit users value obscurity more than software users and vendors.[122] There is a market for computer security publications. Software users and vendors have an incentive to learn about vulnerabilities, exploits and

117. *See id*.; Schneier, *supra* n. 97, at [¶¶ 14, 30, 31].

118. Levy, *supra* n. 38, at [¶ 14] (Aug. 16, 2001);

> One proposed alternative to full disclosure that's been bandied about is to create a closed group of product vendors, security companies, and security experts through which full details of the vulnerabilities can be reported and shared, while the public only gets to learn of the vulnerability's existence.
>
> This is not very different from the old days . . .
>
> Any group of the size being proposed is bound to have leaks. . . . You don't need to look very far into the past for examples of vulnerabilities and exploits leaking to the underground, even when smaller groups are involved. . . . The larger the group the worse the problem becomes.
>
> Along these lines, we start to wonder who would be allowed to join such [a] group. . . . CERT's Internet Security Alliance makes it easy: for $2,500 a year any black hat [malicious attacker] with a business name, P.O. box, and a web site can get advance notice of vulnerabilities before most of the general public—at least in theory. Fortunately, most . . . vulnerabilities become public through open sources and are available to everyone at the same time.

Id. at [¶¶ 10-13].

119. Nevauene, *Exploits, Copyright and Disclosure (Internet)* [¶ 1] (Aug. 24, 2001) <http://kuro5hin.org/story/2001/8/24/16545/1193> (accessed Oct. 4, 2002); e-mail from Sebastian to BugTraq, *Multiple Vendor Telnet Daemon Vulnerability* (July 18, 2001) <http://online.securityfocus.com/archive/1/197804> (accessed Oct. 4, 2002); Brian McWilliams, *Stolen Program Cracks BSD Servers, Group Says* Newsbytes [¶ 5] (July 24, 2001) (available in LEXIS, All News library).

120. Nevauene, *supra* n. 119, at [¶¶ 6-7].

121. *Id*. at [¶ 8].

122. *See* Culp, *supra* n. 103, at [¶¶ 6, 11].

patches before attackers.[123] Prepared, they can lower computer crime costs by preventing attacks.[124] Conversely, attackers have an incentive to learn about vulnerabilities and exploits before anyone else.[125] This race (in which both sides seek to use the information before the other side does) lengthens the window of vulnerability and preserves opportunities to exploit vulnerable targets.[126] One CERT paper has noted that computer criminals have responded to shrinking windows of vulnerability by limiting disclosure and innovating.[127] This, in turn, has reduced users' opportunity to protect themselves.[128] The illicit market for computer security publications appears resistant to the threat of liability.[129] Liability for computer security publications, then,

123. Culp, *supra* n. 102, at [¶ 11].

124. *See* Schneier, *supra* n. 76, at [¶ 10].

125. *See e.g.* U.S. Dept. of J., *Three Kazak Men*, *supra* n. 113; U.S. Dept. of J., *Russian Computer Hacker*, *supra* n. 114.

126. *See* Bergstein, *supra* n. 96; Schneier, *supra* n. 97, at [¶¶ 3-8].

127. *See* Kevin J. Houle & George M. Weaver, *Trends in Denial of Service Attack Technology* 14-15 (Oct. 2001) <http://www.cert.org/archive/pdf/DoS_trends.pdf> (accessed Oct. 4, 2002).

128. *Id*.

129. *See e.g.* Humpin.org, *You Have One Bat and There Are 100 Million Holes* (Nov. 14, 2001) <http://www.humpin.org/decss/> (accessed Oct. 4, 2002) (A computer progam named DeCSS might be a paradigmatic case. As explained in Section III.C.1, *infra*, possession, use and distribution of DeCSS is punishable both civilly and criminally. Nevertheless, the program's utility (and its users' resentment towards legal process that would restrict its availability) has virtually guaranteed its availability. The *Reimerdes* court, which enjoined the publication of DeCSS, commented on the difficulty of effectively inhibiting access to DeCSS (listing over 126 URLs that apparently link to the DeCSS source code).);

> [A] disease metaphor is helpful here. The book infringement hypothetical is analogous to a common source outbreak epidemic. Shut down the printing press (the poisoned well) and one ends the infringement (the disease outbreak). The spread of means of circumventing access to copyrighted works in digital form, however, is analogous to a propagated outbreak epidemic. Finding the original source of infection (e.g., the author of DeCSS or the first person to misuse it) accomplishes nothing, as the disease (infringement made possible by DeCSS and the resulting availability of decrypted DVDs) may continue to spread from one person who gains access to the circumvention program or decrypted DVD to another. And each is "infected," i.e., each is as capable of making perfect copies of the digital file containing the copyrighted work as the author of the program or the first person to use it for improper purposes. The disease metaphor breaks down principally at the final point. Individuals infected with a real disease become sick, usually are driven by obvious self-interest to seek medical attention, and are cured of the disease if medical science is capable of doing so. Individuals

affects legitimate users and vendors differently than computer criminals. While the threat of liability might restrict computer security publications to legitimate, otherwise law-abiding users and vendors, the scarcity of a publication actually increases its value to computer criminals.

3. *Explicit Detail and Automation*

Computer security publications may facilitate both circumvention and defense of computer security, but publications are not an indistinguishable mass in terms of their effects on security. Two factors which make publications significantly more likely to cause more exploitations than patching, are explicit detail and automation. [130]

Explicit details are useful to both the creation of patches and exploits. As a computer language description of the vulnerability, source code appears to be the epitome of explicit detail. The source code of an exploit, for instance, need only be compiled to be a tool for an attacker, but also gives the creator of a patch a very precise description of the vulnerability to be eliminated.[131] The reverse is true as well. The source code for a patch need only be compiled to be used by a security defender, while it provides attackers a precise description of the vulnerability to be exploited.[132] Binary exploit code, on the other hand, is largely, but not wholly, indeciferable to humans.[133] As such, it is already a tool for the attacker, but not very useful to someone attempting to understand (and correct) the exploited vulnerability. Binary exploit code still permits a researcher to verify the existence of a vulnerability and the efficacy of a patch.[134] Although explicit detail does not ensure that an individual publication will cause more

> infected with the "disease" of capability of circumventing measures controlling access to copyrighted works in digital form, however, do not suffer from having that ability. They cannot be relied upon to identify themselves to those seeking to control the "disease." And their self-interest will motivate some to misuse the capability, a misuse that, in practical terms, often will be untraceable.

Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 332 (S.D.N.Y. 2000).

130. *See* Culp, *supra* n. 103, at [¶¶ 4-5]; Arbaugh, *supra* n. 66, at 57-58.

131. *See* Schneier, *supra* n. 97, at [¶¶ 26-27].

132. *See* Schneier, *supra* n. 5, at 340.

133. *See Reimerdes,* 111 F. Supp. 2d at 306, 326.

134. Culp, *supra* n. 103, at [¶ 12].

exploitations than patches, it is a prerequisite. The beneficial long-term effects of explicit computer security publications are discussed later.

On the other hand, automation has been definitively linked with widespread exploitation of security.[135] The most salient finding of *Windows of Vulnerability* was the correlation of widespread vulnerability exploitation with the automation of exploitation, not with the initial disclosure. Although *Windows of Vulnerability* acknowledged certain problems with its data set, it nonetheless presents the best picture of the causal relationship between different kinds of computer security publications and computer security violations.[136] *Windows of Vulnerability* analyzed three different vulnerabilities: a common gateway program called phf that permitted the arbitrary execution of commands; a buffer overflow vulnerability in Internet messaging access protocol (IMAP) servers; and a buffer overflow vulnerability in Berkeley Internet Name Domain (BIND) servers.[137]

After correlating the disclosure of the vulnerability, the automation of the exploit, and the number of security incidents where a particular vulnerability was exploited, Arbaugh, Fithen and McHugh concluded that "automating a vulnerability, not just disclosing it, serves as the catalyst for widespread intrusions."[138] Arbaugh, Fithen and McHugh's final conclusion was that most intrusions occur where a patch has been issued but not supplied; "[m]any systems remain vulnerable to security flaws months or even years after corrections become available. . . . [W]e uncovered overwhelming evidence that a significant problem exists in the deployment of corrections to security problems."[139]

Explicitness and automation are factors central to this article's analysis of computer security publications' exposure to liability. Liability for computer security publications is significant because of the possibility that vendors and system administrators will attempt to shift responsibility for poor implementation of security to computer security publishers.

135. Arbaugh, *supra* n. 66, at 57.
136. *Id*. at 57-58.
137. *Id*. at 55-57.
138. *Id.* at 57.
139. *Id.* at 58.

III. LIMITS OF FIRST AMENDMENT PROTECTION FOR COMPUTER SECURITY PUBLICATIONS

Some computer security publishers will be liable for their publications.[140] The First Amendment offers substantial, but not unlimited, protection against civil and criminal liability.[141] Therefore, any regulation of speech must survive First Amendment scrutiny. This section attempts to delineate both the standards of scrutiny applicable to computer security publications and the most applicable theories of liability.

The First Amendment protection for computer security publications is uncertain for a number of reasons. The term "computer security publication," as defined in this article, encompasses a spectrum of speech, ranging from wholly expressive to almost totally functional. It is therefore uncertain that all computer codes will receive First Amendment protection. Even the presence of First Amendment protection does not guarantee immunity from liability for computer security publications. Regulation of different aspects of computer security publications will receive different levels of First Amendment scrutiny. The First Amendment offers only limited protection for illegal or tortious conduct, whether or not it is expressive. The speech aspects of computer security publications will not protect those publications that otherwise violate the law.

A. *COMPUTER SECURITY PUBLICATIONS AS SPEECH*

This section focuses legal analysis on source and object code publications, rather than English language publications, because of computer code's functionality. This same functionality increasingly narrows the number of humans who comprehend the computer code in question.[142] This feature of computer code has occasionally called into

140. *See Universal City Studios, Inc. v. Reimerdes*, 82 F. Supp. 2d 211, 221 (S.D.N.Y. 2000).

141. *See Giboney v. Empire Storage & Ice Co.*, 336 U.S. 490, 502 (1949).

142. *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 326 (S.D.N.Y. 2000);

> The path from idea to human language to source code to object code is a continuum. As one moves from one to the other, the levels of precision and, arguably, abstraction increase, as does the level of training necessary to discern the idea from the expression. Not everyone can understand each of these forms. Only English speakers will understand English formulations. Principally those familiar with the particular programming language will

question whether computer code is speech at all. Nevertheless, the doubt over computer code's nature as speech should not be overestimated. First Amendment protection for code is a relatively well-settled matter of law.

The first cases to address whether code is speech dealt with encryption code.[143] Until the end of the Clinton administration, encryption products were heavily regulated by the Bureau of Export Administration.[144] These cases are largely moot: export regulations do not now implicate posting source code for consumer encryption products on the Internet.[145] The first of these cases, *Karn v. United States Deptartment of State*, explicitly limited its First Amendment analysis of encryption regulation to source code embedded with human-readable commentary.[146] In *Karn*, the plaintiff's argument is that "source code and comments taken together teach humans how to speak in code."[147] *Karn* reserved judgment as to whether pure source code, which was described as "merely a means of commanding a computer to perform a function," constituted speech.[148] In *Junger v. Daley*, the lower court found that the First Amendment only protected source code's expressive aspects, but not its functional aspects.[149] Ultimately, the lower court denied First Amendment protection to source code because it was not sufficiently expressive; its meaning was neither "unmistakable" nor "overwhelmingly apparent" to qualify for First Amendment protection against export regulation.[150] On review of

> understand the source code expression. And only a relatively small number of skilled programmers and computer scientists will understand the machine readable object code. But each form expresses the same idea, albeit in different ways.

Id.

143. *See Junger v. Daley*, 209 F.3d 481 (6th Cir. 2000); *Karn v. U.S. Dept. of St.*, 925 F. Supp. 1 (D.D.C. 1996).

144. 15 C.F.R. § 740.13 (2002).

145. *Id*. (citing that the Bureau of Export Administration (BXA) has promulgated new regulations to relax U.S. encryption export policies); *Junger*, 209 F.3d at 483-84; *Karn*, 925 F. Supp. at 3.

146. 925 F. Supp. at 10 n.19.

147. *Id*. at 9.

148. *Id*. at 10 n. 19.

149. 8 F. Supp. 2d 708, 716 (N.D. Ohio 1998) (citing *Va. St. Bd. of Pharm. v. Va. Citizens Consumer Counsel*, 425 U.S. 748, 762 (1976); *Roth v. U.S.*, 354 U.S. 476, 484 (1957)).

150. *Id*. at 717-18 (quoting, respectively, *Tinker v. Des Moines Indep. Community School Dist.*, 393 U.S. 503 (1969); *Tex. v. Johnson*, 491 U.S. 397, 406 (1989)).

Junger v. Daley, the court rejected this argument, finding that source code was a means of communication between programmers.[151] The final case addressing encryption, *Bernstein v. United States Department of Justice*, had found source code sufficiently expressive to qualify for First Amendment protection, but that opinion has since been withdrawn and is under *en banc* review.[152] Again, regulation changes have apparently mooted this issue.[153]

The next set of cases that address whether computer code is speech, dealt with the distribution of binary code which permitted DVDs to be decrypted and played on any platform. This controversy has refined the jurisprudence addressing First Amendment protection of computer code. The first set of cases deal with the legality of this binary code under the DMCA, which prohibits the circumvention of technical measures that protect copyrighted works.[154] *Universal City Studios, Inc. v. Corley* rejected the argument that the incomprehensibility of source code (and even binary code) circumscribed its First Amendment protection.[155] *Universal City*

151. 209 F.3d 481, 484 (6th Cir. 2000);

> The Supreme Court has expressed the versatile scope of the First Amendment by labeling as "unquestionably shielded" the artwork of Jackson Pollack, the music of Arnold Schoenberg, or the Jabberwocky verse of Lewis Carroll. . . . Particularly, a musical score cannot be read by the majority of the public but can be used as a means of communication among musicians. Likewise, computer source code, though unintelligible to many, is the preferred method of communication among computer programmers.

Id.

152. 176 F.3d 1132, 1141 (9th Cir. 1999), *withdrawn,* 192 F.3d 1308 (9th Cir. 1999).

153. *See* Cryptome.org, *BXA Advisory on Bernstein Inquiry on Encryption Export Regulations* [¶ 4] (Feb. 17, 2000) <http://cryptome.org/bxa-bernstein.htm> (accessed Sept. 30, 2002) (citing that new regulations have changed the BXA's stance on Bernstein's actions. An archived copy of a letter from the BXA, responding to questions about the effects of the new regulations from Bernstein's counsel, stated that concerns that export regulations might continue to interfere with Bernstein's activity were unfounded).

154. 17 U.S.C. §§ 1201-1204 (2000).

155. 273 F.3d 429, 446 (2d Cir. 2001);

> The "object code" version would be incomprehensible to readers outside the programming community (and tedious to read even for most within the community), but it would be no more incomprehensible than a work written in Sanskrit for those unversed in that language. The undisputed evidence reveals that even pure object code can be, and often is, read and understood by experienced programmers. And source code (in any of its various levels of complexity) can be read by many more. . . . Ultimately, however, the ease with which a work is comprehended is irrelevant to the constitutional inquiry.

Studios, Inc. v. Reimerdes expressly extended First Amendment protection to computer code,[156] and was recently reviewed by *Corley*.[157] *Corley* wholly upheld *Reimerdes*' extension of First Amendment protection to computer code:

> Communication does not lose constitutional protection as "speech" simply because it is expressed in the language of computer code. Mathematical formulae and musical scores are written in "code," *i.e.*, symbolic notations not comprehensible to the uninitiated, and yet both are covered by the First Amendment. . . .
>
> Limiting First Amendment protection of programmers to descriptions of computer code (but not the code itself) would impede discourse among computer scholars, just as limiting protection for musicians to descriptions of musical scores (but not sequences of notes) would impede their exchange of ideas and expression. Instructions that communicate information comprehensible to a human qualify as speech whether the instructions are designed for execution by a computer or a human (or both).[158]

In contrast, *DVD Copy Control Association v. Bunner* distinguished between source code and binary code.[159] *Bunner* dealt with trade secret litigation arising from the same disclosure of code. *Bunner* held that source code was sufficiently expressive to merit First Amendment protection, but stated that when source code was compiled to binary code, "the resulting composition of zeroes and ones would not convey ideas" and would therefore fall outside of First Amendment protection.[160]

Id.

156. 111 F. Supp. 2d 294, 326-27 (S.D.N.Y. 2000) (citing *Hurley v. Irish-Am. Gay, Lesbian & Bisexual Group of Boston*, 515 U.S. 557, 569 (1995) (stating that "[i]t cannot seriously be argued that any form of computer code may be regulated without reference to First Amendment doctrine. . . . All modes by which ideas may be expressed or, perhaps, emotions evoked—including speech, books, movies, art, and music—are within the area of First Amendment concern").

157. 273 F.3d at 434.

158. *Id*. at 445, 448.

159. 113 Cal. Rptr. 2d 338, 347-48 (Cal. App. 2001), *review granted,* 2002 Cal. LEXIS 614 (Feb. 20, 2002) (Review granted without published opinion.).

160. *Id*. at 348 (citing that *Junger v. Daley*, 209 F.3d 481, 482-83 (6th Cir. 2000)

Finally, *United States v. Elcom, Ltd.* dealt with the criminal prosecution of a Russian company that distributed the Advanced eBook Processor (AEBPR).[161] AEBPR permitted its users to circumvent the copyright control technology in Adobe Acrobat eBook Reader, an application that could view books in an electronic format.[162] Elcom was prosecuted under criminal provisions of the DMCA.[163] *Elcom* found that, since computer code was expressive enough to be protected by copyright code, it was expressive enough for First Amendment protection.[164] *Elcom* additionally recognized the controversy over object code's status as speech, but stated that "the better reasoned approach is that it is protected. . . . Object code is merely one additional translation of speech into a new, and different, language."[165]

The incomprehensibility of binary code (and even source code) has occasionally prompted courts to hold that code is not speech at all.[166] This view has found support in academic literature, arguing that binary code "is best treated as a virtual machine."[167] "Executable computer code of the type at issue does little to further traditional First Amendment interests" because so few understand it.[168] Given the relative obscurity of binary code as compared to source code, binary code computer security publications run a greater risk of regulation than source code publications. Nevertheless, the dominant view is that both source code and binary code are speech.[169]

---

does not explicitly state that binary code is incomprehensible, although it is contrasted with source code and its relative comprehensibility by programmers).

161. *U.S. v. Elcom, Ltd.*, 203 F. Supp. 2d 1111 (N.D. Cal. 2002); U.S. Dept. of J., *Russian National Enters into Agreement with United States on First Digital Millennium Copyright Act Case* (Dec. 13, 2001) <http://cybercrime.gov/sklyarov Agree.htm> (accessed Sept. 30, 2002).

162. *Elcom*, 203 F. Supp. 2d at 1117.

163. *Id.* at 1119.

164. *Id*. at 1126.

165. *Id*. (quoting *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 326-27 (S.D.N.Y. 2000)).

166. *See* Mark A. Lemley & Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 Duke L.J. 147, 236 (1998).

167. *Id*.

168. *Universal City Studios, Inc. v. Reimerdes*, 82 F. Supp. 2d 211, 222 (S.D.N.Y. 2000) (imposing a temporary restraining order against the distribution of DeCSS).

169. *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 449-50 (2d Cir. 2001); *Junger v. Daley*, 209 F.3d 481, 485 (6th Cir. 2000); *Reimerdes*, 82 F. Supp. 2d at 219.

B. *STANDARDS OF SCRUTINY FOR COMPUTER SECURITY PUBLICATIONS*

Despite the fact that computer security publications (including computer code) are speech, they may still be regulated.[170] This subsection explores two distinct branches of jurisprudence on First Amendment scrutiny. The first branch applies to computer security publications' expressive content. The First Amendment does not protect any speech when it functions as part of an otherwise criminal act.[171] The second branch of jurisprudence arose to specifically address computer code. It recognizes that computer code has an inherent functionality which natural language does not. This functionality may be regulated more easily than natural language computer security publications.

1. *Speech Acts And Foreseeable Harm: When Context Makes Computer Security Publications Liable*

Brandenburg v. Ohio provides the latest jurisprudence on the limits of First Amendment protection for speech encouraging criminal activity.[172] The *Brandenburg* doctrine extends First Amendment protection to advocacy of abstract lawlessness,[173] but not advocacy that "is directed to inciting or producing imminent lawless action and is likely to incite or produce such action."[174] Speech is thus protected unless its probable effect is to prompt its audience to criminal activity and the speaker knows and intends this. On the other hand, if the speech is part of a crime, the speech itself becomes criminal.[175] "[M]any cases of inchoate crimes" are often or always effected through "speech acts."[176] Such crimes include conspiracy, facilitation,

170. *Corley*, 273 F.3d at 453; *Junger*, 209 F.3d at 485; *Karn v. U.S. Dept. of St.*, 925 F. Supp. 1, 10 (D.D.C. 1996); *Reimerdes*, 82 F. Supp. 2d at 220.

171. *Giboney v. Empire Storage & Ice Co*., 336 U.S. 490, 502 (1949).

172. 395 U.S. 444 (1969).

173. *Id*. at 447.

174. *Id*.

175. *Giboney*, 336 U.S. at 502 ("[I]t has never been deemed an abridgement of freedom of speech or press to make a course of conduct illegal merely because the conduct was in part initiated, evidenced, or carried out by means of language, either spoken, written or printed."); *U.S. v. Varani*, 435 F.2d 758, 762 (6th Cir. 1970) ("[S]peech is not protected by the First Amendment when it is the very vehicle of the crime itself.").

176. U.S. Dept. of J., *1997 Report on the Availability of Bombmaking Information* [¶

solicitation, bribery, coercion, blackmail, and aiding and abetting.[177] The fact that speech is involved does not raise any First Amendment question in regulating the activity.

This point is worth emphasizing. There is no First Amendment protection for speech that is part of an otherwise criminal act, no matter how expressive the speech may be.[178] A hypothetical example may be useful. Imagine an Artful Don, an organized crime figure with prodigious creative and criminal talents. The Artful Don seeks First Amendment protection by giving orders to his underlings carry out extortion, murders and the like. This strategy will be unavailing no matter how creative or expressive the orders are. It does not matter if the orders are given in the form of prose, poetry, paintings, sculptures, operas, modern dance or computer code, the speech is still criminal. While the speech itself, devoid of context, merits First Amendment protection, the Don's speech does not have First Amendment protection.

The jurisprudence on First Amendment protection of information which can facilitate illegal acts is instructive in appraising computer security publications' First Amendment protection. Academic commentators have argued that no instructions that facilitate criminal acts deserve First Amendment protection.[179] However, First Amendment protection is not stripped merely because speech comes in the form of instructions.[180] Rather, *Brandenburg* boils down to this:

6] (April 1997) <http://www.usdoj.gov/criminal/cybercrime/bombmakinginfo.html> (accessed Sept. 30, 2002).

177. *Id*.; *see e.g.* Model Penal Code § 223.4 (ALI 2001) (extortion or blackmail); *id*. § 240.2 (threats and other improper influences in official and political matters); *id*. § 241 (perjury and various cognate crimes); *id*. §§ 5.02, 2.06 (3)(a)(i) (criminal solicitation); *id*. § 5.03 (conspiracy); *id*. § 250.4 (harassment); *id*. § 224.1 (forgery); *id*. § 210.5(2) (successfully soliciting another to commit suicide); *id*. § 250.3 (false public alarms); 18 U.S.C. § 871 (2000) (threatening the life of the President).

178. *Giboney*, 336 U.S. at 502.

179. *See* Loris L. Bakken, Student Author, *Providing the Recipe for Destruction: Protected or Unprotected Speech?*, 32 McGeorge L. Rev. 289, 298 (2000); Bruce Braun et. al, *WWW.Commercial_Terrorism.com: A Proposed Federal Criminal Statute Addressing the Solicitation of Commercial Terrorism Through the Internet*, 37 Harv. J. Legis. 159, 180 (2000); Monica Lyn Schroth, Student Author, *Reckless Aiding and Abetting: Sealing the Cracks That Publishers of Instructional Materials Fall Through*, 29 Sw. U. L. Rev. 567, 571 (2000).

180. *Universal City Studios, Inc. v. Corley*, 273 F.3d 424, 447 n.19 (2d Cir. 2001) (citing *Rice v. Paladin Enter., Inc.*, 128 F.3d 233, 247-49 (4th Cir. 1997); *U.S. v. Barnett*, 667 F.2d 835, 842 (9th Cir. 1982)). "Several courts have concluded that . . .

the context of speech, specifically the speaker's intended audience, determines its criminality.[181] Unless the speaker knows his or her intended audience is likely to use the information to facilitate a crime, the speech cannot be criminal.[182] Nevertheless, courts may impute intent from some aspects of the speech's content, such as its potential utility and its explicitness.

This is true of computer code, just as much as it is true of any other form of speech. In *United States v. Mendelsohn*, the defendants raised a First Amendment defense against charges of aiding and abetting interstate transportation of wagering paraphenalia.[183] The *Mendelsohn* defendants provided an undercover officer a floppy disk with the defendants' program, Sport Office Accounting Program (SOAP), which provided a computerized method for recording and analyzing bets on sporting events.[184] The defendants had previously failed to sell SOAP to legal bookmakers and game companies.[185] The court rejected the defendants' argument that the computer program was protected by the First Amendment.[186] The court held that "[t]he question [was] not whether [the program was] speech, but whether it [was] protected speech" and that "a computer program under other circumstances might warrant [F]irst [A]mendment protection. . . ."[187]

Specifically, the Ninth Circuit upheld the trial court's refusal to permit a jury instruction that closely tracked *Brandenburg* protection of advocacy.[188] In order to support a First Amendment jury instruction,

instructions [facilitating criminal acts] fall outside the First Amendment. However, these conclusions never rest on the fact that the speech took the form of instructions, but rather on the fact that the instructions counseled the listener how to commit illegal acts." *Id*.

181. 395 U.S. 444, 447-48 (1969).

182. *Hess v. Ind.*, 414 U.S. 105, 108-09 (1973) (where a statement "was not directed to any person or group of persons, it cannot be said that" it advocated any action, and without "evidence or rational inference" from the language that that speech was "intended to produce, and likely to produce, *imminent* disorder," the speech cannot be made criminal).

183. 896 F.2d 1183**,** 1184-85 (9th Cir. 1990).

184. *Id*. at 1184.

185. *Id*.

186. *Id*. at 1186.

187. *Id*. at 1185.

188. *Id*. at 1185-86. The proposed instruction foreclosed conviction unless " 'it was the intent of one or both of the defendants and the tendency of the computer program at issue here to produce or incite any lawless act, which was in fact likely to occur. . . .' "

there had to be "some evidence that the defendants' speech was informational in a manner removed from immediate connection to the commission of a specific criminal act."[189] The Ninth Circuit held that there was no evidence that indicated the speaker's intended audience used SOAP legally as "[t]here was no evidence that the defendants thought [the undercover officer] was going to use SOAP for anything other than illegal bookmaking. . . . the defendants knew that SOAP was to be used as an integral part of a bookmaker's illegal activity . . ."[190] SOAP was "too instrumental in and intertwined with the performance of criminal activity to retain first amendment protection . . . 'so close in time and purpose to a substantive evil as to become part of the crime itself.' "[191] SOAP's content was not illicit; it could have been sold and used for legal bookmaking.[192] It was the circumstances around SOAP's publication that made it illegal, particularly defendants' knowledge and intent that SOAP would be used for illegal bookmaking.[193]

The criminality of instructions or information also depends on the speaker's intended audience in other contexts. The lion's share of these cases deal with charges of aiding and abetting against tax protestors who advocate and instruct others on filing fraudulent tax returns.[194] These cases consistently reference criminality's dependence on the speaker's intent and participation. A representative example is *United States v. Buttorff*.[195] In *Buttorff*, the Eighth Circuit upheld the conviction of the appellants for aiding and abetting tax fraud when they explained how to fraudulently reduce tax withholdings.[196] Referencing *Brandenburg*, *Buttorff* found that the appellants' speech

Id. (quoting *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969)).

189. *Id*. at 1185 (citing *U.S. v. Freeman*, 761 F.2d 549, 551 (9th Cir. 1985)).

190. *Id*.

191. *Id*. at 1186 (quoting *Freeman*, 761 F.2d at 552).

192. *Id*. at 1184.

193. *Id*. at 1185.

194. *See e.g. U.S. v. Rowlee*, 899 F.2d 1275, 1276 (2d Cir. 1990), *cert. denied,* 498 U.S. 828 (1990); *U.S. v. Kelley*, 769 F.2d 215, 216 (4th Cir. 1985); *U.S. v. Raymond*, 228 F.3d 804, 815 (7th Cir. 2000); *U.S. v. Moss*, 604 F.2d 569, 570 (8th Cir. 1979), *cert. denied,* 444 U.S. 1071 (1980); *U.S. v. Buttorff*, 572 F.2d 619, 621 (8th Cir. 1978); *U.S. v. Solomon*, 825 F.2d 1292, 1294 (9th Cir. 1987), *cert. denied,* 484 U.S. 1046 (1988); *U.S. v. Freeman*, 761 F.2d 549, 551 (9th Cir. 1985), *cert. denied,* 476 U.S. 1120 (1986); *U.S. v. Dahlstrom*, 713 F.2d 1423, 1424 (9th Cir. 1983).

195. 572 F.2d 619 (8th Cir. 1978).

196. *Id*. at 621-22.

went "beyond mere advocacy of tax reform."[197] *Buttorff* found the speech was not within First Amendment protection because the appellants "explained how to avoid withholding and their speeches and explanations incited several individuals" to tax fraud and provided substantial assistance to that end.[198]

Brandenburg has also been applied in the context of instructions for the manufacture of narcotics.[199] A search warrant was executed against the defendant in *United States v. Barnett* for aiding and abetting the attempted manufacture of phencyclidine (PCP) by mailing instructions for synthesis of the same.[200] *Barnett* refused to quash the results of the search on the basis that the defendant's acts could not constitute aiding and abetting, stating:

> The [F]irst [A]mendment does not provide a defense to a criminal charge simply because the actor uses words to carry out his illegal purpose. Crimes . . . frequently involve the use of speech as part of the criminal transaction. [Many acts] . . . constitute crimes despite the use of speech as an instrumentality for the commission thereof.[201]

Nevertheless, *Barnett* found that the aider-abettors had to have the requisite criminal intent.[202]

Applications of the *Brandenburg* doctrine in the context of civil liability for instructions on committing wrongful acts also analyzes the significance of a speaker's intended audience.[203] Like criminal sanctions, civil liability faces heightened scrutiny when regulating speech.[204] *Herceg v. Hustler Magazine, Inc.* dealt with a negligence action against *Hustler* over an article about autoerotic asphixiation.[205] One of the *Herceg* plaintiffs read the article and consequently killed

197. *Id*. at 624 (citing *Brandenburg v. Ohio*, 395 U.S. 444 (1969)).

198. *Id*.

199. *See U.S. v. Barnett*, 667 F.2d 835 (9th Cir. 1982).

200. *Id*. at 838.

201. *Id*. at 842.

202. *Id*. at 843.

203. *N.Y. Times Co. v. Sullivan*, 376 U.S. 254 (1964).

204. *Id*. at 277 (stating that "what a state may not constitutionally bring about by means of a criminal statute is likewise beyond the reach of its civil law of libel" because the fear of civil liberty might be "markedly more inhibiting than the fear of prosecution under a criminal statute").

205. 814 F.2d 1017, 1018-19 (5th Cir. 1987).

himself by accident while attempting to engage in autoerotic asphixiation.[206] The jury awarded the plaintiffs substantial damages on the grounds that the defendant's article incited the decedent to act.[207] The trial court denied defendant's motion for judgment notwithstanding the verdict.[208] The Fifth Circuit reversed the jury's verdict against the defendant for incitement.[209]

Herceg found that the First Amendment required the *Brandenburg* element to be read into stating that, incitement, the "encouragement of conduct that might harm the public," cannot be the basis of liability unless "directed to inciting or producing *imminent* lawless action and . . . *likely* to incite or produce such action."[210] *Herceg* stated that imminence of the wrongful act produced by the speech was a critical factor for liability.[211] Analyzing the *Hustler* article at issue, the *Herceg* court found that the article's description of autoerotic asphixiation was not too explicit, at least in part, because no great amount of detail is required to commit autoerotic asphixiation.[212] *Herceg* found that there was no evidence the authors of the article intended for their readers to commit autoerotic asphixiation.[213] Indeed, "the article [was] laden with detail about . . . the physiology of how it produces a threat to life and the seriousness of the danger of harm."[214] From this evidentiary basis, the court concluded that the article did not attempt to incite autoerotic asphixiation at all, let alone in a manner for which *Hustler* might be made liable.[215]

Rice v. Paladin Enterprises, Inc. dealt with a wrongful death suit against a publisher of *Hit Man: A Technical Manual for Independent Contractors.*[216] The *Rice* plaintiffs charged that *Hit Man* aided and

206. *Id*. at 1019.
207. *Id*. at 1019-20.
208. *Id*. at 1019.
209. *Id*. at 1025.
210. *Id*. at 1022 (citing *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969).
211. *Id*. (analyzing *Hess v. Ind.*, 414 U.S. 105, 108-09 (1973)).
212. *Id*. at 1023.
213. *Id*. at 1021.
214. *Id*. at 1023.
215. *Id*. at 1017.
216. 128 F.3d 233 (4th Cir. 1997); *see Braun v. Soldier of Fortune Mag.*, 757 F. Supp. 1325, 1326 (M.D. Ala. 1991) (citing liability for magazine which permitted contract killer to place advertisement which resulted in wrongful death), *aff'd,* 968 F.2d 1110 (11th Cir. 1992), *cert. denied,* 506 U.S. 1071 (1993).

abetted James Perry in the course of his contract killing of their family members.[217] *Rice*, recognizing that *Brandenburg* protected many forms of advocacy, determined that the First Amendment did not protect "speech brigaded with action," such as those speech acts previously enumerated.[218] The court found that the speaker's intent was critical to determining the criminality of the speech:

> [I]n order to prevent the punishment or even the chilling of entirely innocent, lawfully useful speech, the First Amendment may in some contexts stand as a bar to the imposition of liability on the basis of mere foreseeability or knowledge that the information one imparts could be misused for an impermissible purpose. . . . [But] where a speaker—individual or media—acts with the purpose of assisting in the commission of crime, we do not believe that the First Amendment insulates that speaker from responsibility for his actions simply because he may have disseminated his message to a wide audience. . . .
>
> [The] First Amendment poses no bar to the imposition of civil (or criminal) liability for speech acts which the plaintiff (or the prosecution) can establish were undertaken with specific, if not criminal, intent.[219]

Rice assumed, but did not hold, that "liability could not be imposed [on instructions for criminal conduct] on a finding of mere foreseeability or knowledge that the instructions might be misused for a criminal purpose."[220] However, the court not only found that Paladin stipulated to such a specific intent, but also that the evidence of the case would permit a jury to find such an intent.[221]

217. 128 F.3d at 241.

218. *Id*. at 244 (citing *Brandenburg*, 395 U.S. 444, 456 (1969)). "[T]he provision of instructions that aid and abet another in the commission of a criminal offense is unprotected by the First Amendment, has been uniformly accepted, and the principle has been applied to the aiding and abetting of innumerable crimes." *Id*. at 245 (citing *e.g. U.S. v. Rowlee*, 899 F.2d 1275 (2d Cir. 1990); *U.S. v. Kelley*, 796 F.2d 215 (4th Cir. 1985); *U.S. v. Buttorff*, 572 F.2d 619 (8th Cir. 1978); *U.S. v. Barnett*, 667 F.2d 835 (9th Cir. 1982); *U.S. v. Freeman*, 761 F.2d 549 (9th Cir. 1985); *U.S. v. Mendelsohn*, 896 F.2d 1183 (9th Cir. 1990)).

219. *Rice*, 128 F.3d at 247-48.

220. *Id*. at 266.

221. *Id*. at 248.

The court cited four indicia which, in concert or possibly individually, provided the necessary evidence from which a jury could conclude that Paladin had specific intent to aid and abet murderers.[222] These criteria could be applied to computer security publications to determine intent. First, *Hit Man* expressly stated that instructing prospective criminals was its purpose.[223] Second, the court found the *Hit Man* text promoted crime so highly, a jury could conclude that Paladin's intent was to instruct murderers.[224] Third, *Rice* found that Paladin's selection of its audience could, by itself, provide a reasonable basis for the inference that *Hit Man*'s intended audience was prospective criminals.[225] "Paladin marketed Hit Man directly and even primarily to murderers and would-be criminals, and, from this permissible conclusion, in turn conclude that Paladin possessed the requisite intent necessary to support liability."[226] Paladin's method of marketing *Hit Man* through its catalogue assured *Hit Man*'s audience would be entirely self-selected and "contemplating or highly susceptible to the commission of murder."[227] Finally, *Rice* found that *Hit Man* had no alternate communicative value beyond the illegitimate one of instructing people how to commit crime (including informing law enforcement of murderers potential techniques or entertainment value to the public at large).[228] "Hit Man's only genuine use is the unlawful one of facilitating such murders."[229] *Rice* made this finding at the same time as it carefully reviewed the explicit detail in *Hit Man*. Moreover, *Rice* rejected the argument that a publication which has any use beyond facilitating a wrongful act must thereby have First Amendment protection.[230]

222. *Id*. at 253.

223. *Id*.

224. *Id*. at 254 ("The unique text of Hit Man alone, boldly proselytizing and glamorizing the crime of murder and the 'profession' of murder as it dispassionately instructs on its commission, is more than sufficient to create a triable issue of fact as to Paladin's intent in publishing and selling the manual.").

225. *Id*.

226. *Id*. (explaining that "Paladin essentially distributed Hit Man only to murderers and would-be murderers—that its conduct was not, at least in law, different from that of a publisher (or anyone else) who delivered Hit Man to a specific person or group of persons whom the publisher knew to be interested in murder").

227. *Id*. at 255.

228. *Id*.

229. *Id*.

230. *Id*. at 263 n. 9 (citing e.g. *U.S. v. Kelley*, 769 F.2d 215, 216-17 (4th Cir. 1985);

The *Rice* court held that the speech in *Hit Man* (instructions facilitating criminal acts) falls outside of *Brandenburg*'s protection. *Rice* reasoned that *Brandenburg* was meant to be applied to advocacy of political change, and that the requirements of "imminence" and "likelihood" are therefore inapplicable to regulations of instructive speech.[231] Regardless of whether *Brandenburg* is the correct test to determine the First Amendment protection of computer security publications, the indicia of First Amendment protection of computer security publications have been delineated. *Mendelsohn*, *Kelley* and *Rice* suggest that a computer security publishers' intended audience is the most significant determinant of the publisher's liability. Likewise, *Herceg* and *Rice* imply that a computer security publication's utility in facilitating criminal acts, particularly its explicitness, might also determine whether the publisher will be held liable.

At the outset, these cases show that even natural language computer security publications do not have unqualified First Amendment protection. The standards articulated in these cases pose some interesting problems for computer security publications. Most computer security publications are freely available on the Internet. The audience will be self-selected because of their interest in computer security. As the epigraph notes, some percentage of any such audience will later use the publication to perpetrate computer crime.[232] *Rice* found that deliberately selecting an audience was adequate evidence for the specific intent on which liability is based.[233] What remains indeterminate is whether (or when) publication on the Internet at large evidences the same intent. If *Rice* is correct, the intent to inform legitimate users as well as computer criminals is no barrier to liability. Courts may well have to look at other indications of the context of a publication to determine a publisher's intent. Moreover, this analysis assumes that the only communication between the publisher and the audience is the publication. When the publication occurs in response to solicitations of information to identify and patch a vulnerability (or to exploit one as part of a criminal scheme), the analysis is much easier.

More concretely, the discussions in *Herceg* and *Rice* regarding the utility and explicitness of instructions, offer grounds to distinguish

U.S. v. Freeman, 761 F.2d 549, 551 (9th Cir. 1985).

231. *Id*. at 262-63, 265.

232. *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 451-52 (2d Cir. 2001).

233. *Rice*, 128 F.3d at 254-55.

computer security publications. Patches and natural language instructions for eliminating vulnerabilities intuitively fall well within First Amendment protection. Determining the First Amendment protection of natural language descriptions of actual vulnerabilities and source code exploits requires more care. The more explicit a computer security publication, the greater its potential utility to both computer criminals and legitimate users and vendors. On the other hand, binary code exploits, by themselves, have much more limited legitimate utility. While patches are probably beyond reproach, First Amendment protection of source code exploits is uncertain and it is likely the presumption will be against binary code exploits. For example, the creator of the "Melissa" virus was charged with, and pleaded guilty to, violations of New Jersey law, the federal Computer Fraud and Abuse Act and aiding and abetting a violation of federal law.[234] No matter that the computer code might have been protectible speech in some other context, the defendant's criminal liability was apparently not worth contesting. When executed "Melissa" mailed itself to the first fifty individuals in a person's address book.[235] This permitted "Melissa" to expand exponentially.[236] The defendant posted the "Melissa" virus to a newsgroup with the expectation that it would infect those who opened it and spread from them.[237] The basis of criminal liability is clear from the predatory nature of the virus, which had little utility to legitimate users but was designed to cause harm, and the speaker's intent, which could be inferred from the nature of the code. Indeed, this example blurs the line between a computer security publisher with illicit intentions and a computer criminal which uses the code.

2. *Regulating Publication Content Itself*

First Amendment protection for speech acts hinges on the context of the speech; the speaker's intended audience determines the speech's

234. U.S. Dept. of J., *Creator of "Melissa" Computer Virus Pleads Guilty to State and Federal Charges* [¶¶ 1, 4, 5] (Dec. 9, 1999) <http://www.cybercrime.gov/melissa.htm> (noting that defendant pleaded guilty to violations of 18 U.S.C. §§ 2, 1030(a)(5)(A) (2000)) (accessed Oct. 3, 2002).

235. *Id*. at [¶ 14].

236. *Id*. at [¶ 15].

237. *Id*. at [¶ 16].

criminal and civil liability.[238] The judiciary uses an altogether different analysis when it considers the First Amendment protection of speech which has an inherently functional element.[239] Liability can be assigned to computer code because of its content, as well as its context.

The level of First Amendment scrutiny applied to speech regulation depends on whether the regulation targets the speech's content or its type.[240] Restrictions based on speech's expressive content face higher scrutiny.[241] The lower standard applies to content-neutral speech regulations: the restriction may not burden substantially more speech than is necessary to serve a legitimate government interest.[242] Appropriate content-neutral restrictions are commonly "time, place, or manner" restrictions.[243] "Government regulation of expressive activity is 'content neutral' if it is justified without reference to the content of regulated speech."[244] "The government's purpose is the controlling consideration. A regulation that serves purposes unrelated to the content of expression is deemed neutral, even if it has an incidental effect on some speakers or messages but not others."[245] One such instance of content-neutral regulation is *United States v.*

238. *See Rice v. Paladin Enterprises, Inc.*, 128 F.3d 233, 248 (4th Cir. 1997).

239. *Id*. at 255-56.

240. *See Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989).

241. *Sable Comm. of Ca., Inc. v. F.C.C.*, 492 U.S. 115, 126 (1989) (explaining that content based restrictions are permissible only if they serve compelling state interests and do so by the least restrictive means available).

242. *Turner Broad. Sys., Inc. v. F.C.C.*, 512 U.S. 622, 662 (1994);

> [A] content-neutral regulation will be sustained if it furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression [and the regulation is] . . . [n]arrowly tailor[ed], [which] in this context requires . . . that the means chosen do not "burden substantially more speech than is necessary to further the government's legitimate interests."

Id.

243. *See U.S. v. O'Brien*, 391 U.S. 367, 377 (1968) (citing that the government prohibition against burning of draft cards is sufficiently justified if, among other things, "the governmental interest is unrelated to the suppression of free expression"); *Clark v. Community of Creative Non-Violence*, 468 U.S. 288, 298 (1984) (citing that the standard for evaluating expressive conduct, including the requirement that regulation be content-neutral, "is little, if any, different from the standard applied to time, place, or manner restrictions"); *Ward*, 491 U.S. at 791 (citing "time, place, or manner" restriction on music permitted where, among other things, regulation was content-neutral).

244. *Hill v. Colorado*, 530 U.S. 703, 720 (2000).

245. *Ward*, 491 U.S. at 791.

O'Brien.[246] In *O'Brien* the Supreme Court upheld the conviction of defendants who burned their draft cards in violation of the Universal Military Training and Service Act, despite defendants' arguments that this application of the Act violated their First Amendment rights.[247] *O'Brien* held that "when 'speech' and 'nonspeech' elements are combined in the same course of conduct, a sufficiently important governmental interest in regulating the nonspeech element can justify incidental limitations on First Amendment freedoms."[248]

The courts in *Reimerdes* and *Corley* applied the *O'Brien* analysis to regulation of computer code.[249] These cases dealt with an injunction obtained by the plaintiffs, a group of movie studios, enjoining defendants from making available or linking to a computer program that eliminated the copy protection features on DVDs by decrypting them.[250] The program, named DeCSS, permitted users to access the data from DVDs on unlicensed platforms and transmit the data across the Internet.[251] The plaintiffs obtained the injunction under the Digital Millennium Copyright Act (DMCA).[252] The relevant provisions of the DMCA prohibited the distribution of DeCSS because it circumvented the copyright protection features incorporated into DVDs.[253] Defendants contested the constitutionality of the DMCA, both facially

246. 391 U.S. 367 (1968).

247. *Id*.

248. *Id*. at 376.

249. 273 F.3d 429, 450 (2d. Cir. 2001); 111 F. Supp. 2d 294, 327-28 (S.D.N.Y 2000).

250. *Corley*, 273 F.3d. at 434; *Reimerdes*, 111 F. Supp. 2d at 303-04.

251. *Corley*, 273 F.3d at 437-39;

> An item of some controversy, both in this litigation and elsewhere, is the extent to which CSS-encrypted DVDs can be copied even without DeCSS. The record leaves largely unclear how CSS protects against the copying of a DVD, as contrasted with the playing of a DVD on an unlicensed player. The [d]efendants' experts insisted that there is nothing about the way CSS operates that prevents the copying of a DVD. . . . However, none of this detracts from these undisputed findings: some feature of either CSS itself, or another (unidentified) safeguard implemented by DVD manufacturers pursuant to their obligations under the CSS licensing scheme, makes it difficult to copy a CSS-encrypted DVD to a hard drive and then compress that DVD to the point where transmission over the Internet is practical.

Id. at 438 n. 5.

252. *Id*. at 434; *Reimerdes*, 111 F. Supp. 2d at 303; 17 U.S.C. §§ 1201-04 (2000).

253. 17 U.S.C. §§ 1201(a)(2), (b)(1).

and as applied, at the district court level and at the Second Circuit.[254] One of the First Amendment defenses raised by defendants' was that the DMCA impermissibly restricted their free speech.[255] *Reimerdes* applied *O'Brien* and found that the DMCA was a content-neutral regulation,[256] and that the DMCA's application against DeCSS furthered the sufficiently substantial government interest of supporting copyrights.[257] On appeal, *Corley* upheld *Reimerdes*, praising the decision as "extremely lucid" and quoting large portions of the lower decision with approval.[258] Likewise, *United States v. Elcom, Ltd.* followed the DeCSS decisions' aplication of *O'Brien*.[259]

254. *Corley*, 273 F.3d at 453-59; *Reimerdes*, 111 F. Supp. 2d at 325- 26.

255. *Corley*, 273 F. 3d at 453-54, 456; *Reimerdes*, 111 F. Supp. 2d at 325-26.

256. *Reimerdes*, 111 F. Supp. 2d at 328-29;

> The reason that Congress enacted the anti-trafficking provision of the DMCA had nothing to do with suppressing particular ideas of computer programmers and everything to do with functionality—with preventing people from circumventing technological access control measures—just as laws prohibiting the possession of burglar tools have nothing to do with preventing people from expressing themselves by accumulating what to them may be attractive assortments of implements and everything to do with preventing burglaries.

Id. at 329.

257. *Id*. at 333.

258. 273 F.3d at 435, 451-52 (citing *Reimerdes*, 111 F. Supp. 2d at 331-32).

259. *U.S. v. Elcom, Ltd.*, 203 F. Supp. 2d 1111, 1130-32 (N.D. Cal. 2002);

> Congress certainly could have approached the problem by targeting the infringers, rather than those who traffic in the tools that enable the infringement to occur. However, it is already unlawful to infringe, yet piracy of intellectual property has reached epidemic proportions. Pirates are world-wide, and locating and prosecuting each could be both impossible and ineffective, as new pirates arrive on the scene. But, pirates and other infringers require tools in order to bypass the technological measures that protect against unlawful copying. Thus, targeting the tool sellers is a reasoned, and reasonably tailored, approach to "remedying the evil" targeted by Congress. In addition, because tools that circumvent copyright protection measures for the purpose of allowing fair use can also be used to enable infringement, it is reasonably necessary to ban the sale of all circumvention tools in order to achieve the objectives of preventing widespread copyright infringement and electronic piracy in digital media. . . . A sufficiently important government interest in regulating the targeted conduct can justify incidental limitations on First Amendment freedoms. . . . [T]he DMCA does not burden substantially more speech than is necessary to achieve the government's asserted goals of promoting electronic commerce, protecting copyrights, and preventing electronic piracy.

Id. at 1132.

Both the *Corley* and *Reimerdes* decisions were based on the functionality of DeCSS and the potential effects of its dissemination on the Internet.[260] The DeCSS decisions help further define the First Amendment protection of computer code and computer security publications. DeCSS drew liability because of the functionality inherent in its expression.[261] As the court acknowledged, the communicative aspect of DeCSS, as with any exploit code, is explicit and detailed.[262] In the context of computer code, regulation of functionality must also monitor that same explicitly detailed expression in code. Indeed, the defendant in *Elcom* argued that it was "impossible to regulate the 'functional' aspects of computer code without necessarily regulating the content of the expressive aspects of the code."[263]

Two guidelines applicable to computer security publications emerge from the DeCSS decisions' analysis. First, computer code's functionality, made possible by and contingent on explicit content, is also the foundation for liability.[264] The greater the detail of a publication, the less First Amendment protection is available.[265] Second, exploit's diminution of the human involvement necessary to cause harm decreases the likelihood of First Amendment protection.[266] From this, it may be concluded that source code (which must be compiled and executed before harm results) receives some marginal degree of First Amendment protection more than binary code (which is

260. 273 F.3d at 451-52, 456; 111 F. Supp. 2d at 311.

261. *Corley*, 273 F.3d at 450-51;

> Unlike a blueprint or a recipe, which cannot yield any functional result without human comprehension of its content, human decision-making, and human action, computer code can instantly cause a computer to accomplish tasks and instantly render the results of those tasks available throughout the world via the Internet. The only human action required to achieve these results can be as limited and instantaneous as a single click of a mouse. These realities of what code is and what its normal functions are require a First Amendment analysis that treats code as combining nonspeech and speech elements, i.e., functional and expressive elements.

Id. at 451.

262. *Reimerdes*, 111 F. Supp. 2d at 315.

263. *Elcom*, 203 F. Supp. 2d at 1128. *Elcom* dismissed this argument as *Reimerdes* did, reasoning that the code was banned, not for what it said, but what it did. *Id*.

264. *Corley*, 273 F.3d at 452.

265. *Id*.

266. *Id*.

both less easily understood and need only be executed before harm results.)

While *Elcom* merely concluded that the DMCA's numerous statutory exceptions generated the balance to withstand intermediate scrutiny, both the district court and the appellate DeCSS decisions acknowledged that using functionality of code to determine the level First Amendment scrutiny slid "over questions of causation that intervene between the dissemination of a computer program and any harm caused by its use."[267] Arguing that sliding over questions of causation prohibiting the use of functionality as a determinant of First Amendment protection, *Reimerdes* adopted (and *Corley* has implicitly upheld) the assumption that the distribution of DeCSS would promote copyright infringement.

> [T]he assumption that the chain of causation [between dissemination of DeCSS and copyright infringement] is too attenuated to justify the use of functionality to determine the level of scrutiny, at least in this context, is not [accurate.] Society increasingly depends upon technological means of controlling access to digital files and systems, whether they are military computers, bank records, academic records, copyrighted works or something else entirely. There are far too many who, given any opportunity, will bypass those security measures, some for the sheer joy of doing it, some for innocuous reasons, and others for more malevolent purposes. Given the virtually instantaneous and worldwide dissemination widely available via the Internet, the only rational assumption is that once a computer program capable of bypassing such an access control system is disseminated, it will be used.[268]

Reimerdes and *Corley* both equate the dissemination of DeCSS and the minimal human involvement required by DeCSS to decrypt DVDs with the use of DeCSS to perpetrate copyright infringement and DMCA violations.[269] As a finder of fact, the *Reimerdes* court can be faulted or second-guessed, but its finding that DeCSS would cause copyright infringement was well within its discretion. Limited to

267. *Reimerdes*, 111 F. Supp. 2d at 331 (citing Lee Tien, *Publishing Software as a Speech Act*, 15 Berkeley Tech. L.J. 629, 694-701 (2000)); *Corley*, 273 F.3d at 451; 203 F. Supp. at 1111).

268. 273 F.3d at 451-52; 111 F. Supp. 2d at 332.

269. 273 F.3d at 452; 111 F. Supp. 2d at 331.

DeCSS, *Corley* and *Reimerdes*' effect is not destabilizing. But courts relying on that holding might overextend it if it is applied uncritically to other computer security publications. This expansion of liability could seriously threaten the market for computer security.

This article merely urges courts and others to consider the empirical effect of suppressing computer security publication. A thorough examination of the First Amendment's necessary causal connection between speech and an underlying harm would be beyond the scope of this article. The Supreme Court has found regulation of speech to be unconstitional when insufficiently related to the underlying harm. Under *New York v. Ferber*,[270] child pornography may be prohibited, even when it is not obscene under *Miller v. California*,[271] and may be regulated.[272] *Ferber* reasoned, in part, that child pornography was "intrinsically related to the sexual abuse of children in at least two ways."[273]

> First, the materials produced are a permanent record of the children's participation and the harm to the child is exacerbated by their circulation. Second, the distribution network for child pornography must be closed if the production of material which requires the sexual exploitation of children is to be effectively controlled.[274]

Like copyright infringement in the digital era, production of child pornography is difficult to detect and prevent, and it is even more difficult to apprehend offenders.[275] Thus, the most effective scheme of

270. 458 U.S. 747 (1982).

271. 413 U.S. 15 (1973).

272. 458 U.S. at 752-64 (1982).

273. *Id*. at 759.

274. *Id*.

275. *Id*. at 760 ("The most expeditious if not the only practical method of law enforcement may be to dry up the market by imposing severe criminal penalties on persons selling, advertising, or otherwise promoting the product.").

> There was a time when copyright infringement could be dealt with quite adequately by focusing on the infringing act. If someone wished to make and sell high quality but unauthorized copies of a copyrighted book, for example, the infringer needed a printing press. The copyright holder, once aware of the appearance of infringing copies, usually was able to trace the copies up the chain of distribution, find and prosecute the infringer, and shut off the infringement at the source. In principle, the digital world is very different. Once a decryption program like DeCSS is written, it quickly can be sent all over the world. Every recipient is capable not only of decrypting and

protecting the underlying governmental interest is to regulate related speech.[276]

However, the Court later found a federal statute prohibiting virtual child pornography (computer-generated images depicting children sexually, even where no actual children were involved) to be unconstitutional.[277] The Court found that virtual child pornography was not "intrinsically related" to the sexual abuse of children as discussed in *Ferber*.[278] One of the government's arguments rejected in *Ashcroft v. Free Speech Coalition* was that virtual child pornography made it very difficult to prosecute actual child pornography and that, therefore, both had to be banned to prevent the underlying sexual abuse.[279]

> The necessary solution, the argument runs, is to prohibit both kinds of images. The argument, in essence, is that protected speech may be banned as a means to ban unprotected speech. This analysis turns the First Amendment upside down. The Government may not suppress lawful speech as the means to suppress unlawful speech.[280]

The Court rejected arguments that virtual child pornography could be used to seduce children or to arouse the appetites of pedophiles and encourage them to commit crimes.[281] The government argued that the statute merely provided that a defendant under the statute prove that the images were computer-generated.[282] The Court

---

> perfectly copying plaintiffs' copyrighted DVDs, but also of retransmitting perfect copies of DeCSS and thus enabling every recipient to do the same. They likewise are capable of transmitting perfect copies of the decrypted DVD. The process potentially is exponential rather than linear.

Cf. Corley, 273 F.3d 429, 452 (2d. Cir. 2001) (quoting *Reimerdes*, F. Supp. at 331).

276. *See Ferber*, 458 U.S. at 760; *Corley*, 273 F.3d at 452.

277. *Ashcroft v. Free Speech Coalition*, 122 S. Ct. 1389 (2002).

278. *Id*. at 1401-02 (quoting 458 U.S. at 759).

279. *Id.* at 1404.

280. *Id*.

281. *Id*. at 1402;

> The Government cannot ban speech fit for adults simply because it may fall into the hands of children. The evil in question depends upon the actor's unlawful conduct, conduct defined as criminal quite apart from any link to the speech in question. . . . The mere tendency of speech to encourage unlawful acts is not a sufficient reason for banning it.

Id. at 1403.

282. *Id.* at 1406.

further rejected that argument on the basis that the statute, as written was unconstitutionally overbroad.[283] However, the Court raised the issue of whether such evidentiary burden on speech would be Constitutional.[284]

In *Ashcroft*, the government's allegation was that virtual pornography encouraged and facilitated actual child pornography and sexual abuse of children.[285] In *Corley*, the DMCA's goal is to restrict underlying copyright infringements and prevent unauthorized access to copyrighted works.[286] Other legal theories may be employed to restrict computer security publications in order to prevent computer crime. However, the First Amendment limits criminal and civil penalties for speech that present the possibility of facilitating criminal activity.

> To preserve these freedoms, and to protect speech for its own sake, the Court's First Amendment cases draw vital distinctions between words and deeds, between ideas and conduct. . . . The normal method of deterring unlawful conduct is to impose an appropriate punishment on the person who engages in it. The government may not prohibit speech because it increases the chance an unlawful act will be committed at some indefinite future time. . . . The Government has shown no more than a remote connection between speech that might encourage thoughts or impulses and any resulting child abuse. Without a significantly stronger, more direct connection, the Government may not prohibit speech on the ground that it may encourage pedophiles to engage in illegal conduct.[287]

Likewise, *Ashcroft* suggests that it is not enough to show that computer security publications might facilitate computer crime in the indeterminate future.[288] Civil or criminal penalties for computer security publications must point to some significant, direct connection between the publication to actual computer crime.

283. *Id*.
284. *Id*. at 1405.
285. 122 S. Ct. 1389 (2002).
286. 273 F.3d 429 (2d Cir. 2001).
287. *Ashcroft*, 122 S. Ct. at 1403.
288. *Cf. id*.

C. *THEORIES OF LIABILITY APPLICABLE TO COMPUTER SECURITY PUBLICATIONS*

Any number of theories of liability may apply to computer security publications. Nevertheless, certain theories emerge as more significant threats to computer security publications. This subsection outlines the most prominent theories of liability. Negligence does not require great discussion, but it certainly could be a theory of liability against a computer security publisher. Conspiracy to commit computer fraud and aiding and abetting computer fraud are obvious sources of criminal liability in certain contexts. Certain state computer fraud laws may also implicate computer security publications. Mail fraud and wire fraud may also apply. However, the most important sources of liability are the DMCA and the prospective implementation of the Council of Europe Convention on Cybercrime. Even though the application of the DMCA may not be especially obvious and the Cybercrime Convention may not be especially well-known, both these laws have far-reaching implications for computer security publications.

1. *The Digital Millennium Copyright Act*

The DMCA is the United States' implementation of the World Intellectual Property Organization (WIPO) Copyright Treaty.[289] There are currently thirty seven signatories to the treaty.[290] The DMCA has three basic provisions. The DMCA first prohibits circumvention of any "technological measure that effectively controls access to a work protected" under the copyright title of the United States code.[291] While

289. *WIPO Copyright Treaty and Agreed Statements Concerning the WIPO Copyright Treaty* (Apr. 12, 1997), Sen. Treaty Doc. No. Treaty Number 105-17 (available at <http://www.wipo.int/clea/docs/en/wo/wo033en.htm> (accessed Sept. 30, 2002)).

290. WIPO, *WIPO Copyright Treaty* (July 25, 2002) <http://www.wipo.int/treaties/documents/english/pdf/s-wct.pdf> (accessed Sept. 30, 2002) (citing current signatories, which include Argentina, Belarus, Bulgaria, Burkina Faso, Chile, Colombia, Costa Rica, Croatia, Czech Republic, Ecuador, El Salvador, Gabon, Georgia, Guinea, Honduras, Hungary, Indonesia, Jamaica, Japan, Kyrgyzstan, Latvia, Lithuania, Mali, Mexico, Mongolia, Panama, Paraguay, Peru, Philippines, Republic of Moldova, Romania, Saint Lucia, Senegal, Slovakia, Slovenia, Ukraine and the U.S.).

291. 17 U.S.C. §§ 1201 (a)(1)(A), (a)(3)(A) (2000) (stating that " 'to circumvent a technological measure' means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a

this provision intuitively applies to products with digital rights technologies incorporated specifically to protect a copyrighted work, it could be also applied to computer crime in general. At issue is the very broad scope of works protected under Title 17. Copyrights subsist in "original works of authorship fixed in any tangible medium of expression . . . from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device."[292] The threshold for originality is low; it means only that a work was independently created by an author, as opposed to copied from other works, and that it possesses at least some "minimal degree of creativity."[293] Many works, such as texts, drawings, or other files that are produced by humans and saved as files onto computer systems, qualify for copyright. To the extent that operating systems and applications are designed to control access to those files (for instance, by requiring a password), they are technological measures which effectively control access to works protected by the copyright title. Therefore, the execution of exploits without authorization that permits access to copyrightable computer files violates the DMCA, even though the security circumvented was not designed to specifically protect copyrighted works.

While this may be a novel application of the DMCA, it does not, by itself, extend liability for computer security publications beyond the traditional limits of aiding and abetting or conspiracy.[294] It is the DMCA's other two core provisions which could directly threaten computer security publications.[295] The DMCA also prohibits the manufacture, distribution or traffic in "any technology, product, service, device, component, or part thereof," which "is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under" Title 17, and "has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively

technological measure, without the authority of the copyright owner"); *id*. § 1201 (a)(3)(B) (stating that "a technological measure 'effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work").

292. 17 U.S.C. § 102 (a).

293. *Feist Publications, Inc. v Rural Tel. Serv. Co.*, 499 U.S. 340, 345 (1991).

294. *See* 17 U.S.C. § 1202(b).

295. *See id*. §§ 1201(a)(2), (b)(1).

controls access to a work protected under this title," or "is marketed by that person or another acting in concert with that person . . . with [the] knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title."[296]

The final provision prohibits the same activities with technologies or devices that circumvent technological measure that "effectively protects a right of a copyright owner."[297] Copyright owners have the exclusive right to reproduction, even in a medium ephemeral as a computer's random access memory.[298] Hence, providing the means to view a file located on one computer by a remote computer would trigger liability under the last provision. The prohibition on distribution of this technology directly implicates computer security publications.

The DMCA provides for civil remedies,[299] including statutory damages up to $2,500 per act of circumvention,[300] injunctions and destruction of violative technologies.[301] The DMCA also provides for criminal penalties for DMCA violations for "commercial advantage or private financial gain" (of up to one-half million dollars in fines and five years in prison for the first offense, and double that for subsequent offenses).[302] Interestingly, exemptions for nonprofit libraries, archives, educational institutions, and public broadcasting entities apply to both civil and criminal remedies.[303]

The application of the DMCA to computer security publications is not straightforward. First, the publication must fall within one of the categories of DMCA's distribution provisions.[304] This may not be a difficult standard to meet. Most exploits published on the Internet for

296. 17 U.S.C. § 1201(a)(2)-(a)(2)(C).

297. *Id*. § 1201(b)(1)(A), (b)(2)(A) (stating that "to 'circumvent protection afforded by a technological measure' means avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure"); *id*. § 1201(b)(2)(B) (stating that "a technological measure 'effectively protects a right of a copyright owner under this title' if the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title").

298. *See e.g. MAI Systems Corp. v. Peak Computer Corp.*, 991 F.2d 511, 518 (9th Cir. 1993).

299. 17 U.S.C.. § 1203(a).

300. *Id*. § 1203(b)(3), (c)(3)(A).

301. *Id*. § 1203(b)(1), (b)(6).

302. *Id*. § 1204(a)(1)-(2).

303. *Id*. §§ 1203(c)(5)(B), 1204(b).

304. *See id*. § 1201(a)(2)(A)-(C).

the sake of demonstrating a vulnerability would probably be found to be primarily designed or produced for the purpose of circumventing digital rights technologies, or to have only limited commercially significant purpose or use besides circumventing digital rights technologies.[305]

The DMCA also has a set of several exemptions,[306] including encryption research,[307] and security testing.[308] Encryption research is defined as "activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products."[309] Encryption research does not violate the DMCA if the encrypted work was lawfully obtained, a good faith effort was made to obtain authorization before decryption, the decryption does not violate any other law, and it is necessary to advance the field of encryption.[310] Courts must consider three factors to determine whether a person qualifies for the encryption research exemption.[311] The factors to be considered are: (1) "whether [the research] was disseminated in a manner reasonably [likely] to advance the state . . . of encryption [research]" as opposed to a manner likely to contribute to copyright infringement, breach of security or invasion of privacy; (2) whether the researcher had appropriate training in encryption; and, (3) the reseacher's timing in providing the copyright owner with the results of the research.[312]

Security testify is defined as "accessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network."[313] Likewise, it is not a violation of the DMCA to "develop, produce, distribute or employ

305. *See id*. § 1201(a)(2), (b)(1)(A).
306. *Id*. § 1201(d)-(j).
307. *Id*. § 1201(g).
308. *Id*. § 1201(j).
309. *Id*. § 1201(g)(1)(A).
310. *Id*. § 1201(g)(2)(A)-(D).
311. *Id*. § 1201(g)(3)(A)-(C).
312. *Id*.
313. *Id*. § 1201(j)(1).

technological means for the sole purpose of performing the acts of security testing."[314] Security testing, unlike encryption research, need only refrain from violating any other laws (such as the Computer Fraud and Abuse Act)[315] to avoid violating the DMCA.[316] Two factors indicate whether a person qualifies for the security testing provision.[317] The factors to be considered are whether the information derived from the security testing was used "solely to promote the security of the owner or operator . . . or shared directly with the developer" of the computer or computer system at issue, and "whether the information derived from the security testing was used or maintained in a manner that [did] not facilitate [copyright] infringement," breach of security or invasion of privacy.[318] The inclusion of a security testing provision tends to support the argument that the DMCA can be applied outside of the context of digital rights technologies designed specifically for copyrighted works.

The encryption research and security testing exemptions offer no certain protection to computer security publishers. At the outset, the encryption research exemption will only apply to exploits which circumvent some kind of encryption system.[319] Publishers must also make a good faith attempt to obtain authorization.[320] As there appear to be no consequences if the authorization is not obtained, this could be viewed as a mere formality, but one which could snare unwary publishers.[321] Moreover, it is not clear whether a researcher must accept conditions on his or her authorization to remain in "good faith." It is not clear, for instance, whether a software vendor could require a researcher to sign a non-disclosure agreement as a condition to authorization to conduct research. This could seriously stifle encryption despite the exemption. The multifactor test for the encryption research exemption tracks the debate between limited-disclosure and full disclosure.

314. *Id*. § 1201(j)(4).
315. 18 U.S.C. § 1030 (2000).
316. 17 U.S.C. § 1201(j)(2).
317. *Id*. § 1201(j)(3)(A)-(B).
318. *Id*.
319. *See id*. § 1201(g)(1)(A).
320. *Id*. § 1201(g)(2)(C).
321. *See id*.

First, the test considers whether the publication generates more benefits to computer security than costs.[322] Also, the third factor in determining exemption indicates that it is necessary to inform the owner of work protected by the encryption of the research results before publicly announcing them.[323] Most disturbing of all, the second factor appears to restrict the availability of the exemption to those legitimately employed, trained or engaged in a course of study of encryption.[324] In a community where many computer security publishers carry out their activity in their private time and out of personal interest rather than by occupation, many otherwise worthy publications will not qualify for the security testing exemption.[325]

In the context of the security testing exemption, publishers are only protected where they distribute technological means of access for the sole purpose of conducting qualified security testing.[326] Publishers' inability to guarantee that their audience would use their publication "solely" for the purpose of investigating or eliminating vulnerabilities jeopardizes that qualification.[327] Moreover, the requirement that a security tester have authorization is onerous and restrictive.[328]

These two exemptions are also inherently uncertain because they require multifactor tests to determine whether a person qualifies for either exemption.[329] As these multifactor tests will only be applied by

322. *See id*. § 1201(g)(3)(A).

323. *See id*. § 1201(g)(3)(C).

324. *See id*. § 1201(g)(3)(B).

325. *See* Megan Carney, *Classifying Vulnerabilities (or Proving What You Already Knew), Impacts and Conclusions* [¶ 1] (Nov. 25, 2001) <http://www.software.umn.edu/~mcarney/> (accessed Oct. 3, 2002) (citing empirical study of the identities of those discovering vulnerabilities publicized by Computer Emergency Response Team (CERT) shows that private individuals and independent firms are the most prolific discoverers of vulnerabilities).

326. *See* 17 U.S.C. § 1201(j)(4).

327. *See id*. § 1201(j)(1).

328. Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 Berkeley Tech. L.J. 519, 545 (1999). "[M]any security flaws discovered in widely deployed systems have been found by researchers who tested the system without permission of either the owner or manufacturer of such systems." *Id*. *See* Don Oldenburg, *w00w00's Instant Message: Listen Up, AOL; Security Experts Discover Coding Hole, Leap In*, Wash. Post C1 (Jan. 05, 2002) (describing the difficutly independent researchers had getting AOL to provide a patch for a vulnerability in its instant messaging program).

329. This interpretation is supported by the mandatory nature of the word "shall" in

courts in the context of litigation or prosecution, there can be no *a priori* qualification for an exemption.[330] The security testing exemption factors would require courts to scrutinize the effect and distribution of the publication.[331] The requirement that courts consider whether the security testing was conducted "solely to promote the security of the owner or operator . . . or shared directly with the developer" and did not facilitate computer crime could restrict computer security publications to the general public where a publisher has knowledge that a publication might facilitate criminal activity.[332]

The DMCA can be interpreted to apply to computer security publications. It is unclear whether any individual publication would fall outside of the DMCA's scope or would qualify for an exemption. As previously discussed, the First Amendment does not stand as a barrier to liability from the DMCA.

2. *The Council of Europe Convention on Cybercrime*

The Convention on Cybercrime was completed and opened for signature on November 23, 2001.[333] It already has thirty two signatories, including the United States.[334] Article 6(1) of the Convention requires signatory states to forbid the production, distribution or procurement of "including a computer program, designed or adapted primarily for the purpose" of illegally accessing computers, intercepting data, or interfering with data or computer

the multifactor tests. *See Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 321 (S.D.N.Y. 2000) (citing that in determining whether one is engaged in good faith encryption research, the court is instructed to consider the multifactor test in 17 U.S.C. § 1201(g)(3)).

330. *Id*. at 319-20 (rejecting defendants' claims for encryption research and security testing exemptions).

331. *See* 17 U.S.C. § 1201(j)(1), (4).

332. *Id*. § 1201(j)(3)(A).

333. Council of Europe, *ETS No. 185—Convention on Cybercrime* (Nov. 23, 2001) <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> (accessed Oct. 3, 2002).

334. *See* CRS Report for Congress, *Cybercrime: The Council of Europe Convention* 2 (Apr. 26, 2002) <http://www.usembassy.it/pdf/other/RS21208.pdf> (accessed Oct. 3, 2002) (citing signatories that included Albania, Armenia, Austria, Belgium, Bulgaria, Croatia, Cyprus, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Republic of Macedonia, Malta, Moldova, the Netherlands, Norway, Poland, Portugal, Romania, Spain, Sweden, Switzerland, Ukraine, United Kingdom, Canada, Japan, South Africa and United States).

systems.[335] This covers exploits.[336] Moreover, the mere possession of such a device is required to by criminalized as well.[337] Thus, the Cybercrime Convention appears to require an element of criminalization beyond the DMCA.

Exceptions within the Convention exempt many exploits from criminalization. States are not required to criminalize production, distribution or possession of otherwise illegal devices where the activity is "not for the purpose of committing an offence . . . such as for the authorised testing or protection of a computer system."[338]

The Cybercrime Convention does require criminalization of exploits, but it does not require an exemption for testing or protection, although it permits it.[339] Nevertheless, the Cybercrime Convention

335. *See* Council of Europe, *supra* n. 333, art. 6(1)(a)(i).

336. Council of Europe, *Explanatory Report to the Convention on Cybercrime* ¶ 71 (Nov. 8, 2001) <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm> (accessed Oct. 3, 2002) ("As the commission of [cybercrime] often requires the possession of means of access ('hacker tools') or other tools, there is a strong incentive to acquire them for criminal purposes which may then lead to the creation of a kind of black market in their production and distribution.").

337. *Id*.

338. *Id*.;

> The drafters debated at length whether the devices should be restricted to those which are designed exclusively or specifically for committing offenses, thereby excluding dual-use devices. This was considered to be too narrow. It could lead to insurmountable difficulties of proof in criminal proceedings, rendering the provision practically inapplicable or only applicable in rare instances. The alternative to include all devices even if they are legally produced and distributed, was also rejected. Only the subjective element of the intent of committing a computer offence would then be decisive for imposing a punishment, an approach which in the area of money counterfeiting also has not been adopted. As a reasonable compromise the Convention restricts its scope to cases where the devices are objectively designed, or adapted, primarily for the purpose of committing an offence. This alone will usually exclude dual-use devices. . . .
>
> The offence requires that it be committed intentionally and without right. In order to avoid the danger of overcriminalisation where devices are produced and put on the market for legitimate purposes, e.g. to counter-attacks against computer systems, further elements are added to restrict the offence. Apart from the general intent requirement, there must be the specific (i.e. direct) intent that the device is used for the purpose of committing [the criminal offenses outlined in previous articles in the Convention].

Id. at ¶¶ 73, 76.

339. Council of Europe, *supra* n. 336, at [¶ 76].

provides a much clearer, broader and unconditioned exemption from liability for computer security publications than the DMCA.

3. *Traditional Inchoate Crimes and Miscellaneous Offenses*

Other theories of liability may apply to computer security publications as well. Georgia, Kansas and Mississippi have criminalized the disclosure of passwords, access codes and "other means of access."[340] Exploits often are means of access and their publication may cause liability under these statutes. Some theories assign liability to computer security publications on the basis of their context rather than their content. For instance, the wire and mail fraud statutes[341] have been used to prosecute the publication of "hacker tutorials," where the publication was part of a broader plan to defraud Bell South Telephone Company.[342]

As previously discussed, the First Amendment will not protect speech when it occurs in the context of aiding and abetting a crime or conspiracy.[343] Conspiracy has three elements: agreement to accomplish an illegal objective, coupled with one or more overt acts in furtherance of the illegal purpose, and the requisite intent to commit the substantive offense.[344] Conspiracy has a limited application to computer security publications—even where publication is an overt act and a computer security publisher has an intent to further a crime, agreement would be difficult to show. While conspiratorial agreements need not be explicit,[345] mere knowledge that a computer security publication may facilitate criminal activity, without cooperation, does

340. Ga. Code Ann. § 16-9-93(e) (2002); Kan. Stat. Ann. § 21-3755(c)(1) (2001); Miss. Code Ann. 97-45-5(1)(b) (2001).

341. 18 U.S.C. §§ 1341, 1343 (2000).

342. *U.S. v. Riggs*, 743 F. Supp. 556, 558 (N.D. Ill. 1990).

343. 18 U.S.C. § 371 (2000).

344. *U.S. v. Dahlstrom*, 713 F.2d 1423, 1429 (9th Cir. 1983); *see Direct Sales Co. v. U.S.*, 319 U.S. 703 (1943); *U.S. v. Falcone*, 311 U.S. 205 (1940); *U.S. v. Pinckney*, 85 F.3d 4, 8 (2d. Cir. 1996); *U.S. v. Blakeney*, 942 F.2d 1001, 1009 (6th Cir. 1991).

345. Mia V. Carpiniello & Abigail Roberts, *Federal Criminal Conspiracy*, 37 Am. Crim. L. Rev. 495, 498-99 nn. 21-22 (citing *U.S. v. Cassiere*, 4 F.3d 1006, 1015 (1st Cir. 1993) (holding agreement need not be express); *U.S. v. Scanzello*, 832 F.2d 18, 20 (3d Cir. 1987) (holding formal agreement not required); *U.S. v. Armstrong*, 16 F.3d 289, 293-94 (8th Cir. 1994) (stating "agreement need not be express or formal"); *U.S. v. Restrepo*, 930 F.2d 705, 709 (9th Cir. 1991) (stating that explicit agreement not required); *U.S. v. Hartsfield*, 976 F.2d 1349, 1354 (10th Cir. 1992) (concluding formal or express agreement not required)).

not satisfy the agreement element of conspiracy.[346] Even the Department of Justice has conceded "as a general matter, the requisite agreement cannot be proved simply by demonstrating that a person has provided a product to another person knowing that the product would be used in the commission of a crime, where the provider of the product is indifferent to its subsequent use."[347] It is not enough that a speaker's intended audience have criminal proclivities for conspiracy liability—some sort of meeting of the minds must be reached.[348] No agreement, legal or illegal, is possible where the publisher's audience does not communicate with the publisher. General publication on the Internet, without more interaction with the audience, does not provide the basis for holding a computer security publisher liable.

Aiding and abetting crime has but two elements: "knowing aid to persons committing federal crimes, with the intent to facilitate the crime."[349] Aiding and abetting has a much stronger application to computer security publication. In *Nye & Nissan v. United States*, the Supreme Court adopted the standard articulated by Judge Learned Hand: To be guilty of aiding and abetting, a defendant "in some sort associate himself with the venture, that he participate in it as something that he wishes to bring about, that he seek by his action to make it succeed."[350] While a publisher must have an intent to facilitate a crime, it is not required that a publisher accused of aiding and abetting know who uses the publication to facilitate computer crime or how it is used.[351] Liability for aiding and abetting results from the existence of "a community of intent between the aider and abettor and the principal."[352] Once that community of intent is established, however,

346. *Direct Sales*, 319 U.S. at 711-12.

347. U.S. Dept. of J., *supra* n. 176, at § IV(A) (citing *Direct Sales*, 319 U.S. 703; *Falcone*, 311 U.S. 205 (1940); *U.S. v. Blankenship*, 970 F.2d 283 (7th Cir. 1992).

348. *Id*.

349. *C. Bank, N.A. v. First Interstate Bank, N.A.*, 511 U.S. 164, 181 (1994) (citing *Nye & Nissan v. U.S.*, 336 U.S. 613, 619 (1994)).

350. 336 U.S. at 619 (quoting *U.S. v. Peoni*, 100 F.2d 401, 402 (2d Cir. 1938)).

351. *Russell v. U.S.*, 222 F.2d 197, 199 (5th Cir. 1955) (stating it is "not essential that the accessory know the modus operandi of the principal"); *U.S. v. Lane*, 514 F.2d 22, 27 (9th Cir. 1975) (citing that it is not necessary that the person accused of aiding and abetting "know all the details of the crime . . . " or "all the persons who were perpetrating the crime").

352. *U.S. v. Moore*, 936 F.2d 1508, 1527 (7th Cir. 1991) (quoting *U.S. v. Torres*, 809 F.2d 429, 433 (7th Cir. 1987) (quoting *U.S. v. Austin*, 585 F.2d 1271, 1277 (5th Cir. 1978))).

an aider-abettor "is liable for any criminal act which in the ordinary course of things was the natural or probable consequence of the crime that he advised or commanded, although such consequence may not have been intended by him."[353] Unlike conspiracy, a computer security publisher need not agree with the principal to be liable under aiding and abetting. All that is required is an intent that the audience use the publication to facilitate criminal activity.[354]

To summarize, First Amendment protection for computer security publications is uncertain. In the proper context, even natural language publications could be found liable either criminally or civilly. Aiding and abetting and, to a lesser degree, conspiracy implicate all forms of computer security publications. Moreover, it is not settled that computer code is classified as speech and merits First Amendment protection. Even where it does, it can be regulated on the basis of its content, because its content has an inherently functional aspect. The DMCA and other computer code regulations could have a serious impact on the publication of exploits, whether in source code or binary code, regardless of the context or the publisher's intent.

IV. IN SEARCH OF AN EFFICIENT RULE OF LIABILITY FOR COMPUTER SECURITY PUBLISHERS

In at least the last thirty years, the dominant ideology behind American jurisprudence has been law and economics. The seminal explanation of law and economics is Ronald Coase's *The Problem of Social Cost*.[355] That article stated a principle of efficient allocation of liability underlying law and economics.

> The problem which we face in dealing with actions that have harmful effects is not simply one of restraining those responsible for them. What has to be decided is whether the gain from preventing the harm is greater than the loss which would be suffered elsewhere as a result of stopping the action which produces the harm.[356]

353. *U.S. v. Barnett*, 667 F.2d 835, 841 (9th Cir. 1982) (quoting *Russell*, 222 F.2d at 199).

354. *Id*.

355. R.H. Coase, *The Problem of Social Cost*, 3 J.L. & Econ. 1 (1960).

356. *Id*. at 27.

The problem posed by computer security publications can be precisely addressed with the same principle. The question is not whether an individual publication causes more harm than good, it is whether a particular rule of liability governing computer security publications causes more harm than good.

Fixing liability on the least cost avoider is a related maxim of law and economics. This approach favors placing liability on the party best able to bear that burden: "[t]his is not so much a matter of [the parties'] respective wealth. . . . Rather it is a matter of [the parties'] capacity to absorb the loss or avoid it."[357] Capacity to absorb loss is an important factor in fixing liability. Large commercial enterprises are better able to distribute losses through prices and rates. As a practical matter, plaintiffs are more likely to recoup serious losses from large commercial enterprises than individuals who may be without significant assets. However, the most efficient determinant of liability is the ability to avoid loss in the first place. Guido Calabresi and Jon Hirschoff's seminal article, *Toward a Test for Strict Liability in Torts*, articulated law and economic's rule of efficient allocation of liability.[358]

> The question for the court reduces to a search for the cheapest cost avoider. . . .
>
> The cheapest cost avoider has been . . . defined as the party "an arbitrary initial bearer of accident costs would (in the absence of transaction and information costs) find it most worthwhile to 'bribe' in order to obtain that modification of behavior which would lessen accident costs most."[359]

357. William L. Prosser, *The Law of Torts* 22 (4th ed., West 1971);

> The defendants in tort cases are to a large extent public utilities, industrial corporations, commercial enterprises, automobile owners, and others who by means of rates, prices, taxes or insurance are best able to distribute to the public at large the risks and losses which are inevitable in a complex civilization. Rather than leave the loss on the shoulders of the individual plaintiff, who may be ruined by it, the courts have tended to find reasons to shift it to the defendants.

Id.

358. Guido Calabresi & Jon T. Hirschoff, *Toward a Test for Strict Liability in Torts*, 81 Yale L.J. 1054 (1972).

359. *Id.* at 1060 n. 19.

Substitute accident costs with computer crime costs, and the same analysis above can be used to construct an efficient rule of liability for computer security.

Section IV examines the ability of four parties to avoid computer crime costs: computer criminals, network administrators, software vendors and computer security publishers—in decreasing order of proximity to the crime. This analysis has a particular eye for the role that software vulnerabilities play in computer crime and the legal impediments to efficient allocation of liability. Section IV discusses the possibility that software vendors or network administrators might seek to distort the market for security to their advantage by shifting liability to computer security publishers. Finally, this section applies Coase's analysis to search for the economically optimal rule of liability for computer security publications.

A. *COMPARISON OF COMPUTER CRIMINALS, NETWORK ADMINISTRATORS, SOFTWARE VENDORS AND COMPUTER SECURITY PUBLISHERS AS THE CHEAPEST COST AVOIDERS*

Computer criminals perpetrate damage directly. Administrators own, operate or are otherwise responsible for inadequately secured computers. Software vendors distribute software laden with vulnerabilities. Computer security publishers facilitate computer crimes through their publications. All have some part to play in the exploitation of a computer security vulnerability.

Computer criminals are the lowest cost avoiders of computer crime and computer torts.[360] For their part, avoidance of computer security costs is a matter of refraining from action, rather than incurring costs of affirmative action. To the extent that computer crime fails to generate benefits, there are no costs imposed when computer criminals refrain from criminal activity. "Bribing" computer criminals, as Calabresi might argue, would restrain computer crime at its source; no other consideration would counterbalance the "bribe" than the

360. Calkins, *supra* n. 53, at 190-93 (applying Kaplow-Shavell and traditional economic models of analysis to the Computer Fraud and Abuse Act). Calkins' article provides a thorough comparison of regulatory alternatives to criminalization of unauthorized computer access, including pure self-help, decriminalization, and tort liability for hackers themselves, third parties with negligently inadequate security and private security providers. Calkins concludes that the most efficient regime will include criminalization.

computer criminals' motivation. However, if criminalization is not an adequate response by the legal system, it is because computer crime is rarely detected, rarely reported, and it is difficult to identify and apprehend its perpetrators.[361]

Several commentators have proposed holding network administrators liable when their negligent failure to secure the computers under their control either allows computer criminals access to third party data stored there or permits computer criminals to stage an attack on third party networks.[362] Administrators are the next lowest cost avoider after computer criminals. "Bribes" to administrators to increase their security would be counterbalanced by the administrators' inertia and whatever the costs of adopting adequate security. Allocating liability on network administrators provides some incentive to adopt non-negligent levels of security.[363] Likewise, a comparative negligence rule would give third-party victims incentive to adopt an appropriate level of security.[364] In turn, the barriers to computer crime would rise and the population of effective computer criminals would shrink, as the Internet becomes more and more secure.[365] Several problems become evident when considering allocating liability on network administrators. As Calkins notes, it would be a practical impossibility to fix one standard of care on the wide community of network administrators (which includes major corporations as well as home broadband subscribers).[366] The concern

361. *See* Levy, *supra* n. 38 (describing detection rates of about one percent and rates of reporting to law enforcement authorities of less than twenty percent).

362. *See* Brooks, *supra* n. 53; Calkins, *supra* n. 53, at 214-18; Faulkner, *supra* n. 53; Gripman, *supra* n. 55, at 179-82.

363. Calkins, *supra* n. 53, at 215 n. 213 (citing Todd Spangler, *Home Is Where the Hack Is* Interactive Week (Apr. 10, 2000) (available in 2000 WL 4065803), which described a class-action suit filed against Pacific Bell by its broadband customers after discovering "that enabling Windows file sharing allowed outside hackers to readily access their computers"); Gripman, *supra* n. 55, at 179.

364. Gripman, *supra* n. 55, at 193-94.

365. Calkins, *supra* n. 53, at 216.

366. *Id.* at 220 (citing Brooks, *supra* note 53, at 360-65, for the proposition that security standards are still evolving and judicial standards have only been articulated for service providers in the areas of copyright and defamation).

> [P]ersonal users certainly should not be required to establish military-grade systems. . . .
>
> . . .
>
> [W]hile an individual connected to the Internet via a cable modem may be required to purchase a commercially available personal computer software

that holding administrators liable for negligence will cause overinvestment in security or over penalize administrators (who are, after all, victims as well in this scenario) gives one pause.[367] Nevertheless, courts have enjoined computer systems from connecting to the Internet when they were found to be unacceptably insecure.[368]

This concern becomes a stronger consideration when evaluating the important role software vulnerabilities play in computer crime. Administrators and software vendors would seem to share responsibility for patching vulnerabilities. As vulnerabilities are identified, vendors should have some responsibility to respond and issue patches in a timely manner. As patches are issued, administrators should have some responsibility to collect and apply them in a timely manner. However, at some point the burden of applying patches on administrators becomes unreasonable, and the administrator may be excused for failing to apply patches.[369]

At the point the cost of securing software outstrips the costs of writing secure software, the software vendor becomes the next cheapest cost avoider of computer crime to the computer criminal.[370]

> firewall and to install readily available software patches, a research university connecting hundreds of workstations to the Internet might be required to do significantly more.

Stephen E. Henderson & Matthew E. Yarbrough, *Suing the Insecure?: A Duty of Care in Cyberspace*, 32 N.M. L. Rev. 11, 17, 21 (2002).

367. *Id*. at 216 (noting that "[f]orcing all middlemen to conform to a high security standard would thus be inefficient because some middlemen would have to over invest in security and might even be driven from the market due to an inability to pay").

368. *See* Bruce Schneier, *Crypto-Gram Newsletter: Judges Punish Bad Security* [¶¶ 15, 16] (Dec. 15, 2001) <http://www.counterpane.com/crypto-gram-0112.html> (accessed Oct. 7, 2002) (describing two court cases where injunctions forced defendants off the Internet until their security could be established, including the injunction against the Department of Interior discussed by Balaran *supra*, note 46).

369. Jeffrey Benner, *It's a Dread to Patch Code Red* [¶¶ 8-10] (Aug. 3, 2001) <http://www.wired.com/news/infostructure/0,1377,45763,00.html> (accessed Oct. 7, 2002) (considering the response of a Microsoft employee to a claim that it was necessary to read seventy eight security bulletins to secure Microsoft NT 4.0 against Code Red, a Microsoft employee stated: "I don't think things are nearly as bad as you are making them out to be. . . . Following the instructions, it boils down to installing the latest software for three packages, installing the SRP [Security Rollup Package], following six workarounds and applying three patches"). *Id*. at [¶ 10].

370. Brian Fonseca & Tom Sullivan, *Virus Sounds Industry Code Red*, 23 InfoWorld 33 (Aug. 13, 2001); Robert Bryce, *Hack Insurer Adds Microsoft Surcharg*e [¶¶ 1, 5] (Aug. 19, 2001) (on file with *Whittier Law Review*) (stating that a nascent response by the insurance industry to high costs of securing certain software may be emerging. J.S.

Allocating liability on software vendors will provide an incentive to write software which is not negligently insecure. To extend Calabresi's analysis, "bribing" software vendors achieves computer security when it surmounts the inertia of vendors and covers the costs of writing software which can be secured reasonably. While the costs of writing secure software are substantial, they must be compared against the duplicative costs of every user securing the system with a patch. While there is a dearth of empirical information about these costs, at some point it is efficient to shift liability to the software vendor.

However, allocating liability for software vendors is not straight forward. The economic loss doctrine has serious implications on holding software vendors liable for negligently insecure software. Software manufacturers are the favored sons of contract, product liability and tort law: the economic loss doctrine limits damages against software vendors to the terms of the license, usually to the price of the software itself.[371] The underlying rationale for the economic loss doctrine is the "concern that product liability claims could circumvent the objectives of the [Uniform Commercial Code]."[372] This concern was repeated by the Supreme Court in *East River Steamship Corporation v. Transamerica Delaval, Inc.*:

> The expectation damages available in warranty for purely economic loss give a plaintiff the full benefit of its bargain by compensating for foregone business opportunities. . . .

Wurzler Underwriting Managers increased computer security insurance rates by up to 15 percent for policyholders that use Microsoft's Internet Information Server). Wurzler based the increase on more than 400 security analyses done by the firm over the past three years and on the relative diligence of different operating systems' administrators in applying security patches. *Id*.

371. *See* Donald R. Ballman, *Software Tort: Evaluating Software Harm by Duty of Function and Form*, 3 Conn. Ins. L.J. 417 (1997);

> An unlikely combination of arcane and outdated case law, provisions of the Uniform Commercial Code and U.S. copyright laws effectively shield software manufacturers from the standard of care reasonably expected from all other manufacturers. Often, the only liability the software manufacturer faces is replacement of defective software or payments not to exceed the original licensing fees (sale price).

Id. at 420.

372. Steven C. Tourek et al., *Bucking the "Trend": The Uniform Commercial Code, the Economic Loss Doctrine, and Common Law Causes of Action for Fraud and Misrepresentation*, 84 Iowa L. Rev. 875, 887 (1999) (citing *E. River Steamship Corp. v. Transamerica Delaval, Inc.*, 476 U.S. 858, 871 (1986)).

> A warranty action also has a built-in limitation on liability, whereas a tort action could subject the manufacturer to damages of an indefinite amount. The limitation in a contract action comes from the agreement of the parties and the requirement that consequential damages, such as lost profits, be a foreseeable result of the breach. . . .
>
> In products-liability law, where there is a duty to the public generally, foreseeability is an inadequate brake. . . . Permitting recovery for all foreseeable claims for purely economic loss could make a manufacturer liable for vast sums.[373]

The economic loss doctrine limits damages to the cost of the product only "[w]hen a product injures only itself."[374] It does not apply when the product causes personal injury or physical harm,[375] or when the product causes damage to property, "other than the product itself, that was not readily foreseeable or anticipated by the parties" when the product was sold.[376]

Hopes that the "other property" exception would encompass the damage to data permitted by negligently insecure software would be undermined by *Transport Corporation of America v. International Business Machines, Inc*.[377] In *Transport*, IBM leased a computer system which tracked the customer's shipping and inventory data on a customer's computers.[378] When the system's software malfunctioned, valuable data was lost and the downtime imposed serious costs on *Transport*'s business.[379] IBM raised the economic loss doctrine when it was sued. *Transport* held that loss of data from the defective software was not "other property," because the data on the disk drive was integrated into the computer system.[380] "[W]here a defect in a component part damaged the product into which that component was incorporated, economic losses to the product as a whole were not losses

373. 476 U.S. at 873-74.

374. *Id*. at 871.

375. *See* Tourek et al., *supra* n. 372, at 889 (citing Reeder R. Fox & Patrick J. Loftus, *Riding the Choppy Waters of East River: Economic Loss Doctrine Ten Years Later*, 64 Def. Couns. J. 260, 262-63 (1997)).

376. *Id*. at 890.

377. 30 F.3d 953 (8th Cir. 1994).

378. *Id*. at 955.

379. *Id*. at 955-56.

380. *Id*. at 956.

to 'other property.' "[381] *Transport* has been followed in similar circumstances.[382] It is not clear to what extent *Transport* is distinguishable from the contemporary situation where software is often purchased separately from the computer; it seems that the software would be a product in itself, rather than a component incorporated into the entire computer.[383]

In sum, the economic loss doctrine casts doubt over the liability of a software vendor for software that cannot be reasonably secured. While software vendors are the cheapest cost avoider of computer crime in some circumstances, they may well escape liability because of the vagaries of American tort law.

B. *LIABILITY-SHIFTING THREATENS THE MARKET FOR COMPUTER SECURITY*

There is a risk that software vendors and administrators would engage in rent-seeking behavior by suppressing computer security publications and reducing the demand for security. Administrators could reduce the costs of maintaining secure computers. Security would not be a factor in the competition between software vendors. Without verifiable, independent evaluations of the security of their software, vendors face reduced overall competition. Administrators

381. *Id*. at 957 (citing *Minneapolis Socy. of Fine Arts v. Parker-Klein Assocs. Architects, Inc.*, 354 N.W.2d 816, 820 (Minn. 1984); *Rockport Pharmacy, Inc. v. Digital Simplistics, Inc.*, 53 F.3d 195 (8th Cir. 1995) (as discussed in India S. Nicholson, Student Author, *Rockport Pharmacy v. Digital Simplistics, Inc.: Viewing Economic Loss and Computers with Raised Eyebrows*, 6 J. Pharmacy & Law 69, 74 (1997)).

382. *See Rockport Pharmacy, Inc.*, 53 F.3d at 198 (citing failure of a customized computer system, including hardware and software, which destroyed data, did not fall into "other property" exception to economic loss doctrine); Nicholson, *supra* n. 381; Daniel T. Perlman, *Who Pays the Price of Computer Software Failure?*, 24 Rutgers Computer & Tech. L.J. 383, 395-97 (1998).

383. *Cf. Heidtman Steel Prods., Inc. v. Compuware Corp*., 164 F. Supp. 2d 931, 938-39 (N.D. Ohio 2001) (citing economic loss doctrine does not apply to provision of computer system, because it is a service); *Montgomery County v. Microvote Corp.*, 2000 WL 134708 (E.D. Pa. Feb. 3, 2000) (citing county's negligence and negligent misrepresentation claims against vendor corporation and manufacturer of allegedly defective electronic voting machines were barred by economic loss doctrine, precluding recovery in tort); *Peerless Wall & Window Coverings, Inc. v. Synchronics, Inc.*, 85 F. Supp. 2d 519 (W.D. Pa. 2000) (citing economic loss doctrine applies to software developer who provided defective software, but whose license restricted damages).

and vendors could suppress computer security publications through litigation and the threat of litigation. This would shift liability from negligent administrators and vendors with insecure software to the publishers that exposed these problems. However, there is likely to be an imbalance among the litigation capabilities of major software vendors and major system administrators and individual publishers.

Corporations have used even dubious theories of liability to silence critics in order to further corporate goals. These suits are often called "strategic lawsuits against public participation" (SLAPPs). It is not an uncommon tactic for powerful institutions, such as corporations, to file meritless lawsuits to silence their critics.[384] Speaking of litigation as a tactic to suppress speech, one court has said: "Short of a gun to the head, a greater threat to First Amendment expression can scarcely be imagined."[385] Unfortunately, it is a tactic that has seen increased application in recent times.[386] Computer security publications would suffer doubly from such litigation. As discussed above, the First Amendment would not protect all publications, and the indeterminacy of First Amendment protection would surely deter some publications that would be protected.

Over the long term, the suppression of computer security publications deprives computer security consumers of information necessary to distinguish between products. One limited empirical study showed that most vulnerabilities are found by researchers independent of the software vendor.[387] Without independent publications, the market for security would be restricted to two forms

384. *See* George W. Pring & Penelope Canan, *Slapps: Getting Sued for Speaking Out* 3-8 (Temple U. Press 1996) (explaining SLAPPs is an acronym, coined by Pring and Canan, for "strategic lawsuits against public participation"). Although their book addresses speech protected by the Petition Clause, the common understanding of SLAPPs has expanded to phenomenon outside the narrow scope of the original definition to any lawsuit where the costs of litigation are intended to deter speech, even if the litigation is baseless. *Id*.

385. *Gordon v. Marrone*, 155 N.Y. Misc. 2d 726, 736 (N.Y. Sup. Ct. 1992).

386. *See e.g.* Joshua R. Furman, Student Author, *Cybersmear or Cyber-SLAPP: Analyzing Defamation Suits Against Online John Does as Strategic Lawsuits Against Public Participation*, 25 Seattle U. L. Rev. 213 (2001); Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation and Discourse in Cyberspace*, 49 Duke L.J. 855 (2000); David L. Sobel, *The Process that "John Doe" is Due: Addressing the Legal Challenge to Internet Anonymity* 5 Va. J.L. & Tech ¶ 3 (2000) (available at <http://www.vjolt.net/vol5/symp2000/v5i1a3-Sobel.html> (accessed Oct. 7, 2002)).

387. *See* Carney, *supra* n. 325, at [¶¶ 4-5].

of information: information from vendors and information from victims of completed attacks. Information provided by vendors is not likely to contribute to an objective evaluation of their product. Perpetuating the perception that their products are secure increases and promotes profits.[388] Issuing patches undermines that perception and increases costs. Vendors have an incentive to refrain from creating and issuing patches in the absence of independent computer security publications.[389] Information from victims of completed attacks is also inadequate: many attacks will not be discovered, and many discovered attacks will not be reported,[390] in part because administrators have incentives to avoid reporting security violations. Any individual firm disclosing security violations would compare disfavorably to the rest of their competition in the minds of the public, even though the rate of security violations was uniform. Moreover, users and administrators are denied the opportunity for advance notice of vulnerabilities. There is no way to learn about vulnerabilities for which exploit code has not been developed without independent computer security publications. In their absence, users are entirely reliant on the vendor to inform them of the possibility of a vulnerability and to provide them with a means of preventing an attack.

Ultimately, suppression of computer security publications will distort the market for security by depriving security consumers the ability to distinguish between products. In the absence of a clear, efficient market for it, computer security will be neglected or will decline. Where legal action supplements or substitutes for computer security, it also reduces the incentive to develop effective security. There has been a suggestion that the makers of CSS understood ahead of time that their encryption was deeply flawed.[391] Some of the digital

388. *Id*. at [¶¶ 4-5].

389. *Id*.

390. *See* Mitchell & Banker, *supra* n. 43, at 708.

391. Cryptome.org, *Critique of DVD DeCSS Claims* [¶ 16] (Jan. 3, 2000) <http://cryptome.org/dvd-bogk.htm> (accessed Oct. 7, 2002) (citing one of the correspondents for the Linux community observing the *Reimerdes* case and recounting his discussion of the encryption with one of the designers of the encryption:

> [T]hey *knew* about the weaknesses. At [a computer] security conference in Berlin, I've [sic] talked to the guy from Intel who designed the key management mechanism for DVD . . . and asked him if he didn't consider the 40 bit keylength a little weak. His answer was (and this was before the DeCSS release, and before public analysis) that there's a 2^16 attack on the bulk cipher, and that his part of the scheme was one of the strongest parts

rights technologies produced by Adobe and broken by Dimitry Sklyarov and Elcomsoft were also apparently quite poor.[392]

The threat of retaliatory litigation has become less theoretical and more material every day. When an exploit affecting HP's (formerly Hewlett-Packard) Tru64 server was published, HP warned (then relented) the publishers that they could be civilly and criminally liable under the DMCA.[393] The publishers informed HP of the exploit and waited for three months for HP to issue a patch for the exloit before finally publishing the exploit.[394] HP promised to issue a patch within 48 hours after the exploit was published.[395] It is also disturbing that some publications have already been withheld[396] or published pseudonymously[397] for fear of legal retribution.

> overall, and that the DVD Consortium knows about this. [Emphasis in original].

Id.

392. Bruce Perens, *Dimitry Sklyarov: Enemy or friend?* [¶ 3] (Aug. 1, 2001) <http://zdnet.com.com/2100-1107-530420.html> (accessed Oct. 7, 2002);

> [I]t turns out that the encryption software of at least two manufacturers is so weak that it can be broken instantly. One publisher, Sklyarov found, uses a cypher called rot13 that has been known since Caesar's time. An encryption vendor uses a cypher so weak that programmers refer to it as the "Hello World" of cryptography programs, and another embeds code key information in the document, so that the key can be found and used to unlock the document instantly.

Id.

393. George V. Hulme, *HP Threatens Legal Action Against Security Group; Researchers May Become Reluctant to Publicize Vulnerabilities* [¶ 2] (Aug. 5, 2002) <http://www.informationweek.com/story/IWK20020802S0033> (accessed Oct. 7, 2002).

394. *Id*. at [¶ 7].

395. *Id*.

396. *See* Niels Ferguson, *Censorship In Action: Why I Don't Publish My HDCP Results* [¶¶ 6-7] (Aug. 15, 2001) <http://www.macfergus.com/niels/dmca/cia.html> (citing encryption research discussing his decision not to release attack on High-bandwidth Digital Content Protection encryption scheme developed by Intel) (accessed Oct. 7, 2002).

397. *See* Amy Harmon, *Programmer Exposes Microsoft Flaws*, N.Y. Times C11 (Oct. 23, 2001); Wade Roush, *Breaking Microsoft's e-Book Code* [¶¶ 2-3] (Nov. 2001) <http://www.technologyreview.com/articles/innovation11101.asp> (accessed Oct. 7, 2002); "Beale Screamer," *Microsoft's Digital Rights Management Scheme—Technical Details* (Oct. 18, 2001) <http://cryptome.org/ms-drm.htm> (accessed Oct. 7, 2002) (discussing the security flaws in Microsoft's digital rights technology incorporated into the Windows Media Player).

Moreover, it has proven difficult in the past to secure safe ground to publish. Edward Felten, a computer science professor, had found a technique that circumvented the technology used by the Secure Digital Music Initiative.[398] Upon discovering that Felten intended to present his work at a scientific conference,[399] counsel for the Recording Industry Association of America wrote a letter that suggested the dangers of presenting his work: "[P]ublic disclosure of [this] research . . . could [render Felten] subject to enforcement actions under federal law, including the DMCA."[400] Felten delayed the presentation of his work until he had filed a declaratory action against the Recording Industry Association of America and the Department of Justice, seeking an injunction that the DMCA was unconstitutional as applied to his presentation. The court found that Felten lacked standing, as any controversy between the parties was not ripe, and Felten's fear of prosecution and litigation was not reasonable.[401]

398. Edward W. Felten, *Statement Regarding the SDMI Challenge* [¶ 3] (2001) <http://www.cs.princeton.edu/sip/sdmi/announcement.html> (accessed Oct. 7, 2002).

399. Edward W. Felten, *Statement, SDMI Message* [¶¶ 3-4] (Apr. 26, 2001) <http://www.cs.princeton.edu/sip/sdmi/sdmimessage.txt> (accessed Oct. 7, 2002) (read at the Fourth International Information Hiding Workshop, Pittsburgh, Pa., April 26, 2001);

> [T]he Recording Industry Association of America, the SDMI Foundation, and the Verance Corporation threatened to bring a lawsuit if we proceeded with our presentation or the publication of our paper. Threats were made against the authors, against the conference organizers, and against their respective employers.
>
> Litigation is costly, time-consuming, and uncertain, regardless of the merits of the other side's case. Ultimately we, the authors, reached a collective decision not to expose ourselves, our employers, and the conference organizers to litigation at this time.

Id. at [¶¶ 3-4]; *see* Electronic Frontier Foundation, *EFF's & Professor's First Amended Complaint in Felten v. RIAA* (June 26, 2001) <http://www.eff.org/sc/felten/20010626_eff_felten_amended_complaint.html> (accessed Oct. 7, 2002); Edward Felten, *Status of the Paper "Reading Between the Lines: Lessons from the SDMI Challenge"* (Aug. 15, 2001) <http://www.cs.princeton.edu/sip/sdmi/> (accessed Oct. 7, 2002).

400. Matthew J. Oppenheim, *RIAA/SDMI Letter* [¶ 5] (April 19, 2001) <http://www.cs.princeton.edu/sip/sdmi/riaaletter.html> (accessed Oct. 7, 2002).

401. Electronic Frontier Foundation, *Final Hearing Transcript, Felten v. RIAA* (Nov. 28, 2001) <http://www.eff.org/sc/felten/20011128_hearing_transcript.html> (accessed Oct. 7, 2002). "The plaintiffs liken themselves to modern Galileos persecuted by authorities. I fear that a more apt analogy would be to modern day Don Quixotes feeling threatened by windmills which they perceive as giants." *Id*. at 26.

The Tru64 and Felten matters show that publication-suppressing liability could be a matter of slow encroachment. Felten was prepared to defend himself, but few researchers can muster the same effort and resources. HP ultimately relented on its threats to take action under the DMCA this time, but there is no guarantee HP (let alone less forthright companies) will show similar restraint on a future occasion. Without those resources, veiled threats of litigation have much greater efficacy in silencing others. However, the threat of litigation does not stop the development of flawed software, nor does it stop vulnerability research.[402] It does restrict legitimate user's and administrator's access to information, however. That same restriction increases the advantage computer criminals derive from a publication.[403]

C. *CONCLUSIONS*

The key insight in Coase's analysis is that it is not whether a particular publication generates more benefits than losses. The question to be answered is whether a particular rule of liability for computer security publishers generates more benefits than losses. This is a subtle difference, as the efficiency of a rule of liability will largely be determined by the efficiency of the publications it punishes and deters, and those that it protects.

An efficient rule of liability for computer security publications considers not only every incident of computer crime the publication would facilitate, but also every incident of computer crime prevented because of the vulnerability patch or the vulnerable software being discarded or temporarily removed. Although the DeCSS decisions considered how DeCSS would facilitate crime, they did not consider how it would benefit DVD publishers. In that case, it is unlikely that such consideration would have changed the outcome, but a calculus based on a different set of facts could generate a different result. Security consumers will benefit greatly from an environment that permits them to distinguish between products of varying levels of security, as opposed to an environment where vulnerabilities are only identified after they are exploited.

402. *See* Schneier, *supra* n. 97, at 5-6 (citing security vulnerabilities are inherent in the software development process).

403. Houle & Weaver, *supra* n. 127, at 14-15.

All computer security publications provide information about security vulnerabilities. The nature of that information, and its utility to software users, varies with the publication, but it hinges on the communicative value of the publication. Patches obviously have the greatest utility to users, but are more difficult to produce without access to the software's source code. They also may fail to disclose the nature of the vulnerability. Natural language publications are most easily understood, but they may not describe the problem precisely. Their utility would then be diminished. Source code exploits can be compiled and used against software users, but they also provide a precise description of the problem. Even binary exploits have a utility for users: they confirm that a vulnerability exists and they can confirm that a patch is effective. Automated exploits, however, provide no additional useful information to users, but they have great utility for computer criminals.[404]

The totality of computer security publications' effects must be examined before assigning liability. These publications promote diligence. As administrators become responsive to vulnerabilities (perhaps out of liability, perhaps from market pressure), the likelihood of beneficial effect rises as patches are applied more diligently. The *Windows of Vulnerability* study showed that the main cause of vulnerability exploitation was the failure to apply available patches.[405] Likewise, this will probably instill responsiveness in vendors to introduce fewer vulnerabilities and produce more effective patches more quickly. Administrators will avoid software with higher security costs if they are informed of those costs. Demand for security will eventually force vendors to write more secure software. Unless courts recognize the utility of computer security publications, it is unlikely that an efficient market for computer security will ever arise.

404. *See supra* nn. 71, 135-138 and accompanying text.

405. Arbaugh, *supra* n. 66, at 58.