International Journal of Communications Law & Policy

Issue 9 - Special Issue on Cybercrime, Spring 2005

THE PRICE OF RESTRICTING VULNERABILITY PUBLICATIONS

By Jennifer Stisa Granick[†]

ABSTRACT

There are calls from some quarters to restrict the publication of information about security vulnerabilities in an effort to limit the number of people with the knowledge and ability to attack computer systems. Scientists in other fields have considered similar proposals and rejected them, or adopted only narrow, voluntary restrictions. As in other fields of science, there is a real danger that publication restrictions will inhibit the advancement of the state of the art in computer security. Proponents of disclosure restrictions argue that computer security information is different from other scientific research because it is often expressed in the form of functioning software code. Code has a dual nature, as both speech and tool. While researchers readily understand the information expressed in code, code enables many more people to do harm more readily than with the non-functional information typical of most research publications. Yet, there are strong reasons to reject the argument that code is different, and that restrictions are therefore good policy. Code's functionality may help security as much as it hurts it and the open distribution of functional code has valuable effects for consumers, including the ability to pressure vendors for more secure products and to counteract monopolistic practices.

INTRODUCTION

Today, attackers[1] can gain unauthorized access to computer systems, transmit harmful programs called "worms" and "viruses" that slow down the network, and send unwanted "spam" emails to other Internet users with apparent impunity. These problems did not exist before computer networks existed. But now, such network-only offenses pose a direct threat to privacy, business productivity and intellectual property assets.

There are calls from some quarters to restrict the publication of information about security vulnerabilities[2] in an effort to limit the number of people with the knowledge and tools needed to attack computer systems. Scientists in other fields have discussed similar

[†] Jennifer Granick is Executive Director of the Stanford Law School Center for Internet and Society and teaches the Cyberlaw Clinic. She teaches, speaks and writes on the full spectrum of Internet law issues including computer crime and security, national security, constitutional rights, and electronic surveillance. Granick came to Stanford after almost a decade practicing criminal defenselaw in California.

[1] The term "attacker" is the accurate one. "Hacker" traditionally means someone who uses a computer in unexpected ways, "artists, pioneers, explorers." *See, e.g.*, STEVEN LEVY, HACKERS: HEROES OF THE COMPUTER REVOLUTION (1984). More recently, the term is used to mean computer *criminals*, so people have adopted the awkward taxonomy of "white hat," "grey hat" and "black hat" hackers. These linguistic acrobatics are best avoided by restoring "hacker" to its original meaning and using "attacker" for those engaging in criminal behavior.

[2] "Vulnerability" is defined as "a flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy." SANS Glossary of Terms Used in Security and Intrusion Detection, Last updated May 2003, *at* http://www.sans.org/resources/glossary.php#V.

proposals and rejected them, or adopted only narrow voluntary restrictions. As in other fields of science, there is real danger that publication restrictions will inhibit the advancement of the state of the art in computer security. However, unlike research in other fields of science, computer security information is often expressed in code. Code has a dual nature, as both speech and tool. Would-be attackers can readily code from research publications. However, there are strong reasons to reject the argument that code is different, and that restrictions are therefore good policy.

Part One of this paper explains the current state of computer (in)security and sets forth three ways to restrict publications followed by the most common arguments for and against. It then illustrates the popularity of security publication restrictions with an overview of proposed and enacted publication restrictions. Part Two reviews the debate surrounding publication restrictions in other scientific fields and shows that, except in rare cases, policy makers and scientists agree that the strong interest in sharing, peer review and cooperation that is essential to the development of scientific knowledge outweighs the benefit to security interests attained from restraining publication. The law cannot regulate code without impacting research, so policy makers must decide whether any security gain from disclosure restrictions is worth the price. Part Three asks how computer security is different from other fields of science and whether these differences warrant a more or less restrictive approach to regulating vulnerability publications. The paper concludes that while the functionality of code superficially appears to be a strong factor in favor of limiting computer security publications, security is not improved by secrecy in the computer context. Additionally, code restrictions undesirably favor anti-competitive practices on the part of market actors in a networked economy. The public interest particularly benefits from openness in computer security.

PART ONE

I. THE STATE OF COMPUTER (IN)SECURITY

Computer insecurity is pervasive and apprehending criminals is difficult and expensive. Faced with this set of circumstances, some have proposed limiting disclosure of information about vulnerabilities on the grounds that potential attackers could use such information. Advocates of limited disclosure argue that controlling vulnerability information will reduce the number of people with the ability to attack, thereby reducing attacks.

Attacks need to be reduced. Approximately 60 percent of businesses suffer some kind of unauthorized computer use in a year.[3] Many of these security incidents are the result of flaws in software that allow unauthorized use or malicious interruptions in service. Security firm Symantec reports that 2,636 flaws were discovered in 2003 and 2,587 in 2002.[4]

[3] Lawrence A. Gordon, et al., *2004 CSI/FBI Computer Crime and Security Survey*, *at* http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf. This study has been sharply criticized for its methodology, but remains one of the only surveys of its kind.

[4] Press Release, Symantec Corporation, Symantec Internet Security Threat Report Tracks Rise in Blended Threats, Worms Targeting Corporate and Consumer Systems, Severe Attacks (March 15, 2004), *at* http://www.symantec.com/press/2004/n040315b.html.

A substantial number of flaws are not caught by whatever quality assurance processes software vendors implemented before placing software products in the market.[5] After-the-fact remedies are less than adequate at reducing the incidents of computer crime. Once the software product is in the market, security researchers, as well as potential attackers, examine and test it for security holes. When a researcher discovers a flaw[6] and notifies the vendor, the vendor may then decide to issue a patch, which customers must learn about, locate and properly install, if not pay for. Patches may not be sufficient, and often complicate matters further; they may break implementations of the software; create other vulnerabilities; contain untrusted code; or impose undesirable license terms. Customers sometimes do not install patches reliably, leaving machines vulnerable long after flaws are announced. Patching is an expensive and inefficient way to fix flaws.[7]

A majority of incidents of digital crime go unpunished. Law enforcement cites anonymity, the difficulties of working with international law enforcement, the fragility and dispersal of digital evidence, lack of training and lack of resources as reasons for the low prosecution rate.[8] Statistics from the Department of Justice suggest an additional determinative factor as to why computer crimes do not get prosecuted: despite the reported number of attacks and the publicity about computer crime, individual computer crime incidents tend to be relatively minor. In the aggregate, there's a problem. But each individual case appears not to be worth the trouble to prosecute. For example, spam is a serious annoyance for most Internet users, and imposes unwanted costs on Internet Service Providers (ISPs). However, an individual spammer may not cause any real harm to any one ISP or recipient.

In 2002, using data related to computer fraud[9] supplied by the Department of Justice to the Transactional Records Access Clearinghouse ("TRAC"),[10] Matthew Scherb, a Center for Internet and Society summer intern and graduate of Northwestern University Law School, performed a statistical analysis of DOJ enforcement actions. Scherb found that as of March 2002, the DOJ declined to prosecute 268 referrals (64

[5] The only known empirical study shows that most flaws are discovered in-house, but that external reports are a significant source (over 20%) of vulnerability information. TIINA HAVANA, COMMUNICATION IN THE SOFTWARE VULNERABILITY REPORTING PROCESS (2003) *at* http://www.ee.oulu.fi/research/ouspg/protos/sota/reporting/.

[6] If an attacker finds the flaw first, he probably will keep the information to himself, or to a close circle of friends. The information is only valuable so long as administrators of systems using the flawed software don't know about and don't do anything about the problem. If they are unaware of the problem, they can be attacked without realizing it.

[7] MARK G. GRAFF & KENNETH R. VAN WYK, SECURE CODING: PRINCIPLES AND PRACTICES 56 (2003) (arguing that patching is sixty times more expensive than fixing the flaw at the design stage).

[8] Steve Brown, *Catching Cyber Criminals Is Easier Said Than Done*, FOX NEWS, Dec. 9, 2003, *at* http://www.foxnews.com/story/0,2933,105214,00.html (last visited Nov. 22, 2004).

[9] The data were comprised of enforcement actions for violations of 18 U.S.C. §§ 1030 or 2701 *et seq.*, computer "bulletin boards" and other schemes in which a computer is the target of the offense, including when charged as violations of 18 U.S.C. §§ 1343, 2314, or 2319, e.g., computer viruses or where the defendant's goal was to obtain information or property from a computer or to attack a telecommunications system or data network.

[10] TRAC Reports, Inc, *TRACFED Criminal Enforcement Database*, *available at* http://tracfed.syr.edu/index/ crimindex.html.

percent) received during fiscal year 1998. The reasons for those declinations are shown in the table below.

Reason for Declinations	*No.*	*% of Declinations*	*% of Total Referrals*
Weak or insufficient admissible evidence	53	19.78%	12.71%
Lack of evidence of criminal intent	46	17.16%	11.03%
No known suspect	29	10.82%	6.95%
Minimal federal interest or deterrence value	24	8.96%	5.76%
Agency request	25	9.33%	6.00%
No evidence of federal offense	20	7.46%	4.80%
Suspect to be prosecuted by other authorities or on other charges	16	5.97%	3.84%
Lack of investigative or prosecutorial resources	11	4.10%	2.64%
Pre-trial diversion complete	7	2.61%	1.68%
Jurisdiction or venue problems	7	2.61%	1.68%
Juvenile suspect	6	2.24%	1.44%
Civil, administrative, or other disciplinary alternatives	6	2.24%	1.44%
Office policy (fails to meet prosecutorial guidelines)	6	2.24%	1.44%
Other	12	4.48%	2.88%

Approximately 23 percent of the cases were not pursuable for lack of resources, jurisdiction problems, or inability to identify a suspect. A large percentage of cases were not filed simply because it was not worth pursuing a federal criminal case.[11] This is not as surprising as it may first seem, given that the hoopla about computer crime often exaggerates the reality. Loss estimates often include intangibles like employee productivity and computer cycles, thus cost estimates are often wildly awry.[12] As an example, the mi2g consultancy firm estimated that January 2004's "mydoom" worm, which replicated by email and installed a backdoor in infected computers, cost businesses $38.5 billion.[13] In comparison, the National Climatic Data Center estimates that 2003's hurricane Isabel, which killed more than 40 people and was declared a major disaster, cost $4 billion.[14]

Since software is pervasively insecure and companies are not getting better at secure coding, and since the sources of unwanted network traffic are difficult to locate and regulate, some suggest regulating publishers of information about security vulnerabilities. Advocates of these proposals seek to keep information that could be used to compromise a computer system out of the hands of would-be attackers. A recent survey shows that receivers of vulnerability reports, including vendors and system administrators, tend to support limited vulnerability disclosure.[15]

[11] The author is working on a future paper on this topic, using a broader data set.

[12] The author is working on a future paper on this topic.

[13] Press Release, mi2g Limited, Mydoom Becomes Most Damaging Malware As SCO Is Paralysed (Feb. 1, 2004), *available at* http://www.mi2g.com/cgi/mi2g/press/010204.php.

[14] National Climatic Data Center, *Billion Dollar U.S. Weather Disasters, 1980-2003* (Feb. 3, 2004), *available at* http://www.ncdc.noaa.gov/oa/reports/billionz.html.

[15] Havana, *supra* note 5, at 56.

II. TYPES OF VULNERABILITY DISCLOSURE RESTRICTIONS

Advocates of limited disclosure focus on three areas for regulation: to whom disclosure should be made ("audience restrictions"), the timing of disclosure ("time restrictions") and the nature of the information disclosed ("content restrictions").

A. Audience Restrictions

Audience restrictions limit the entities to which vulnerability information is revealed, either permanently or in temporal stages. Advocates of audience restrictions say that there is no need for the general public to be informed of vulnerabilities until after they have been fixed. Rather, only trusted people should have access to information that might be abused. Then defenders would have the advantage of having more information than attackers.

Defenders clearly find vulnerability information valuable. Hundreds of thousands of people read Web pages and subscribe to mailing lists that report on vulnerabilities. The federal government funds, sponsors or participates in many information sharing networks including the CERT Coordination Center at Carnegie Mellon University[16] (federally funded), CERIAS at Purdue University[17] (federally funded), Infragard[18] (Federal Bureau of Investigation), the Department of Homeland Security's Information Assurance and Infrastructure Protection ("IAIP") Directorate[19] (consolidation of the Commerce Department's Critical Infrastructure Assurance Office and the FBI's National Infrastructure Protection Center), FedCIRC[20] (IAIP), the Computer Emergency Response Team[21] (Department of Defense), and the Computer Incident Advisory Capacity[22] (Department of Energy). Additionally, some companies now pay for vulnerability information.[23]

Audience restrictions would give certain industries critical information during the interim period after a flaw is discovered but before a patch or fix is created, the "window of vulnerability."[24] Banking, critical infrastructure and some government services are often cited as entities that would benefit from early information sharing. For example, the 2001 White House's proposal on cybersecurity, entitled the National Strategy to Secure

[16] http://www.cert.org

[17] http://www.cerias.purdue.edu

[18] http://www.infragard.net

[19] http://www.dhs.gov/dhspublic/display?theme=52&content=918.

[20] http://www.fedcirc.gov

[21] http://www.cert.mil

[22] http://www.ciac.org/ciac

[23] iDefense is one example of a firm that sells such information to its customers. *See* iDefense Website, *available at* http://www.idefense.com/

[24] The term comes from William A. Arbaugh, William L. Fithen, and John McHugh, *Windows of Vulnerability: A Case Study Analysis*, COMPUTER, Dec. 2000, at 52.

Cyberspace, heavily promoted information sharing between industry and government[25] while discouraging revelations of information to the general public.[26]

However, defenders who find vulnerability information valuable cannot be segregated from the general public in any principled way. Every business wants to be part of the circle of those "in the know." Why should some sectors qualify for membership and others fail? Once the vulnerability information is disclosed, leaks are inevitable. Worse, once some people know about a flaw, they have an edge over those who do not know. At this point the secrecy itself, not the information, may be the primary source of danger.

Additionally, audience restrictions are no assurance that attackers have not discovered the flaw through other means. Though the flaw has not been publicized, there is the possibility, if not probability, that someone other than the researcher has discovered the vulnerability.[27] It is conventional wisdom among computer security practitioners that there is no security through obscurity.[28] These discoverers may want to attack and will not report the flaw to the vendor, for fear that the vendor will fix the problem and the flaw will no longer be valuable to them. Discoverers may write exploit programs to take advantage of the flaw and may tell other potential attackers about the problem. While the public waits for a patch, these attackers can run amok and customers would not even know it. Audience restrictions exacerbate this problem by keeping valuable information out of the hands of defenders.

Whatever the security benefit of audience restrictions, it lasts only until the time the patch is published. If only the vendor is notified of the problem, and if all works properly, it will fix the flaw and produce a patch. Since customers patch patchily, some machines will remain vulnerable. And once a patch is available, potential intruders will know about the flaw. They can use the information provided with the patch, or reverse engineer the patch, to create a program to exploit the flaw. [29]

B. Time Restrictions

Time restrictions would give software vendors a period of time to patch flaws and users time to install the patches before the problems are more widely revealed. Proponents of delay argue that it is best to keep potentially dangerous information out of the hands of would-be attackers during the window of vulnerability. Opponents again

[25] NATIONAL STRATEGY TO SECURE CYBERSPACE 24 (2003), *available at* http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.

[26] *Id.* at 25.

[27] Matt Blaze, a research scientist at AT&T and professor at University of Pennsylvania, made this statement at the Stanford Center for Internet and Society Conference on CyberSecurity, Research, and Disclosure on November 23, 2003.

[28] The principle comes from the work of Auguste Kerckhoffs. See A. Kerckhoffs, *La Cryptographie Militaire*, JOURNAL DES SCIENCES MILITAIRES, Jan. 9, 1883, at 5-38, *available at* http://www.petitcolas.net/fabien/kerckhoffs/.

[29] *Cybersecurity and Vulnerability Management: Hearing Before the Subcomm. on Technology, Information Policy, Intergovernmental Relations and the Census, House Comm. on Government Reform*, 108th Cong. (2004) (statement of Scott Culp, Senior Security Strategist, Trustworthy Computing Team, Microsoft Corporation), *available at* http://www.microsoft.com/presspass/exec/ScottCu/06-02-04TestimonyWritten.asp.

argue that, at the point that any one researcher discovers some vulnerability, it is very likely that other researchers elsewhere around the globe have also discovered it. Certainly, the narrowing window of time between distribution of patches and creation of exploits means controlling information after the patch is issued is useless. The information attackers need is contained in the patch itself. Waiting to disclose information to defenders may be valuable, but only before a patch is issued and only if a significant number of attackers do not already have information about the vulnerability. There is no way to tell if some attackers already know about the vulnerability.

C. Information Restrictions

Information restrictions would limit the release of detailed descriptions of the flaw that might aid attackers hoping to gain unauthorized access to or interfere with computer systems. Proponents particularly want to restrict functional code that is capable of exploiting the vulnerability (exploit code), or code that specifically describes and demonstrates the vulnerability (proof-of-concept code), but which could also be the basis for an exploit. Under information restrictions, code would not be disclosed or would be disclosed to a limited audience, or would not be disclosed until a later time when a patch is available. The heart of the debate on information restrictions is the distribution of software code.

Code is the major way that computer security publications differ from publications in other scientific fields. Code is the language computer scientists use to convey ideas in an exact and scientific way.[30] Computer science professionals and academics use code examples to express ideas and inform readers in a clear and succinct way.[31] But code is also functional, a tool that can be used, possibly to attack a computer or break a security system. In other scientific fields, for example medicine, an explanation of how to synthesize polio does not endow an audience with the particular tools necessary to do so.

Still, code gives security defenders invaluable information about the nature of a security problem, information that only code can convey. Defenders can use proof-of-concept code to evaluate security techniques, test the effectiveness of patches and create intrusion detection signatures. Administrators can use the code to modify firewalls to better protect networks from the flaw. Security companies can use the information to improve security scanning programs. The existence of working exploit code can help vendors find the problem, motivate them to fix it expeditiously and educate coders about how not to repeat the same mistake.

Proponents feel that the benefits of code publication are reaped not by the general public, but only by highly knowledgeable people. More “bad guys” than “good guys” are empowered by its release, thus justifying restrictions. For example, Microsoft’s Director of Security, Steven Lipner, has opined that “the set of users that would use exploit code

[30] Universal City Studios, Inc. v. Corley, 273 F.3d 429, 445-446 (2d Cir. 2001).

[31] R.C. Fox, “Old Law and New Technology: The Problem of Computer Code and the First Amendment” 49 UCLA L. REV. 871, 879 (2002).

to protect themselves . . . is probably much smaller than the set of people who would be put at risk by it."[32]

Despite the precept that the reporting researcher is unlikely to be the only party aware of the vulnerability, many if not most security researchers have responded to arguments such as Lipner's by voluntarily adopting a policy of delaying publication of proof-of-concept code in situations where the vendor takes the time to actually fix the problem and issue a patch.[33] An early disclosure policy, developed by RFPolicy in 2000 and modified in 2001 by security researcher Rain Forest Puppy, encourages finders to reveal to vendors first and give them five days to respond, and then to continue to delay disclosure so long as the vendor is working on the problem and keeping in touch.

Also in 2001, the moderator of NTBugtraq, a mailing list devoted to security issues in Windows NT, released his own standards for responsible vulnerability disclosure. In 2003, the Organization for Internet Safety ("OIS"), a new organization of mostly U.S.-based vendors and researchers that include Microsoft, issued a disclosure policy that recommended waiting for 30 days.[34] Today, security groups including eEye, Nomad Mobile Research Centre, and Last Stage of Delirium, first alert the vendor and refrain from publishing full technical details to anyone but the vendor until it develops an advisory or a patch, regardless of how long it takes.[35]

Proponents of information restrictions say that since patching is an inadequate remedy for vulnerabilities, publishing code at any point in time is dangerous, with the danger diminishing over time as more people implement the patch. But while researchers may disagree on when to release functioning code, they mostly agree that, at some point, software code explaining the flaw is highly valuable for defenders and should be published.

Moreover, researchers remember that vendors historically have not been eager to take responsibility for flaws in their products. Many security experts believe that the threat of further disclosure may be the only thing that encourages vendors to issue patches.[36] If vendors fail to issue patches or otherwise fix the flaw, a concerned researcher may have no choice but to release vulnerability information to the public before a patch is available. This is not to say that as a general matter, vendors and system administrators do not value security. A recent survey shows that both these entities (receivers of vulnerability information) and also security researchers (reporters) highly value security, but differ as to why security is important.[37] The data tend to show that

[32] Kevin Poulsen, *Exploit Code on Trial*, SECURITYFOCUS, Nov. 23, 2003, *available at* http://www.securityfocus.com /news/7511.

[33] Paul Roberts, *Expert Weighs Code Release In Wake Of Slammer Worm*, IDG NEWS SERVICE, Jan. 30, 2003, *at* http://www.computerworld.com/securitytopics/security/story/0,10801,78020,00.html; Kevin Poulsen, *Exploit Code on Trial*, SECURITYFOCUS, Nov. 23, 2003, *at* http://www.securityfocus.com /news/7511.

[34] *See* Organization for Internet Safety, *Guidelines for Security Vulnerability Reporting and Response* at 6, *at* http://www.oisafety.org/reference/process.pdf.

[35] *See, e.g.*, eEye Digital Security, *Upcoming Advisories*, *at* http://www.eeye.com/html/Research/Upcoming/index.html; Nomad Mobile Research Centre, *Vulnerability Release Policy*, *at* http://www.nmrc.org/pub/advise/policy.txt; Last State of Delirium at http://lsd-pl.net.

[36] *See e.g.*, Bruce Schneier, *Internet Shield: Secrecy and Security*, S.F. CHRON., March 2, 2003, *available at* http://www.schneier.com/essay-033.html.

[37] Havana, *supra* note 5..

"the receivers seek to fulfill the expectations that their stakeholders have towards their products, and the reporters seek to gain security that is the best possible for the benefit of the public."[38] Disclosure of flaws will undermine customer satisfaction. However, warding off customer disillusionment with the product should not be a factor in disclosure policy making. In the absence of other considerations, customers have a right to know whether the products they purchase are secure.

III. PROPOSED AND ENACTED PUBLICATION RESTRICTIONS

Given the vigorous debate over restrictions, it may be surprising that policy makers have already moved on the attractive possibility of restricting publication of vulnerability tools.

For example, the Council of Europe's new Cybercrime Treaty requires signatories to criminalize the production, sale, procurement for use, import and distribution of a device or program designed or adapted primarily for the purpose of committing unauthorized access or data intercept[39]. Non-European signatories include the U. S. and Japan. Signatories can exempt tools possessed for the authorized testing or protection of a computer system.[40] This exception was not included in original drafts and was heavily lobbied for by security professionals concerned that the article would interfere with both security testing and education.[41]

Member states are already introducing laws that impact vulnerability disclosure. For example, in April 2004, France proposed "La Loi pour la Confiance dans l'Économie Numérique" or LEN, which prohibits having or distributing exploit code and/or detailed vulnerability information and/or information about hacking techniques.[42]

Domestically, the U.S. government and various American companies have used the anti-circumvention provisions of the Digital Millennium Copyright Act ("DMCA"), which regulates the distribution of software primarily designed to circumvent technological protection measures that control access to a work protected under copyright laws, to squelch publication of information about security vulnerabilities.[43] The movie industry successfully used the DMCA to enjoin distribution of DeCSS, a program that demonstrated flaws in the CSS encryption scheme that the industry used as part of its anti-piracy efforts.[44] The Recording Industry Association of America threatened to use the law to stop Princeton University Computer Science Professor Ed Felten and other academics from publishing information about security flaws in a technological protection scheme for digital music.[45] In 2002, Hewlett-Packard threatened SNOsoft, a collective of vulnerability researchers, under the DMCA after the researchers released information

[38] *Id.* at p. 70.

[39] E.U. Convention on Cybercrime, Nov. 23, 2001, art. 6, C.E.T.S. No. 185, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[40] *Id.*

[41] *See* Eugene Spafford et al., *Statement of Concerns regarding the International Treaty on Crime in Cyberspace*, *at* http://www.cerias.purdue.edu/homes/spaf/coe/TREATY_LETTER.html.

[42] C. PÉN. 323-3-1.

[43] *See* 17 U.S.C. § 1201;

[44] *See* Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).

[45] *See* John Markoff, *Record Panel Threatens Researcher with Lawsuit*, N.Y. TIMES, Apr. 24, 2001, at C4.

about a vulnerability in an HP operating system.[46] The U.S. government charged a Russian programmer and his employer under the statute for creating and distributing a program which could decrypt Adobe eBooks.[47] Congress enacted the DMCA pursuant to international treaty, and other nations who are also signatories have passed or will pass laws that may have the same effect as the DMCA.[48]

Less well-publicized than the DMCA, the Critical Infrastructure Information Act of 2002 also regulates vulnerability information. The Act is intended to encourage private sector sharing of information about vulnerabilities with the government. In response to complaints from industry, the statute gives special protections to information submitted to the government under the Act.[49] Any critical infrastructure information ("CII") that is voluntarily provided to the government is however exempt from disclosure under the Freedom of Information Act, state sunshine laws, the Federal Advisory Committee Act and to Congress.[50] Additionally, CII-marked information may not be used in civil actions without the submitter's consent.[51] The Department of Homeland Security recently adopted new regulations implementing that statute.[52] Commentators have expressed concern that the provision will allow industry to stamp information as CII in order to hide it from public review.[53]

Non-governmental organizations have also weighed in with proposals for voluntary restrictions. At the urging of two researchers (Steve Christey and Chris Wysopal, security researchers from Mitre Corp. and @Stake, respectively[54]), the Internet Engineering Task Force took up the issue of appropriate procedures for vulnerability disclosure in early 2002. However, it eventually demurred, saying that the organization was not the proper forum for standardizing human procedures.[55] Later that year, the OIS, of which @Stake is a member, promulgated a policy for time-limited disclosure, in the hope that the industry would adopt it and thereby create a "best practice."[56]

[46] Declan McCullagh, *Security Warning Draws DMCA Threat*, CNET NEWS.COM, July 30, 2002, *at* http://news.com.com/2100-1023-947325.html.

[47] The programmer was given diversion and the employer beat the charges following a jury trial. *See* Lisa M. Bowman, *ElcomSoft Verdict: Not Guilty*, CNET NEWS.COM, December 17, 2002, *at* http://news.com.com/2100-1023-978176.html.

[48] Though the debate over the scope of the DMCA, its impact on fair use, and its relationship to the World Intellectual Property Organization (WIPO) treaty (WIPO Copyright Treaty, Dec. 20, 1996, Diplomatic Conference CRNR/DC/94) are beyond the scope of this paper, note that the treaty does not require an anti-circumvention regulation that impacts fair use or protects an owner's non-copyright rights. *See* Jane C. Ginsburg, *Copyright Legislation for the "Digital Millennium"*, 23 COLUM.-VLA J.L. & ARTS 137, 140 (1999).

[49] 6 U.S.C. 131 (2004).

[50] 6 U.S.C. 133 (2004).

[51] 6 U.S.C. 133(a)(1)(C) (2004).

[52] Procedures for Handling Critical Infrastructure Information, 69 Fed. Reg. 8,073 (Feb. 20, 2004) (to be codified at 6 CFR pt. 29).

[53] *See, e.g.*, Beryl Howell, *Information Overload*, LEGAL TIMES, June 2, 2003, at 52.

[54] Linda Rosencrance, Bug-reporting Standard Proposal Pulled from IETF, ComputerWorld, March 21, 2002, *available at* http://www.computerworld.com/securitytopics/security/story/0,10801,69391,00.html

[55] Brian McWilliams, Security Bug Disclosure Standard Dead in the Water, NEWSBYTES, March 20, 2002, *available at* http://www.computeruser.com/news/02/03/20/news2.html.

[56] *See, e.g.*, James Middleton, *Coalition Condemns Full Disclosure*, VNUNET.COM, Nov. 9, 2001, *at* http://www.vnunet.com/News/1126760; Organization for Internet Safety, *About Organization for Internet Safety*, at http://www.oisafety.org/about.html#1 (listing membership).

Ironically – considering its participation in the OIS – a recently filed class action lawsuit accuses Microsoft of publishing information about software vulnerabilities in a manner that aids criminals more than it helps network administrators.[57] That suit is still pending.

In contrast to these proposals promoting obscurity, a new law in California requires companies to disclose to customers computer-security breaches in which the customer's confidential information may have been accessed.[58] The law does not require the company to reveal how the information was accessed, only that it was. The dueling proposals reflect a growing recognition that there may be consumer rights reasons for information disclosure.

PART TWO

I. SCIENTIFIC ADVANCEMENT REQUIRES PUBLICATION AND OPENNESS

The debate over whether and when to publish scientific research that could be used for illegitimate purposes is not limited to the computer security field. Most recently, following the attacks of September 11, scientists have reconsidered whether research on biological pathogens should not be published for fear of helping terrorists. Policy makers considering restrictions on computer security information have lessons to learn from the long-standing debates and practices in other scientific fields.[59]

The fundamental consensus among scientists is that the ability to publish results, obtain peer review and replicate experiments is an inherent and essential part of the scientific method. Limitations on publication may interfere with scientific advancement. Researchers have argued that omission of information that allows replication of results compromises the scientific process and leads to abuses and errors.[60] As a result, current federal policy is highly favorable to unfettered publication. That policy is enshrined in National Security Decision Directive 189, issued in 1985 by Ronald Reagan. The Directive says that to the maximum extent possible, the products of basic and applied research should be unrestricted, except if the result should be classified for national

[57] Hamilton v. Microsoft, Superior Court of California (Los Angeles, 2003), Complaint, section F. "During the last year, Microsoft issued over 50 security warnings of such technical complexity that a normal member of the General Public could not reasonably understand the security warning and/or could not implement the Microsoft distributed security patches before the fast moving hackers could move to exploit the Microsoft publicized weakness. Thus, while Microsoft has issued strings of alerts, they cannot be understood by the General Public and the method of delivery of the warning has actually increased the probability of harm from hackers who are educated by the information about the flaws and potential breach in the operating systems as described by Microsoft."

[58] CAL. CIV. CODE §§ 1798.29, 1798.82, 1798.84 (2003).

[59] In this section, I heavily relied on Dana A. Shea, CRS Report for Congress, *Balancing Scientific Publication and National Security Concerns: Issues for Congress*, last updated February 2, 2004, *available at* http://www.fas.org/irp/crs/RL31695.pdf.

[60] Conducting Research During the War on Terrorism: Balancing Openness and Security, hearing before the House Comm. on Science, 108th Cong. (testimony of Ronald M. Atlas, President, American Society for Microbiology).

security reasons.[61] The general classification policy states that only scientific, technological or economic matters relating to national security, which includes defense against transnational terrorism, may be classified.[62]

Classification completely controls the distribution of scientific information, but can only be imposed in limited circumstances. Executive Order 12958, issued on April 17, 1995, as amended by Executive Order 13292, issued on March 25, 2003, limits classification to information owned by, produced for, or under the control of, the U.S. Government. The information may only be classified if the unauthorized disclosure could reasonably be expected to result in damage to the national security and the classifying authority is able to identify or describe the damage.[63] Moreover, only information concerning certain limited topics can be classified. The information must concern:

(a) military plans, weapons systems, or operations;

(b) foreign government information;

(c) intelligence activities (including special activities), intelligence sources or methods, or cryptology;

(d) foreign relations or foreign activities of the U.S., including confidential sources;

(e) scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;

(f) U.S. Government programs for safeguarding nuclear materials or facilities;

(g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans or protection services relating to the national security, which includes defense against transnational terrorism; or

(h) weapons of mass destruction.[64]

In the 1970s, the U.S. Government established another category of information subject to restrictions: armaments, military technologies and dual use commercial goods. “Dual use” means goods that have both civilian and military applications. These technologies are subject to export controls under the Department of Commerce Export Administration Regulations (“EAR”) and the Department of State International Traffic in Arms Regulations (“ITAR”). The Export Administration Act of 1979 was not reauthorized by Congress in 2001. Therefore, George W. Bush has used the International

[61] White House, Office of the President, *National Security Directive 189*, September 21, 1985, *available at* http://www.fas.org/irp/offdocs/nsdd/nsdd-189.htm.

[62] Executive Order 12,958 (April 17, 1995) as amended by Executive Order 13,293 (March 25, 2003).

[63] *Id.* at § 1.2.

[64] *Id.* at § 1.4

Economic Emergency Powers Act to maintain export controls.[65]

Export controls do not directly regulate the distribution of technology or technological information within the U.S., only information transfer to other countries. However, publication accessible to foreign nationals, which includes essentially all Internet publication, including websites and mailing lists, would violate the export restrictions. In the past, universities have been called upon to withdraw papers from conferences, present research only in closed sessions and isolate visiting researchers to ensure that foreigners are not exposed to information that falls under export controls.[66]

In some cases, federal agencies have imposed publication restrictions through contracts for federal funding for research. According to Shea, "[i]n general, these restrictions have not been applied to entire research fields, but, instead, have been targeted at research considered to be of import or relevant to national defense or where portions of a contract may contain classified information."[67] The restrictions can only apply to federally funded research performed under contract. Nonetheless, university administrators often renegotiate or reject contracts with prepublication review clauses.[68]

Scientists are more inclined to accept voluntary self-regulation, though even these proposals have engendered a lot of dissent. In February 1975, in response to concerns about genetic engineering and other biotechnology research, the industry met at Asilomar, California, and adopted voluntary restrictions on recombinant DNA research. According to the Irish Council on Science Technology and Innovation:

> *The outcome of the conference was the development of a series of guidelines designed to ensure the safety of genetic engineering research. It also led to the establishment of the Recombinant DNA Advisory Committee ("RAC") by the U.S. National Institute of Health ("NIH") and the eventual publication in 1976 of what subsequently became known as the RAC Guidelines.*[69]

Specialists in biotech and risk assessment crafted the guidelines, but they mostly targeted certain types of research, with the concern of preventing accidental release of microorganisms, so as to avoid malicious use of research.

Following the terrorist attacks of September 11, 2001, the American Association for the Advancement of Sciences became concerned with the potential for malicious uses and adopted voluntary restrictions on the publication of potentially "dangerous science."[70] Publications detailing a genetic modification to the mousepox virus that

[65] Exec. Order No. 13,222, 66 Fed. Reg. 44,025 (Aug. 22, 2001).

[66] *See* HAROLD RELYEA, SILENCING SCIENCE: NATIONAL SECURITY CONTROLS AND SCIENTIFIC COMMUNICATION 125-26 (1994).

[67] Dana A. Shea, CRS Report for Congress, *Balancing Scientific Publication and National Security Concerns: Issues for Congress*, last updated February 2, 2004, *available at* http://www.fas.org/irp/crs/RL31695.pdf.

[68] Anne Marie Borrego, *Colleges See More Federal Limits on Research*, CHRON. OF HIGHER EDUC., Nov. 1, 2002, at 24; Connie Cass, *Science Community Struggles With Terror-wary Feds*, ASSOCIATED PRESS, January 2, 2003; As related in the minutes of the University Senate of the University of Minnesota on April 25, 2002, *available at* http://www1.umn.edu/usenate/usen/020425sen.html.

[69] IRISH COUNCIL ON SCIENCE TECHNOLOGY AND INNOVATION, REPORT ON BIOTECHNOLOGY (February 2002), *at* http://www.forfas.ie/icsti/statements/biotech01/regulation.htm.

[70] Press Release, American Association for the Advancement of Science, World's Leading Journal Editors Urge Self-Governance and Responsibility in Publishing Potentially "Dangerous" Science (Feb, 16, 2003),

infects previously vaccinated animals,[71] and assembling poliovirus from readily available chemical sequences,[72] among others, raised new concerns. The voluntary restrictions focused on journals that publish this kind of research, but even these voluntary restrictions met with great controversy. Professional science organizations have adopted positions that all information necessary to reproduce experiments must be included in articles submitted for publication, as part of the scientific process. Dr. Ronald Atlas, a proponent of voluntary restrictions and President of the American Society for Microbiology ("ASM") has stated:

> *Omission of materials and methods from scientific literature would compromise the scientific process and could lead to abuses as well as the perpetuation of errors. Independent reproducibility is the heart of the scientific process. Even within the context of heightened scrutiny, research articles must be published intact. If scientists cannot assess and replicate the work of their colleagues, the very foundation of science is eroded.*[73]

Additionally, if professional journals in the U.S. choose not to publish certain research, international journals will do so and fill this vacuum, or scientists may independently self-publish on the Internet.

In an attempt to balance these concerns, the Society for Microbiology has adopted very narrow publication restrictions. The society's policy states that "the ASM recognizes that there are valid concerns regarding the publication of information in scientific journals that could be put to inappropriate use. Members of the ASM Publications Board will evaluate the rare manuscript that might raise such issues during the review process." However, the standard for refusing publication is very slim. It is not whether the published information could be misused, but whether the submission "describes misuses of microbiology or of information derived from microbiology."[74]

Furthermore, scientists genuinely disagree about the risks of certain publications. For example, after *Science* magazine published the controversial article about the synthesis of polio from available building blocks, the editor asserted that informed scientists agreed that there were no valid security concerns regarding the publication.[75]

More recently, the U.S. Government has been considering imposing additional publication restrictions following 9/11, and possibly establishing another category of information to restrict, "sensitive, but not classified.". On March 19, 2002, White House

at http://www.aaas.org/news/releases/2003/0216bio.shtml. *See also* David Malakoff, *Science and Security: Researchers Urged to Self-Censor Sensitive Data*, 299 SCIENCE 321 (2003); David Malakoff, *Biological Agents: New U.S. Rules Set the Stage for Tighter Security, Oversight*, 298 SCIENCE 2304 (2002).

[71] Joan Stephenson, *Biowarfare Warning*, 285 JAMA 725 (2001).

[72] Rich Weiss, *Polio-Causing Virus Created in N.Y. Lab: Made-From-Scratch Pathogen Prompts Concerns About Bioethics, Terrorism,* WASH. POST, July 12, 2002, at A1.

[73] Conducting Research During the War on Terrorism: Balancing Openness and Security, hearing before the House Comm. on Science, 108th Cong. (testimony of Ronald M. Atlas, President, American Society for Microbiology).

[74] American Society for Microbiology, *Policy Guidelines of the Publications Board of the ASM in the Handling of Manuscripts Dealing with Microbiological Sensitive Issues*, *at* http://www.journals.asm.org/misc/Pathogens_and_Toxins.shtml.

[75] Donald Kennedy, Response to *A Not-So-Cheap Stunt*, 297 SCIENCE 769 (2002).

Chief of Staff, Andrew Card, sent a memo to executive agencies cautioning that information that could be reasonably expected to assist in weapons of mass destruction development or use should not be inappropriately disclosed.[76] The memo emphasized that “sensitive, but unclassified” information related to homeland security should be protected. That term is not defined in the memo. However, the National Security Agency defines “sensitive, but unclassified” as “any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs or the privacy to which individuals are entitled under [the Privacy Act] but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.”[77]

The Homeland Security Act created the department of Homeland Security and states that, while to the greatest extent practicable, the results of research funded by the DHS are to be unclassified, the President shall:

> *... [p]rescribe and implement procedures under which relevant federal agencies … identify and safeguard homeland security information that is sensitive but unclassified. … The President shall ensure that such procedures apply to all agencies of the Federal Government.*[78]

On July 29, 2003, the President delegated the authority to do this to the Secretary of Homeland Security.[79] There is some uncertainty as to whether the rulemaking will be public or not,[80] but as far as the public knows, those procedures have not yet been established.

Response to these initiatives has been mixed, but even where there is recognition that some publications could assist terrorists, scientists are extremely wary of imposing publication restrictions. “If policy measures to prevent terrorists from acquiring pathogens, equipment, and technical information are not crafted with great care, they may have a significantly adverse effect upon critically important research activities.”[81]

In 2002, the Presidents of the National Academies released a joint statement asserting that the government should continue its current practice of allowing unfettered publication of non-classified information and not develop a less well-defined category for sensitive research.[82] Unless distinctions are very clear, they argue that scientific

[76] Memorandum from Andrew H. Card, Jr., Assistant to the President and Chief of Staff, to Heads of Executive Departments and Agencies (March 19, 2002), *available at* http://www.usdoj.gov/oip/foiapost/2002foiapost10.htm.

[77] National Security Agency, Committee on National Security Systems, *National Information Assurance Glossary*, CNSS Instruction No. 4009, *at* http://www.nstissc.gov/Assets/pdf/4009.pdf

[78] Homeland Security Act of 2002 § 892, 6 U.S.C. § 482 (2003).

[79] *See* Exec. Order No. 13,311, 68 Fed. Reg. 45,149 (July 29, 2003).

[80] OMB Watch, *Executive Order Assigns Information Sharing Development to DHS*, *at* http://www.ombwatch.org/article/articleview/1734/1/1/ (“It is unclear how these provisions will be developed and if any public input or congressional oversight will be incorporated.”).

[81] Conducting Research During the War on Terrorism: Balancing Openness and Security, hearing before the House Comm. on Science, 108th Cong. (testimony of Ronald M. Atlas, President, American Society for Microbiology).

[82] Bruce Alberts, et al., *Statement on Science and Security in An Age of Terrorism,* National Academies, October 18, 2002, *at* http://www4.nationalacademies.org/news.nsf/isbn/s10182002b?OpenDocument.

creativity and national security will both suffer. HSA restrictions would "reduce media's access to government and in the process diminish the government's accountability to the public."[83] This consensus, reflected in U.S. Government Policy, has kept restrictions on scientific publications to a minimum.

II. How Publication Restrictions Cannot Target the Utilitarian Aspects of Code Without Chilling Legitimate Research and Burdening the Advancement of Computer Security

The primary way that computer security research is different from other fields is its reliance on code to express ideas.[84] Legislatures have tried to regulate code like other tools that can be used to commit criminal acts.[85] Therefore, courts have tried to balance code regulations with First Amendment protections for the expression it contains. But the law cannot regulate code without impacting expression because the two are intertwined. Any regulation of code threatens to impact computer science in a manner rejected by the government and researchers in other fields.

Publication of computer security information clashed against the export control scheme in the case of *Bernstein v. United States Department of State*. Daniel Bernstein was a mathematics PhD student who wrote an encryption program called "Snuffle." Bernstein wanted to publish his program and a paper describing it on the Internet for other cryptographers' review and comments. The U.S. State Department told Bernstein that he could not post the information because it would violate the export control regulations. According to the Department, since encryption programs were classified as munitions and publication on the Internet was tantamount to export, people in other countries could obtain the information. Bernstein sued the U.S. Government. The U.S. District Court hearing the case held that regulation targeting encryption was aimed at speech on a specific type of expression and that the statutory safeguards were inadequate to prevent government content discrimination. The ITAR and EAR regulations were therefore an unconstitutional prior restraint on speech and the court granted an injunction forbidding the government from prosecuting Bernstein for exporting encryption programs.[86] The court held that the code is essential in expressing ideas in computer science and cryptography, and to restrict the code publication because of those topics was impermissible.[87]

[83] Press Release, OMB Watch, "Sensitive But Classified" Provisions In the Homeland Security Act of 2002, June 11, 2003, *at* http://www.ombwatch.org/article/articleview/1568/1/1/

[84] See 49 U.C.L.A. L.Rev. 871, 887-903.

[85] *See, e.g.*, 18 U.S.C. 2512(1)(b) (illegal to possess eavesdropping devices); CAL. PENAL CODE § 466 (burglary tools).

[86] 922 F. Supp. 1426 (N.D. Cal. 1996) (Bernstein I), Bernstein v. United States Dept. of State, 945 F. Supp. 1279 (N.D. Cal. 1996) (Bernstein II), Bernstein v. United States Dep't of State, 974 F. Supp. 1288 (N.D. Cal. 1997) (Bernstein III).

[87] *Id.* at 1305 ("By the very terms of the encryption regulations, the most common expressive activities of scholars—teaching a class, publishing their ideas, speaking at conferences, or writing to colleagues over the Internet—are subject to a prior restraint by the export controls when they involve cryptographic source code or computer programs. In the field of applied science ideas are not just expressed in abstract, theoretical terms, but in precise applications. Those applications are subject to licensing under the

More recently, however, courts considering the constitutionality of statutes restricting the distribution of computer code have upheld such regulations if they are content neutral regulations targeting the functional rather than communicative aspects of the code. In *Universal City Studios, Inc. v. Corley*,[88] the Second Circuit considered a hacker magazine's challenge to an injunction under the anti-circumvention provision of the DMCA, preventing it from linking to code that decrypted DVDs. The court determined that the statute targeted a function of the decryption code, not the message the code communicated about the ways in which the DVD encryption scheme could be broken.[89] The court then applied intermediate scrutiny and determined that the injunction did not unduly burden defendants' First Amendment rights in light of the governmental interest in controlling dispersal of the decryption code.[90]

Similarly, in *United States v. Elcom*,[91] a corporation and individual defendant were criminally prosecuted for violating the DMCA by distributing a product that allowed users to remove use restrictions from electronic books, including restrictions that prevented the book from being copied and redistributed. As did the Second Circuit, the Northern California District Court held that, while computer code is speech and is therefore protected by the First Amendment, the DMCA is sufficiently tailored to protect legitimate and substantial governmental interests, and so did not burden the defendant's First Amendment rights.[92]

Based on these and other cases, Ethan Preston and John Lofton assert that the First Amendment will provide only limited protection for vulnerability information, specifically because code is not only communicative but also inherently functional.[93] This concerns the authors, who believe that the legal system should extend liability to publishers of computer security information only with extreme caution. [94] If code is a precise way of communicating information about a security flaw, and that expression inherently has functionality, then regulating that functionality will inevitably constrain both utility and the message. Court-drawn distinctions between speech and function in software code are a legal fiction.

Certainly some software programs may be more expressive than others. Professor Dan Burk has questioned whether all software code is communicative. While there may be some kernel of expression in almost any activity, that kernel may not be sufficient to warrant constitutional protection, particularly where the form of expression is so fundamentally utilitarian.[95] However, it is hard to argue that every program does not

encryption regulations and are excluded from the exemptions for fundamental research and educational information.").

[88] 273 F.3d 429 (2d Cir. 2001).

[89] *Id.*

[90] *Id.*

[91] 203 F.Supp.2d 1111 (N.D. Cal. 2002).

[92] *Id.*

[93]Ethan Preston & John Lofton, *Computer Security Publications: Information Economics, Shifting Liability and The First Amendment*, 24 WHITTIER L.REV. 71, 129 (2002).

[94] *Id*. at 142.

[95] See D.L. Burk, *Patenting Speech*, 79 TEX. L.REV. 99, 112 (2000).

communicate something to a computer scientist, even if the only information is instructions on how to accomplish some task.

Other commentators have argued that to properly protect expression in code while allowing regulation of dangerous functionality, the law should treat source code as speech governed by the First Amendment and by copyright law, and treat object, or machine-readable code, as a device regulated by patent law.[96] But this parsing would not resolve the problem of harmful code. Source code is readily compiled into object code, and object code can be reverse engineered into source. During legal battles over the export of Snuffle and Phil Zimmerman's Pretty Good Privacy encryption program, enthusiasts and activists exported scannable printouts of the source code designed to be read by optical character recognition software and easily converted into digital source code, then compiled into object code.[97]

Even non-functional natural language publications that instruct readers how to exploit vulnerabilities may not receive full First Amendment protection.[98] As a general principle, courts have been loath to impose civil or criminal liability for speech that instructs on how to commit a crime. The tendency of speech to encourage unlawful acts does not constitute justification for banning it.[99] For example, in *NAACP v. Claiborne Hardware Co*.[100] the Court held that statements that could be interpreted as inviting violent retaliation were protected in the absence of evidence that the speaker had "authorized, ratified, or directly threatened acts of violence."[101] Nor can speech by a law-abiding possessor of information be suppressed in order to deter conduct by a non-law-abiding third party.[102]

Only in narrow circumstances can the law regulate speech that enables or even incites others to commit crimes. In *Brandenburg v. Ohio*, the Supreme Court held that advocacy of criminal activity is protected speech unless it is "directed to inciting or producing imminent lawless action and is likely to incite or produce such action."[103] In addition, courts have withheld First Amendment protection for statement that the speaker makes **intending** that crime will result.[104]

Some courts have inferred a speaker's criminal intent from publication to a general audience, as opposed to a co-conspirator or known criminal, if the publisher

[96] L.J. Camp & S. Syme, *Code as Embedded Speech, Machine and Service*, J. INFO. L. & TECH. (2001), *available at* http://elj.warwick.ac.uk/jilt/01-2/camp.html (last visited Nov. 30, 2004).

[97] *See, e.g.*, http://www.mirrors.wiretapped.net/security/cryptography/literature/cracking-des/chap-4.html.

[98] Preston & Lofton, *supra* note 88, at 109; Eugene Volokh, *Crime Facilitating Speech*, 57 STAN. L.R. (forthcoming Feb 2005), at 30-39.

[99] Ashcroft v. Free Speech Coalition, 535 U.S. at 253 (striking down "virtual child pornography" restrictions because the chance that such material "whets the appetites of pedophiles" is not "likely to incite imminent lawless action" under Brandenburg v. Ohio, 395 U.S. 444, 447 (1969)).

[100] 458 U.S. 886 (1982).

[101] *Id.* at 929.

[102] Bartnicki v. Vopper, 532 U.S. 514, 530 (2001) (holding that First Amendment protects right of innocent radio stations to broadcast illegally intercepted communications).

[103] 395 U.S. 444, 447 (1969).

[104] *See* United States v. Raymond, 228 F.3d 804, 815 (7th Cir. 2000); United States v. Aguilar, 883 F.2d 662 (9th Cir. 1989), *superseded by statute as noted in* United States v. Gonzalez-Torres, 273 F.3d 1181 (9th Cir. 2001); United States v. Freeman, 761 F.2d 549, 552 (9th Cir. 1985); United States v. Holecek, 739 F.2d 331, 335 (8th Cir. 1984).

merely **knows** that the information will be used as part of a lawless act.[105] For example, in *United States v. Buttorff*,[106] the defendants were convicted of aiding and abetting persons who filed false or fraudulent tax returns after they spoke at a public meeting advising listeners of various ways to avoid payment of taxes. The Eighth Circuit found that this was sufficient to remove First Amendment protection, even though the defendant did not incite imminent lawless activity per *Brandenburg*. "The defendants did go beyond mere advocacy of tax reform. They explained how to avoid withholding and their speeches and explanations incited several individuals to activity that violated federal law and had the potential of substantially hindering the administration of the revenue."[107] The *Buttorff* defendants did not have personal contact with the tax evaders, or knowledge that false returns were in fact filed, but merely gave speeches before large groups encouraging and advising others to evade income taxes.

Similarly, in *United States v. Barnett*,[108] the Ninth Circuit held that the First Amendment did not preclude using a recipe for phencyclidine (PCP) as evidence in support of a search warrant. The defendant had advertised in *High Times*, a drug-related periodical, as a "reliable source" for instructions on how to manufacture PCP and then mailed a formula for the manufacture of the drug to a man who was later observed making the drug from the formula.[109] The defendant provided essential information for the manufacture of the drug.

Both *Buttorff* and *Barnett* suggest that the *usefulness* of the defendant's information, even if distributed to people with whom the defendant had no prior relationship or agreement, is a potential basis for aiding and abetting liability, despite free speech considerations.

In contrast, in *Herceg v. Hustler Magazine*,[110] the Fifth Circuit held that a magazine was not liable for publishing an article describing autoerotic asphyxiation after a reader followed the instructions and suffocated. The article included details about how the act is performed, the kind of physical pleasure those who engage in it seek to achieve and ten different warnings that the practice is dangerous. The Court held that the article did not encourage *imminent* illegal action, nor did it *incite*. "Although it is conceivable that, in some instances, the amount of detail contained in challenged speech may be relevant in determining whether incitement exists, the detail in [this article] is not enough to permit breach of the First Amendment. The manner of engaging in autoerotic asphyxiation apparently is not complicated. To understand what the term means is to know roughly how to accomplish it."[111] The court raised, but did not answer, the question of whether written material might ever be found to create culpable incitement unprotected by the First Amendment.

[105] *See also* United States v. Featherston, 461 F.2d 1119, 1122 (9th Cir. 1972); United States v. Mendelsohn, 896 F.2d 1183, 1186 (9th Cir. 1990). Of course, if there is proof that the publisher intended to assist criminal activity, the First Amendment will not shield the publication from civil or criminal liability. *See, e.g.*, Rice v. Paladin Enterprises, 128 F.3d 233 (4th Cir. 1997).

[106] 572 F.2d 619 (8th Cir.), *cert. denied*, 437 U.S. 906 (1978).

[107] *Id.* at 624.

[108] 667 F.2d 835 (9th Cir. 1982).

[109] The Court did not consider whether this alone would be sufficient evidence to uphold a conviction.

[110] 814 F.2d 1017 (5th Cir. 1987).

[111] *Id.* at 1023.

Buttorff and *Barnett* are probably the outside limits of government ability to punish non-*Brandenberg* speech. Aiding and abetting, the offenses charged in *Buttorff and Barnett*, require more than mere advocacy. They require that the speaker make the effort to assist the recipient of information in committing a crime. Inchoate offenses like solicitation and conspiracy require criminal intent in addition to the speech act.[112] The Department of Justice has taken the position that speech restrictions – like a recent statute prohibiting the publication of bomb making information – would violate the First Amendment without requiring that the defendant actually and consciously intended to cause a crime.[113] While the First Amendment would not protect targeted speech to an audience of intended criminals, it is unclear that criminal law could punish the general publication of crime instructions information, even where the writer, publisher or seller of the information has the purpose of generally assisting unknown and unidentified readers in the commission of crimes.[114]

Legitimate researchers are not comforted by this lack of legal clarity. Security researchers frequently share vulnerability information on Web pages or on security mailing lists. These communities are open to the public and include both “white hat” and “black hat” hackers. The publishers know that some of the recipients may use the information for crimes. The new restrictions applicable to code have already engendered an unfriendly legal climate that has adversely affected research. Following the highly publicized DMCA claims levied against foreign researchers and U.S. academics, publishers are not sure that a prosecutor will not come after them. Some researchers and conferences have boycotted the U.S., hindering normal information sharing within the profession.[115]

[112] *See., e.g.*, MODEL PENAL CODE §§ 5.02, 2.06 (3)(a)(i) (criminal solicitation); §5.03 (conspiracy) (ALI 2001). *See also* MODEL PENAL CODE § 223.4 (ALI 2001) (extortion or blackmail); § 240.2 (threats and other improper influencing official and political matters); § 241 (perjury); § 224.1 (forgery); § 210.5(2) (successfully soliciting another to commit suicide). Somewhat to the contrary, the Ninth Circuit has interpreted 18 U.S.C. § 871 (2000) (threatening the life of the President) to require only that the defendant intentionally make a statement, written or oral, in a context or under such circumstances wherein a reasonable person would foresee that the statement would be interpreted by those to whom the maker communicates the statement as a serious expression of an intention to inflict bodily harm upon or to take the life of the President, and that the statement not be the result of mistake, duress, or coercion. United States. v. Merrill, 746 F.2d 458, 462 (9th Cir. 1985), cert. denied, 469 U.S. 1165, 105 S. Ct. 926, 83 L. Ed. 2d 938(1985). A defendant's intent to make or carry out a threat is not an element of the crime. United States v. Twine, 853 F.2d 676, 680 (9th Cir. 1988).

[113] DEPARTMENT OF JUSTICE, REPORT ON THE AVAILABILITY OF BOMB MAKING INFORMATION, THE EXTENT TO WHICH ITS DISSEMINATION IS CONTROLLED BY FEDERAL LAW, AND THE EXTENT TO WHICH SUCH DISSEMINATION MAY BE SUBJECT TO REGULATION CONSISTENT WITH THE FIRST AMENDMENT TO THE UNITED STATES CONSTITUTION (April 1997), *available at* http://www.derechos.org/human-rights/speech/bomb.html. “[T]he First Amendment almost certainly would require that the ‘intent’ scienter provision in such a statute be construed to mean an actual, conscious purpose to bring about the specified result.” *Id.* at Section VI.B; Government’s Motion for Reversal of Conviction at 6-7 & n.3, United States v. McDanel, No. 03-50135 (9th Cir. 2003) (taking the position that communicating such information may violate the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030(a)(5)(A), 1030(e)(8), but only if the speaker intended to facilitate security violations, rather than intending to urge the software producer to fix the problem).

[114] DOJ REPORT ON AVAILABILITY OF BOMB MAKING INFORMATION, Section VI, A, 2. *Available at* http://www.usdoj.gov/criminal/cybercrime/bombmakinginfo.html

[115] *See, e.g.,* Will Knight, *Computer Scientists Boycott US Over Digital Copyright Law*,

This concern is exacerbated by the likelihood that prosecutors and courts will weigh the social perception of the legitimacy of the publisher's "hacker" audience, or the respectability of the publisher himself, in deciding whether the researcher published with a criminal intent. Even legitimate researchers can feel marginalized and disrespected in the security field. Some vendors and system administrators openly mistrust researcher intentions. Researchers spend their time figuring out how to break into computer systems. Researchers often operate independently. They are not necessarily credentialed, nor do they necessarily have any formal training or degree. There is often a generation gap between researchers and the business people that run software companies and large ISPs. Figuring out how to break into systems may require a certain unorthodox mindset that can aggravate more traditional business people. For example, one "hacker" group is called Last Stage of Delirium or LSD. "Cult of the Dead Cow" featured a raucous launch of its remote administration tool, "Back Orifice." This cultural divide exacerbates the problem of researchers and publishers being able to work together. This cultural misunderstanding also contributes to a feeling within the business that researchers and attackers are essentially the same, and regulation is the only way to control them, since the perception is that the researchers cannot be trusted.[116]

This perception is dangerous. Even in the absence of publication, research is essential to the improvement of product security, though it is not always welcome by the vendors, or by law enforcement. In one example, in 2001, Tornado Systems, a now-defunct Los Angeles-based Internet messaging company, convinced the U.S. Department of Justice to prosecute a former employee who informed the company's customers of a security flaw in its webmail service.[117] The company claimed that the defendant was responsible for its lost business. As a result, security researcher Bret McDanel was convicted of a violation of 18 U.S.C. § 1030(a)(5)(A) which prohibits the transmission of code, programs, or information with the intent to cause damage to a protected computer for sending email to customers of his former employer, informing them that the company's web messaging service was insecure. The statute defines damage as any impairment to the integrity or availability of data, a program or system. The government's argument at trial was that McDanel impaired the integrity of his former employer's messaging system by informing customers about the security flaw. Outsiders could potentially access the system, and current customers were upset. The company therefore had to correct the flaw that McDanel revealed. Because fixing that preexisting problem cost money, the government argued that McDanel caused loss to the messaging

NEWSCIENTIST.COM, July 23, 2001, *available at* http://www.newscientist.com/news/ news.jsp?id=ns99991063.

[116] Still, the quality of the product and the skill of the researcher can outweigh his or her unorthodoxy. Marc Maiffret, Chief Hacking Officer of eEye, has had blue hair, and posed for Newsweek magazine holding a hammer in front of a number of computer monitors. *See* Brad Stone, *An eEye on Microsoft*, NEWSWEEK, March 22, 2004, at 40, *available at* http://www.msnbc.msn.com/id/4486825/site/newsweek/. In late June of 2004, eEye contracted with the United States Department of Defense for its vulnerability scanning tool. *See* Press Release, eEye Digital Security, eEye Digital Security's Technology Selected for DISA Task Order Valued at Over $6 million to Provide Information Assurance Vulnerability Management (June 23, 2004), *at* http://www.eeye.com/html/company/press/PR20040623.html. Many hackers eventually go to work for large security companies, vendors or the government.

[117] *See* United States v. McDanel, No. CR-01-638-LGB (C.D. Cal. Mar. 25, 2003), *rev'd*, No. 03-50135 (9th Cir. Dec. 15, 2003).

company. On appeal, the government disavowed this view, and agreed with the defendant that a conviction could only be based on evidence that the "defendant intended his messages to aid others in accessing or changing the system or data."[118] McDanel's conviction was overturned on appeal, but not before he served sixteen months in prison.

Professor Eugene Volokh has considered the inconsistent, if not incoherent, application of free speech principles in cases such as these and argues that courts should develop a uniform theory of First Amendment protection for crime-facilitating speech. First, Volokh notes that most crime facilitating speech is "dual purpose." Speech that enables criminal activity by giving the listener the tools, motivation or means to avoid capture, also helps people engage in lawful behavior, as with vulnerability information.[119] It can also help people evaluate and participate in public debate (especially about crime policy), promote government accountability and customer awareness, be used for self-edification, or even just for entertainment value.[120] Volokh proposes that protections for crime-facilitating speech depend on several factors including the extent of harm that could result, the speaker's *mens rea*, the social value of the speech, and how the speech is presented or advertised. Volokh argues for an exception to the First Amendment for speech to particular people known to be criminals and "single-use" speech that has few if any lawful uses.

McDanel's ordeal proves that courts can miss obvious free speech issues when adjudicating computer disputes. A rule based on court interpretations of the social value of speech may not work in an area that is new, unfamiliar, and where social norms are less developed and less widely known. Without clearly defined and understandable rules, legitimate researchers will be scared away from fruitful fields of study.[121] Legal penalties may deter only the well-intentioned or hapless researcher. Researchers may turn to illicit or undesirable activities. For example, there is already a growing commercial and black market for vulnerability information: at a recent conference at Stanford Law School on Cybersecurity, Research and Disclosure, participants reported that they know researchers who are paid to find network vulnerabilities for exploitation by spammers. Others could continue to publish exploit code under cover of anonymizing technologies. Additionally, by making security research and reporting illegal, otherwise legitimate researchers may be less reluctant to engage in other unrelated illegal practices.

It is difficult, if not impossible, to restrict the publication of functional code, or even natural language information an attacker could use, without burdening or criminalizing legitimate research, and creating a new class of criminals. Therefore, we must decide whether disclosure restrictions are worth the price.

[118] Government's Motion for Reversal of Conviction, United States v. McDanel, No. 03-50135 (9th Cir. 2003), *available at* http://cyberlaw.stanford.edu/about/cases/united_states_v_mcdanel.shtml.

[119] Volokh, *supra* note 98.

[120] *Id*.

[121] *Conducting Research During the War on Terrorism: Balancing Openness and Security: Hearing Before the House Comm. on Science*, 108th Cong. (2004) (testimony of M.R.C. Greenwood, Chancellor, University of California, Santa Cruz); *Conducting Research During the War on Terrorism: Balancing Openness and Security: Hearing Before the House Comm. on Science*, 108th Cong. (2004) (testimony of Sheila Widnall, Institute Professor and Professor of Aeronautics and Astronautics, Massachusetts Institute of Technology).

PART THREE

Despite national security concerns, scientists and policy makers share a strong consensus in favor of openness and sharing. Everyone recognizes that good science requires publication, reproducibility and peer review to advance knowledge and avoid errors. In the rare cases in which government imposes publication restrictions, it does so only if the risk is extreme and non-theoretical, and where the security payoff is identifiable and outweighs the benefits of publication. For example, information cannot be classified unless it falls into a certain defined category and the classifying authority specifically identifies the risk.[122] Under the ITAR and EAR regulations, there are strict standards for when an export license can be denied.[123] Other research is generally unfettered or subject to only narrow, voluntary restrictions. The prevailing policy recognizes the difficulty in determining when publication is potentially harmful, and the chilling effect that strict and punitive enforcement of publication restrictions would have on scientists.

Policy makers have taken an extremely cautious approach against regulating scientific expression generally. Why then are vulnerability disclosure restrictions so popular? The major difference between computer security publications and other science publications is the use of code to express computer science ideas. This section considers the functionality of code, as well as other ways in which computer security research is different than research publications in other fields, and whether those differences justify publication restrictions despite the principles that have lead to the general rejection of regulation in other fields.

I. Computer Security Benefits More From Widespread Dissemination of State of the Art Knowledge Than Do Other Scientific Fields

As in other scientific fields, restrictions place a heavy burden on the development of knowledge in the field. Scientific advancement is based upon the open exchange of information and requires researchers to communicate their results, collaborate, peer review, test and critique each other. This is no less true with computer security.

Computer security particularly benefits from public openness. Because more people program and maintain computers than perform high-level biological and chemical research, more people need to know about computer security. There are hundreds of thousands of people releasing freeware, shareware and open source products, and writing code for businesses that the general public uses. Openness helps both network defenders who want functional code for risk abatement and patch testing and programmers. State of the art information about secure programming techniques improves security. Researcher Jeremy Rauch has written:

> [B]uffer overruns were once an obscure topic, but now they have been discussed and dissected to the point where many programmers understand how to prevent them, even if they are incapable of writing an exploit.

[122] Exec. Order 12,958, 60 Fed. Reg. 19,825 (Apr. 17, 1995), *as amended by* Exec. Order 13,292, 68 Fed. Reg. 15,315 (Mar. 25, 2003).

[123] *See, e.g.*, 22 C.F.R. § 120-30 (governing export regulations).

> Where there were once ten new exploits based on the buffer-overrun concept each week, the rate at which they are found has slowed to a trickle. The discussion of these problems in an open, collaborative forum helped to promote understanding, which in turn has significantly reduced the number of vulnerabilities of this type. There are other examples of this —from race conditions to file-permission problems to authentication mechanisms and even simple things like password management — that are now understood by enough people that they no longer plague every other program in existence.[124]

If both computer security research and programming practices improve through information sharing, this may be a reason to protect openness more in computer science than in other fields, especially since Lipner's insight that attackers benefit more than defenders from exploit code is probably wrong.[125]

II. Computer Insecurity Poses Less Harm Than That Threatened by "Dangerous Science"

Harm from misuse of research in microbiology and other fields is more serious than risks from the misuse of computer security information. Misuse of a publication discussing how to synthesize more virulent forms of the smallpox virus and anthrax bacteria, assemble the polio virus from readily accessible chemicals, or map the bubonic plague genome can result in some, if not many, deaths. Additionally, there is a long history of germ warfare, from ancient civilizations to the recent anthrax case in the U.S.

Misuse of vulnerability information results in unauthorized access to or damage to data in computers. Computers can serve very important functions and people depend on computers for the necessities in life. Government and industry may choose to run critical systems on computer networks. But with computers, we have a choice that we do not have with biology. People have no choice but to become ill from pathogens. Computers do not need to operate critical infrastructures on publicly accessible networks. If a security breach occurs there are backups, and systems can be taken off line and alternative systems used. The vast majority of computer attacks cause little harm, and those that are damaging cause almost exclusively economic harm. Historically, there has never been a documented case of cyberterrorism, in the U.S. or abroad.[126]

III. **The Likelihood of Abuse of Computer Security Information is Greater Than In Other Scientific Fields**

While the magnitude of harm is less, the opportunity for abuse is greater. This is mostly due to the functionality of code, which allows otherwise ignorant people to

[124] Jeremy Rauch, *Full Disclosure: The Future of Vulnerability Disclosure?*, USENIX, Nov. 1999, *available at* http://www.usenix.org/publications/login/1999-11/features/disclosure.html.

[125] *See* discussion of Peter Swire's work, section V, infra.

[126] Andrew Donoghue, *Cyberterror: Clear and Present Danger or Phantom Menace?*, INSIGHT, *available at* http://insight.zdnet.co.uk/0,39020415,39118365,00.htm.

become attackers. But is also caused by the accessibility of computer security knowledge and the democratization of computers and programming skills. Computer networks are more widely understood and more easily manipulated than, say, microbiological specimens. Very few people are able to use the information published in scientific journals to synthesize polio or make weapons-grade anthrax. Those who are sufficiently knowledgeable have probably studied with other scientists at universities, taken ethics classes, or absorbed a code of responsibility during the course of their education. This explicit or implicit moral standard of conduct means that peers will not approve of misuse, and peer approval is essential to employment, funding, promotion and other desirable professional rewards. Moreover, when investigating the anthrax attacks in the U.S., law enforcement had only a relatively finite number of people able to develop the expertise needed to do those attacks. Would-be attackers need hard-to-obtain and expensive lab equipment to carry out their experiments and create the tools for their attack.

In contrast, many more people are capable of running an exploit program that attacks a computer or network. The attacker need not be knowledgeable about computer security principles to use these automated programs. Even educated security professionals are often self-trained. They may have no formal inculcation of social norms. A security professional's relevant peer group may or may not know about attacks which an attacker could launch over the Internet from the privacy of his own home without need of a jointly-used laboratory. Unlike other scientists, computer security professionals are often freelancers not competing for university teaching jobs, promotion, or grant funding for research. Therefore, more people have the ability to attack, without systematic ethical or professional reward restraints, and with the ability to operate in relative secrecy. These people are also harder to catch and prosecute, if only because there are a greater number with the tools necessary to attack. As a result, computer security information is far more likely to be clandestinely abused than other scientific data.[127] This might be a reason to control vulnerability information, particularly functional code, more than arcane scientific information, even though the category of harm is less serious.

IV. Secrecy Is Unlikely to Benefit Security More Than Openness in the Context of Computer Networks

In the context of computers, secrecy is unlikely to benefit security more than openness does, and may harm it. This is because there is no practical difference between security tools and attack tools, because the economics of attack are such that vulnerabilities do not remain secret for long, and because defenders find vulnerability information at least as useful as attackers do.

Scientists often find no discernable difference between beneficial security tools and attack code. The same code that explains a flaw tests for it and exploits it. The same code that tests a system to make sure it is secure can also be used to break systems. Writing for over eighty security professionals and academics lobbying the Council of

[127] *But see* Kyle B. Olson, *Aum Shinrikyo: Once and Future Threat?*, 5 EMERGING INFECTIOUS DISEASES 513 (1999), *available at* http://www.cdc.gov/ncidod/EID/vol5no4/pdf/olson.pdf.

Europe to change the European Union Cybercrime Treaty to permit a security exception to the European Union's proposed rule banning tools for accessing computer systems, Professor Eugene Spafford stated:

> System administrators, researchers, consultants, and companies all routinely develop, use, and share software designed to exercise known and suspected vulnerabilities. Academic institutions use these tools to educate students and in research to develop improved defenses. Our combined experience suggests that it is impossible to reliably distinguish software used in computer crime from that used for these legitimate purposes. In fact, they are often identical.[128]

Empirical data also shows that patch code and exploit code are increasingly functional equivalents. Gerhard Eschelbeck of Qualys has mapped the lifecycle of several recent vulnerabilities. His data suggests that even without disclosure, attackers can develop exploits by reverse engineering available patches and then circulating those exploits on the Internet within a matter of days from when the patch is released. [129] Microsoft's Scott Culp agrees that the public is increasingly adept at crafting exploits from patches.

> One of the key security trends over the past three years has been the dramatic shortening of the time between issuance of a patch that fixes a vulnerability and the appearance of a worm carrying exploit code targeting that vulnerability. For the NIMDA virus, that period was 331 days. Only two years later, the Blaster worm shortened the window to just 26 days. And with the Sasser worm outbreak, which was first identified on April 30, 2004, a mere 17 days passed between patch and worm. . . . As a result of this narrowing window, effective patch management, while essential, is not sufficient. [130]

We know, then, that publication restrictions have little or no value after patches are released. Perhaps pre-patch restrictions remain valuable. Still, the decreasing time from patch to exploit suggests that attackers not only increasingly have the knowledge required to create an attack from a patch, but perhaps also to find vulnerabilities in the first place.

[128] *Id.*

[129] Eschelbeck presented this study at the Stanford Center for Internet and Society Conference on CyberSecurity, Research, and Disclosure on November 23, 2003 and at the Black Hat Briefings in a presentation entitled "The Laws of Vulnerabilities" (released in July 2004). The presentation information is accessible and updated regularly *at* http://www.qualys.com/laws. Eschelbeck's conclusions are interesting, but need further study, taking into account the relative seriousness of the vulnerability (e.g. does it allow remote exploits or user exploits), how widely deployed the vulnerable software is, the resources of the typical entities that use the software, public perception of the seriousness of the vulnerability, whether patches issued by the vendor were effective and whether the threat of disclosure played a role in the timely creation, distribution and implementation of any patch.

[130] *Cybersecurity and Vulnerability Management: Hearing Before the Subcomm. on Technology, Information Policy, Intergovernmental Relations and the Census, House Comm. on Government Reform*, 108th Cong. (2004) (statement of Scott Culp, Senior Security Strategist, Trustworthy Computing Team, Microsoft Corporation), *available at* http://www.microsoft.com/presspass/exec/ScottCu/06-02-04TestimonyWritten.asp

Further, the little theoretical work in the legal field on the relationship between security, secrecy and openness supports the theory that computer security, even pre-patch, benefits most from publication. Professor Peter Swire argues that secrecy benefits security more when the attackers have a lot to learn, and the defenders have little to learn, while openness benefits security more when the attackers have little to learn and defenders have a lot. [131] Other variables include the effectiveness of the defensive feature at stopping the first attack, the number of attacks, the ability of the attacker to learn from previous experience, the extent to which the attacker communicates this learning to other attackers, and the extent to which the defenders can effectively alter the defensive feature before the next attack. The effectiveness of secrecy will vary depending on these factors.[132]

Physical security differs from computer security and secrecy plays a different role. In computer systems, copyright protection systems, and other encryption schemes, attackers can attack repeatedly and easily learn and communicate their findings with others. "Firewalls, mass-market software, and encryption are major topics for computer and network security. In each setting, there are typically high values for number of attacks (***"N"***), learning by attackers (***"L"***), and communication among attackers (***"C"***). Secrecy is of relatively little use in settings with high ***N***, ***L***, and ***C***—attackers will soon learn about the hidden tricks. By contrast, many physical-world security settings have lower values for ***N***, ***L***, and ***C***. In these settings of persistent and higher uniqueness, secrecy is of greater value to the defense."[133]

To put this in another way, computer scientists are right, at least in their own field, when they embrace the mantra that there is no security through obscurity. It is far more likely that someone unknown to the vendor or legitimate research community has already found the flaw. When individuals have access to vast computing power and do not need years of training to understand how computer programs work or fail to work, the ability to find security vulnerabilities is much more widespread. There are many more people who can find the next vulnerability in Windows than can find how to synthesize the small pox virus. Secrecy, then, is less valuable because the vulnerability information can be more readily and independently derived by the malfeasants.

Open source software[134] may be a special case that can illustrate the benefit or detriment of openness on security. With open source software the source code is publicly available and so vulnerabilities are easier to find. Many advocates of open source software believe that it is more secure than closed source or proprietary programs, where only the functioning binary code is available. This is because a large group of users can read open source code to cheaply and repetitively search for and find vulnerabilities, while it is expensive and time consuming to debug proprietary software.

Ross Anderson, an expert in the economics of computer security, has argued that neither open source nor closed source software is necessarily more secure. If it is harder for attackers or users to find flaws, it is also harder to perform quality assurance testing

[131] Peter Swire, "A Model for When Disclosure Helps Security: What Is Different About Computer and Network Security?", available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=531782.

[132] *Id*. at 12.

[133] *Id*. at 13

[134] "Open source" means that the object code or source code of the program is publicly available.

and increase the reliability of the software. This is true even though proprietary or closed software vendors rely on initial "alpha testing" by paid insiders with access to source code. Alpha testing is more expensive than subsequent testing performed on closed source in more of a trial and error fashion (beta testing). At a certain point, the rate of bugs found by alpha testers slows and the cost of finding each new flaw increases. At that time, a company will switch to beta testing as a function of pure economics. In a complex system with many flaws, "eventually—in fact, fairly quickly—the beta test effort comes to dominate reliability growth."[135] As a result, making it easier or harder to find attacks helps attackers and defenders equally. Therefore, Anderson argues, the decision of whether open or closed source code is more secure may be more influenced by secondary factors. These include transaction costs that accrue to proprietary vendors who have to fix more flaws if their source code is widely available, vendor reluctance to admit their product is flawed and to ship patches without the threat of disclosure, government pressure to keep vulnerability information quiet so that it can be exploited by law enforcement and national intelligence agents, and the benefit of a numerous testing population that does not have the benefit of source code and is not improperly focusing only on testing certain portions of the code.[136]

Anderson's work is not specifically about vulnerability disclosure, but about the availability of source code as part of the process of testing software for vulnerabilities. But his insight is that greater information benefits defenders and attackers equally because the information can be used both to increase the security of software as well as to attack it. This is the position of those who want vulnerability information, including working code, to use in system defense. Restriction proponents do not deny that the information is useful, only that there are many more attackers who learn from it than defenders. But Swire theorizes that ease of communication (***"C"***) and ease of learning (***"L"***) characterize computer security attacks. ***C*** and ***L*** also characterize computer defense. While Lipner may be right that fewer people know how to use proof of concept code to reconfigure their firewall or improve a virus scanner, the defenders who do know can easily share with those with less expertise. If so, Anderson's insight is true for vulnerability publications. Information helps defenders and attackers equally. Secrecy is false security.

V. Publication Restrictions Contribute to the Market Failure in Security Provision

Perhaps the most compelling reason to permit publication of security vulnerabilities, including operational code, is that consumers need the information to combat monopolistic business practices enabled by new technologies. Today, security measures are rarely implemented for security's sake.[137] They are implemented to lock in customers and to leverage a company's market share in one product into sales in a

[135] Ross Anderson, *Security in Open versus Closed Systems—The Dance of Boltzmann, Coase and Moore*, p. 4 (2002) *at* http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/toulouse.pdf

[136] *Id*. at 4-5.

[137] Ross Anderson, *Why Information Security is Hard—An Economic Perspective*, *at* http://www.cl.cam.ac.uk/~rja14/econsec.html.

complementary product or service. For customers to retain choice and to exert market pressure on vendors to provide secure products, they must have vulnerability information, including code.

Economic studies show that vendors implement weak security, if any, as a rational response to network economies. Network economies are those where the value of a product or service increases with the number of other users. Because value increases when more people use the product, the first vendor to market it has a powerful economic advantage called first mover advantage. Companies want to get their product out to customers as quickly and cheaply as possible, thus will deal with security quickly and cheaply if at all. If security interferes with the work of applications developers or other complementary business, companies will not make resolving the security issues a priority because having more complementary services means the product's value will increase and more people will adopt it.[138]

Also, if security poses an obstacle for users, companies will sell products default insecure.[139] Wireless technology is paradigmatic. The wireless 802.11 waveband can be intercepted by anyone with the appropriate networking card. If users want to keep their wireless transmissions secure, they must either encrypt the signal or block unauthorized wireless network cards from using the wireless router. Both measures make it more difficult for customers to get their own machines on the wireless service. Businesses therefore sell wireless routers with all security turned off. It is easier for customers who are happy that their new toy works and it is cheaper for the vendor, who does not have to field that many more technical support calls. As a result, the users rather than the vendors shoulder the risk of insecurity.

Vending insecure products, then, may be the result of rational economic decision making rather than malfeasance or even lack of know-how on the part of business. For this reason, Ross Anderson and economics professor Hal Varian have argued that discussions about improving security have focused too much on system design and not enough on economic or political issues.[140] Anderson says that insecurity is best explained by network externalities, asymmetric information, moral hazard, adverse selection, risk dumping, and Tragedy of the Commons effects, than it is by lack of information about good design.[141]

If network economies tend to produce less secure products, the problem is exacerbated when customers have less information about that insecurity than the vendors do. When buyers do not have as much information as sellers do, there is a downward pressure on a product's price and quality. When information about computer security is expensive to obtain, buyers must make sub-optimal decisions. They will choose the older, more well-known products that may contain much insecurity over a newer, unknown and more secure product. Uninformed buyers will refuse to pay a higher price for a better product, since they cannot be sure it is better. Vendors will have no economic incentive to sell the better product, if no one knows that it is superior or is willing to pay for it.

[138] *Id*. at 2.

[139] *Id*. at 3.

[140] *See* Hal R. Varian, *Managing Online Security Risks* N.Y. Times, June 1, 2000, *available at* http://www.sims.berkeley.edu/~hal/people/hal/NYTimes/2000-06-01.html.

[141] Anderson, *Why Information Security is Hard*, 8.

Security as a whole suffers from lack of public oversight, particularly since the current market does not promote allocation of sufficient resources to combat vulnerabilities in products. Customer pressure for better products is one important incentive for companies to create secure products. The ability of consumers to bring that pressure to bear must be backed, not undermined, by law. Varian argues that system design will not improve unless liability rules are structured such that the party who is best suited to manage risk bears the financial responsibility if security is breached. Varian points to Ross Anderson's study of fraud at automated teller machines. In the U.K., where errors are presumptively against bank customers, the machines are insecure and fraud is rampant. In the U.S., where errors are presumptively the fault of the bank, teller machines are far more secure and there is far less fraud. Liability rules can allocate the incentives for security to maximize benefit.[142] However, liability cannot be imposed in the absence of information about insecurity. In a networked economy, it is all the more important for customers to be well informed about security.

Working code in particular is critical if consumers are to escape anti-competitive restraints companies are currently encoding in security measures. In a networked economy, it is especially important that customers do not switch products, so companies will prefer a proprietary and obscure architecture that increases customer lock-in.[143] They may also try to make it more difficult for competitors to create compatible products, or to leverage strength in one market for sales in another. As a result, we see businesses implementing security measures, not for information security per se, but to meet other economic objectives, including (1) differentiated pricing and (2) artificially increasing switching costs by, for example, making systems incompatible and hard to reverse engineer.[144]

Anderson uses the example of Microsoft's Passport product, which stores usernames and passwords for multiple websites and Internet services that a customer may access:

> Microsoft can collect a huge amount of data about online shopping habits and enable participants to swap it. If every site can exchange data with every other site, then the value of the network to each participating web site grows with the number of sites, and there is a strong network externality. So one such network may come to dominate, and Microsoft hopes to own it. Second, the authentication protocols used between the merchant servers and the Passport server are proprietary variants of Kerberos, so the web server must use Microsoft software rather than Apache or Netscape (this has supposedly been "fixed" with the latest release, but participating sites still cannot use their own authentication server, and so remain in various ways at Microsoft's mercy). So Passport isn't so much a security product, as a play for control of both the web server and purchasing information markets.[145]

[142] Varian.

[143] Anderson, *Why Information Security is Hard*, 3.

[144] *Id*. at 3-4.

[145] *Id.* at 4.

Anderson gives other examples of cryptographic security in laser printers for the purpose of downgrading print quality if users install competitor toner cartridges, and security in mobile phones that notes if the user has installed a competitor's batteries and drains them more quickly.[146] Security is used to protect market share, not to protect consumer information.

Two recent DMCA cases illustrate the central role exploit code plays in liberating customers from these lock-in strategies: *Lexmark v. Static Control Components*[147] and *Chamberlain Group Inc. v. Skylink Technologies Inc.*[148] In both cases, vendors tried to force customers who bought one of the company's products to also buy the vendor's complementary product rather than that of a competitor.

Lexmark makes laser printers and sells compatible toner cartridges. It sells discounted cartridges with a shrink-wrap agreement that states that the purchaser agrees to use the cartridge only once and then return it to the company for remanufacture and refill. Software code on a computer chip in the cartridge communicates with code in the printer to check that installed toner cartridges are authorized Lexmark refills rather than third party refills. If the cartridge is not authenticated, then necessary software programs—the Toner Loading Program ("TLP"), which was stored on the cartridge microchip, and the Printer Engine Program ("PEP"), which was stored in the printer—will not operate.

The defendant Static Control Components ("SCC") manufactured compatible printer cartridges. Lexmark's approved cartridges had microchips that contained the authentication code and the Toner Loading Program ("TLP"). SCC's chips contained a short software program that mimicked the authentication sequence and an exact copy of Lexmark's TLP.[149] By mimicking the authentication sequence, the competing cartridges were able to make use of, or "access" the copyrighted TLP and PEP programs.

Lexmark claimed that the authentication sequence controlled access to the TLP and the PEP and that SCC's chips, by mimicking the authentication process, illegally circumvented that access control. The trial court found that the chip's sole purpose was designed to, had the sole commercial purpose of, and was marketed for circumventing the authentication sequence and thereby making the TLP and PEP operate.[150] Therefore, the chip was an illegal circumvention device and the court enjoined SCC from selling its toner cartridges.

SCC argued that its products were designed to work with the Lexmark printers (interoperate) and therefore fit under an exception to the DMCA for reverse engineering.[151] The trial court rejected this defense. The DMCA exception for reverse

[146] *Id.*

[147] 253 F.Supp.2d 943 (E.D. Ken. 2003).

[148] 292 F.Supp.2d 1040 (N.D. Ill. 2003).

[149] *Id.* at 970.

[150] *Id.* at 968.

[151] "Notwithstanding the provisions of subsection (a)(1)(A), a person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively controls access to a particular portion of that program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to the person engaging in the circumvention, to the extent any such acts of identification and analysis do not constitute infringement under this title." 17 U.S.C. 1201(f)

engineering only applies if the circumvention device is made available to others "solely for the purpose of enabling interoperability of an independently created computer program with other programs, and to the extent that doing so does not constitute infringement under this title or violate applicable law other than this section." [152] The court held that the SCC chips were not "independently created" because they "serve no legitimate purpose other than to circumvent Lexmark's authentication sequence and … contain exact copies of Lexmark's Toner Loading Programs."[153] On appeal, the Sixth Circuit reversed. It rejected the trial court's holding that the TLP was protected by copyright. Because the TLP is a functional lock-out mechanism, it does not receive copyright protection or alternatively, SCC's copying was fair use.[154]

In *Chamberlain Group Inc. v. Skylink Technologies Inc.*[155], the court declined to extend DMCA protection from competition to plaintiff Chamberlain, a company that made rolling code garage door openers ("GDOs"). Defendant Skylink manufactured and sold a device that would open a variety of garage door openers, including those manufactured by the plaintiff. Mirroring the successful claims in *Lexmark*, Chamberlain argued that the defendant mimicked its rolling code technology to make use of, or "access" the code that opened the garage door and that Skylink's GDO was therefore an illegal circumvention device under the DMCA.

In ruling against Chamberlain, the trial court focused on the fact that the compatible transmitters opened garage doors only if homeowners inputted the transmitter signal into the GDO.[156] The homeowner is authorized to operate the Chamberlain GDO because Chamberlain does not place any restrictions on the type of transmitters homeowners are permitted to use.[157] Therefore, the devices only access the GDO code with authorization of Chamberlain through the homeowner. Chamberlain countered that it did not anticipate competition in the market for universal transmitters that would open its rolling code GDO.[158] The District Court rejected this argument, noting that customers could reasonably expect that they would have the right to use a universal GDO manufactured by another company.[159] The Appellate Court affirmed, holding that the DMCA does not restrict code that circumvents any applied technological protection measure, but only code that circumvents such measures that prevent access to the copyrighted work for the purpose of copy control.[160]

SCC's chip in *Lexmark* and Skylink's garage door opener in *Chamberlain* both contained exploit code that functionally circumvents a security measure. The facts of both cases demonstrate that companies use security measures to lock-out competitors. Exploit code enables consumers to use whatever toner cartridges they like in their printers, just as the shaving public can use whatever razor blades they like in their razors.

[152] 17 U.S.C. 1201(f)(2),(3).

[153] *Id.* at 971.

[154] *Lexmark v. SCC*. "On this record, pure compatibility requirements justified SCC's copying of the Toner Loading Program."

[155] 292 F.Supp.2d 1040 (N.D. Ill. 2003).

[156] *Id.* at 1044.

[157] *Id.* at 1044-45.

[158] *Id.*

[159] *Id.* at 1046.

[160] 381 F.3d 1178, ___, 2004 U.S.App. LEXIS 18513, *66-67 (Fed. Cir. 1994).

While both cases eventually resulted in victories for the exploit code purveyor, the DMCA's legal restrictions on exploit code left both businesses under an expensive legal cloud.

If vendors are using security mechanisms primarily to limit customer choice rather than to protect customer data, then restrictions on the publication of functional code primarily promote customer lock-in, increased transaction costs, and product tying, not information security. Policy makers should loathe putting the power of law behind these anti-competitive practices, particularly in a networked economy that already provides few incentives for the production of secure products. Only the availability of working exploit code—which opens garage doors, interoperates with printers, or allows users to play DVDs on the device of their choosing—can serve this purpose.

CONCLUSION

Researchers, civil libertarians and policy makers have long agreed that uncensored publication and thorough peer review is essential to developing accurate scientific knowledge. Based on this consensus, U.S. law generally restricts publication only of information owned by or produced for the U.S. Government, when disclosure could reasonably be expected to result in damage to the national security, if the classifying authority can describe the damage from disclosure, and in specific areas of study that pose special problems for national security like weapons of mass destruction, nuclear facility or materials security, and military operations.

Computer science and encryption researchers often use computer code to explain ideas and prove results. As with formulas in mathematics or laboratory descriptions in microbiology, code is the clearest and most precise way to convey information from the computer science researcher to the reader. It can also be compiled either directly or with some modifications into a functional program. In this way, computer security publications differ from publications in other scientific fields. The publication not only says something, it does something. Peers and vendors can use the functional code to confirm the researcher's results. Some system administrators find this working code helpful in testing their systems or configuring firewalls and intrusion detection (early warning) systems. The U.S. Government recognizes the value of sharing vulnerability information and sponsors or participates in many popular mailing lists for this information. But attackers also use the code as a tool to take advantage of security flaws.

Legislators have readily restricted the publication and distribution of software code and shown an inclination to regulate other security vulnerability publications as well. The DMCA outlaws the distribution of computer code that circumvents technological access controls placed on copyrighted works. Copyright owners have used the law to threaten academics publishing research papers, computer hackers disclosing operating system flaws, magazines publishing programs that allow owners to play DVDs on the device of their choosing, as well as companies selling after-market garage door openers and toner cartridges. The U.S. Critical Infrastructure Information Act encourages companies to tell the government about infrastructure vulnerabilities, but then prohibits disclosure under the Freedom of Information Act, state sunshine laws, the Federal Advisory Committee Act or to Congress. The European Cybercrime Treaty requires signatories to treat security tools like burglary tools and outlaw them unless they are possessed for a legitimate security or research purpose.

Willingness to restrict security publications is only partially a result of concern about the functionality of code. This approach is also popular because catching computer attackers is difficult, time consuming, and often not worth the trouble, though the problem of insecurity is in aggregate serious. Regulating intermediaries like publishers is easier. There is also a cultural divide. Corporate managers do not tend to trust the stereotypical security researcher. Perhaps most importantly, technology and content vendors do not want customers to either know that their products are insecure or be able to break technological lock-in measures they have developed. These vendors are an important and effective lobby for their cause. They have been able to frame the debate as creators vs. pirates (*Universal Studios v. Reimerdes*), or vendors vs. crackers (*United States v. Bret McDanel*). But as the *Lexmark* and *Chamberlain* cases show, an equally accurate description is would-be monopolists vs. consumers.

Customers need information about computer insecurity to pressure vendors to patch products and to make security a priority. Network economics at work in the technology market strongly favor first movers. If security is not a priority for consumers—and it cannot be if they are uninformed—companies will not spend resources getting it right. If security makes the product more difficult for customers to use, companies will ship the products in an insecure mode or leave security out altogether. And, if security interferes with developers of complementary products or services, companies will leave it out. This is not immoral; it is just rational economic decision-making. Where companies do take the time to implement security measures, it is often to parlay success in one market into success in the provision of a complementary product. Security measures are used to lock-in customers as Ross Anderson explains of Microsoft Passport, laser printers and toner cartridges, cell phones and batteries. Natural language information about vulnerabilities in these technological protection measures is not enough. Only working exploit code frees consumers from the lock-in.

So in addition to the usual scientific reasons to protect sharing and openness in computer science research, there are special reasons why openness, including the availability of exploit code, promotes security and benefits the public. Moreover, secrecy probably does not benefit security as much as proponents of disclosure restrictions would hope. Certainly there are many more attackers who benefit from exploit code than there are defenders who can use it to test patches or create intrusion detection signatures. The risk that computer security code will be misused is currently much greater than the risk that other scientific research will be misused. Computer attacks simply do not cost as much or pose the same risk of getting caught that misuse of “dangerous science” does. On the other hand, the harm from a computer attack is of a different magnitude than the harm from a biological weapon, for example.

But it is more likely in the computer security field that an attacker has already discovered a vulnerability and is using it. While in the military realm, loose lips do indeed sink ships, Peter Swire’s work suggests that in the networked world there is truth to the adage that there is no security through obscurity. The hallmark of the Internet is its value as a communications device. Computer attackers benefit from this frictionless environment. Would-be intruders can inexpensively and easily gain the expertise needed to break security through study, repeated test attacks, and easy communication with other attackers. Under these circumstances, secrecy is of little value. Attackers will learn the hidden tricks.

There are better ways to thwart computer crimes that do not impinge on scientific progress, or scare legitimate researchers and companies, or limit customer choice. Policy makers should promote the exchange of security information, peer review and field-testing; encourage users to protect computer systems by installing secure software, using encryption, and exercising sound judgment about the disclosure of sensitive information; and use market factors, insurance and liability allocation to encourage vendors to make security a priority.

END